

Declaration

Name of candidate:

Brian Foster

This Thesis/Dissertation/Research Project entitled:

The Socio-Economic Impact of Unsolicited Bulk Email (spam) on New Zealand Organisations and Employees: Comparative Case Studies

is submitted in partial fulfillment for the requirements for the Unitec degree of
Master of Computing

CANDIDATE'S DECLARATION

I confirm that:

- This Thesis/Dissertation/Research Project represents my own work;
- The contribution of supervisors and others to this work was consistent with the Unitec Regulations and Policies.
- Research for this work has been conducted in accordance with the Unitec Research Ethics Committee Policy and Procedures, and has fulfilled any requirements set for this project by the Unitec Research Ethics Committee.

Research Ethics Committee Approval Number: **2006.548**

Candidate Signature:Date: **3 October 2007**

Student number: **1104382**

**The Socio-Economic Impact of Unsolicited Bulk Email (spam)
on New Zealand Organisations and Employees:
Comparative Case Studies**

By
Brian Foster

A dissertation submitted in partial fulfilment of the
requirements for the degree of Master of Computing
at Unitec New Zealand, August 2007

Abstract

Unsolicited Bulk Email (UBE), or as it is more commonly known, spam, has in a few short years become arguably the most annoying, frustrating and even hated aspects of life on the Internet today, turning what was once considered the Internet's "killer app" into a technical and security disaster of global proportions. Although significant international research has been done into studying the effects of UBE and ways of preventing it, very little is known about the impact it has within New Zealand.

This research document details an exploratory investigation into how UBE is affecting organisations and their employees within New Zealand, by choosing two organisations from completely different industries in Auckland, New Zealand, and conducting in-depth comparative case studies into the economic cost of UBE to the organisations, and the effect it has on the employees who are receiving it. The primary goals were to calculate the economic cost of UBE to each organisation with their current anti-spam system(s), an estimated cost if no anti-spam system was in place, and to try and measure the attitudes and effective states of the employees who are receiving UBE.

Key findings of the research indicate that for an organisation receiving high volumes of UBE, use of a properly configured and maintained anti-spam system (or layered systems) will provide a considerable economic saving over no system at all, but an incorrectly configured and maintained system can actually be no better or worse than having no anti-spam system at all, and high levels of UBE or false positives are resulting in customer orders being accidentally deleted. Just as importantly, the main effect UBE has on employees is to cause work-related stress in the form of anger and frustration, not only about the UBE received, but also the number of false positives the anti-spam systems are generating in attempts to prevent it.

Acknowledgements

The first acknowledgement must go to my wife, Ely, who has probably been through as much stress over the last five years of study as I have, and I have been truly blessed to be married to such a special person as she is.

I must particularly thank Dr. Donald Joyce, my principal supervisor, who taught one of the first papers I took, and made me realise that Information Technology is not just about the technology, it's about the people who are affected by it too. Your guidance was invaluable, and your understanding through all that events that occurred during the course of the research was greatly appreciated.

Thanks also to my other supervisors, who contributed greatly to the final product, Dr. Logan Muller and Shaneel Narayan.

A special thanks to Dr. Deepa Marat from the Unitec Postgraduate Centre, who provided many hours of assistance with the analysis, and guidance with the writing.

Thanks to Dr. Kay Fielden for all you taught me about the research process, and for proof reading parts of this at such short notice.

Thanks also to my manager, Gerard, and John our (now former) IT Director, for giving me a job and making this all possible in the first place, and for your encouragement.

To the participating organisations, their IT managers and their employees, who will remain anonymous, but without whose cooperation this research would not have been possible, and to the EMA (Northern), who found them for me, thank you, and I hope the results help you and other organisations within New Zealand.

Finally, to both of my mothers, neither of who were able to see this, and to Dad, who was able to, this is for you too.

Table of Contents

Abstract	2
Acknowledgements	3
List of Tables.....	9
List of Figures	15
Abbreviations.....	16
Definitions	16
Chapter 1 - Introduction.....	17
1.1 Background.....	17
1.2 Purpose Statement	19
1.3 Research Questions	19
1.4 Delimitations	20
1.5 Limitations.....	20
1.6 Significance	21
1.7 Summary.....	21
Chapter 2 - Literature Review	22
2.1 Introduction	22
2.2 Economic Impact of UBE	23
2.3 Social Impact of UBE.....	24
2.4 Legal Impact of UBE.....	27
2.5 Technical Impact of UBE.....	31

2.6	Organisational Best Practices to Minimise the Impact of UBE	32
2.7	Summary.....	33
Chapter 3 - Research Design		34
3.1	Introduction	34
3.2	Methodology.....	34
3.3	Methods	35
3.4	Research Framework	36
3.5	Data Collection Design.....	37
3.5.1	Sampling Design	37
3.5.2	Instruments	38
3.6	Data Analysis.....	44
3.6.1	Quantitative Data	44
3.6.2	Qualitative Data – Thematic Analysis	48
3.7	Follow-up Discussions	48
3.8	Ethics Issues	48
3.9	Summary.....	49
Chapter 4 - Results and Descriptive Analysis.....		50
4.1	Introduction	50
4.2	Organisation Backgrounds	50
4.2.1	Organisation 1 Background.....	50
4.2.2	Organisation 2 Background.....	51

4.3	Results Question Map.....	54
4.4	Survey Socio-Economic Results and Descriptive Analysis	55
4.5	Analysis of Employee Interviews (RQ2).....	121
4.6	Economic Analysis	130
4.6.1	Introduction	130
4.6.2	Comparative Cost Analysis and Filtering Return on Investment.....	130
4.6.3	Organisational Spam Filtering Models (RQ1)	133
4.6.4	Spam Filtering Cost Analysis Organisational Differences	134
4.6.5	The Cost of Spam in New Zealand Organisations	136
4.6.6	Rule-of-Thumb Economic Cost of Spam for Organisations (RQ1).....	137
4.7	Summary.....	137
Chapter 5 - Discussion and Inferential Analysis		139
5.1	Introduction	139
5.2	How UBE is impacting organisations economically (RQ1).....	139
5.2.1	Anti-spam systems and the economic impact of spam	139
5.2.2	Content Based Filtering (CBF) and the economic impact of spam	140
5.2.3	Anti-spam techniques and the economic impact of spam.....	142
5.3	How UBE is impacting employees in NZ organisations (RQ2).....	144
5.3.1	Affective impacts	144
5.3.2	Behavioural impacts.....	146
5.3.3	Cognitive impacts.....	148

5.4	How employees are impacted differently because of their gender (RQ3)	150
5.4.1	“Sexual” spam affects women significantly more than men	150
5.4.2	More men than women like to receive certain types of spam.....	151
5.4.3	Women are usually more frustrated by spam than men	151
5.4.4	Men usually don’t care about spam	151
5.4.5	Gender stereotypes and emotional responses to spam	151
5.5	Summary.....	152
Chapter 6 - Conclusions and Recommendations		153
6.1	Introduction	153
6.2	Conclusions	153
6.3	Recommendations	154
6.3.1	Organisational best practice to reduce the impact of UBE	154
6.3.2	Recommendations for further research	155
6.4	Limitations of the research	156
6.5	Strengths of the research.....	156
6.6	Summary.....	156
Appendix A - Organisational Questionnaires (RQ1, RQ2)		157
	Cost calculation data for Organisation 1 (OQ1.2).....	158
	Cost calculation data for Organisation 2 (OQ2.2).....	160
Appendix B – Job Emotion Scale (JES)		161
Appendix C – Online Employee Survey		162

Appendix D – UBE Cost Analysis Spreadsheet Model	170
Appendix E – Employee Interview Forms	171
Appendix F – Individual Employee Interviews	173
References	223

List of Tables

Table 1: Question Type Model, based on (de Vaus, 1995) and (Zikmund, 2003)..... 39

Table 2: Question Design for Organisational Questionnaire, OQx.1 (RQ1, RQ2) 40

Table 3: Question Design for Web-based Employee Survey (RQ2, RQ3) 41

Table 4: Research Method/Question/Results Table map..... 54

Table 5: Gender/Ethnicity (RQ2, RQ3)..... 55

Table 6: Wage/Salary Range (RQ1) 56

Table 7: Experience Using Email (years) (RQ2, RQ3) 57

**Table 8: Have Ever Received Any Spam Emails in Work Account (RQ1, RQ2, RQ3)
..... 58**

Table 9: Have Received Spam Email in the Past Two Weeks (RQ1, RQ2, RQ3) 58

Table 10: Spam email Received (per day) (RQ1, RQ2) 59

Table 11: Descriptive statistics for: Spam email received (per day) (RQ1, RQ2)..... 60

Table 12: Time to Identify and Delete One Spam Email (RQ1) 61

**Table 13: Descriptive Statistics for: Time to Identify and Delete One Spam Email
(Seconds, all Respondents) (RQ1) 62**

Table 14: Frequency of deleting Spam Email (RQ1, RQ2) 63

**Table 15: Do You Believe You Are Receiving Less or More Spam Now Than a Year
Ago? (RQ1)..... 64**

Table 16: Why Am I Receiving Spam? (RQ2)..... 65

Table 17: Other Reasons why I may be Receiving spam (Org1) (RQ2)..... 67

Table 18: Other Reasons why I may be Receiving spam (Org2) (RQ2)..... 68

Table 19: Thematic Summary of Respondent’s Reasons why they may be Receiving spam (RQ2) 68

Table 20: Generally Block Spam Quite Well (RQ1, RQ2, RQ3) 70

Table 21: Let Too Many Spam Emails Through (RQ1, RQ2, RQ3) 70

Table 22: Block Unsolicited Emails (Spam) I Want (RQ1, RQ2, RQ3) 72

Table 23: Block Good Emails (Non-Spam) I Want (RQ1, RQ2, RQ3) 72

Table 24: Other Organisations Have Ever Bounced-back Your Email as Spam (RQ1, RQ2)..... 74

Table 25: Have Ever Accidentally Deleted Good Emails While Deleting Spam (RQ1, RQ2)..... 74

Table 26: Have Ever Opened Untagged Emails That Looked Like Possible Spam (RQ1, RQ2) 74

Table 27: Reasons for Opening (possible) Spam Email (Org1) (RQ1, RQ2)..... 76

Table 28: Reasons for Opening (possible) Spam Email (Org2) (RQ1, RQ2)..... 78

Table 29: Thematic Summary of Reasons for Opening (possible) Spam Email (RQ1, RQ2)..... 78

Table 30: Have Ever Clicked on a Graphic or Link within a Spam Email (RQ2, RQ3) 81

Table 31: Reason Given for Clicking on Link within a Spam Email (RQ2)..... 81

Table 32: Have Ever Purchased a Product or Service Offered in a Spam Email (RQ2, RQ3)..... 82

Table 33: Have Ever Received a "Phishing" Type Email for a Bank, PayPal etc. (RQ2)	83
Table 34: Have Ever Clicked on Link in Phishing Email and Logged-in (RQ2)	83
Table 35: Selling Cheap Software (RQ2, RQ3)	84
Table 36: Sexual Performance Drugs (RQ2, RQ3)	85
Table 37: Weight Loss Drugs/Programmes (RQ2, RQ3).....	86
Table 38: Male Enhancement/Enlargement Products (RQ2, RQ3)	87
Table 39: Mortgage/Loan Financing (RQ2, RQ3).....	88
Table 40: Job/Employment Offers (RQ2, RQ3)	89
Table 41: Adult Pornography Websites (RQ2, RQ3).....	90
Table 42: Child Pornography Websites (RQ2, RQ3).....	91
Table 43: Dating Websites (RQ2, RQ3)	92
Table 44: Stock Market "Tips" (RQ2, RQ3)	93
Table 45: Online Casino Websites (RQ2, RQ3).....	94
Table 46: "Nigerian" Fraud (RQ2, RQ3)	95
Table 47: Selling Other General Products/Services (RQ2, RQ3)	96
Table 48: Spam in General (RQ2, RQ3)	97
Table 49: It is a Waste of my Time at Work (RQ2, RQ3)	98
Table 50: I Worry that Fellow Employees Might see it (RQ2, RQ3).....	99
Table 51: It Makes me Angry (RQ2, RQ3)	100
Table 52: I Enjoy Receiving it (RQ2, RQ3)	101

Table 53: It is an Intrusion on my Privacy (RQ2, RQ3).....	102
Table 54: I Delete them Immediately (RQ2, RQ3).....	103
Table 55: They are Sometimes Interesting to read (RQ2, RQ3).....	104
Table 56: The email was sent by the Person it says it is "From:" (RQ2, RQ3).....	105
Table 57: I Sometimes Forward it on to Colleagues or Friends (RQ2, RQ3).....	106
Table 58: It Makes me Frustrated (RQ2, RQ3).....	107
Table 59: I Believe they are Mostly Deceptive or Fraudulent (RQ2, RQ3).....	108
Table 60: I have Sometimes Replied to them (RQ2, RQ3).....	109
Table 61: I Sometimes Report it to my Manager or IT Dept (RQ2, RQ3).....	110
Table 62: I Sometimes find the Content of the Email is Objectionable (RQ2, RQ3)	111
Table 63: I am Concerned I Might Accidentally Delete good Emails with spam (RQ2, RQ3).....	112
Table 64: I wish the IT Dept would do more to stop it (RQ2, RQ3).....	113
Table 65: I am Worried I am Receiving it Because I may have Accidentally Visited a Website with Similar Content (RQ2, RQ3).....	114
Table 66: I Hate Receiving it (RQ2, RQ3).....	115
Table 67: I Worry my Colleagues or Manager Might see me Reading it, if it is Objectionable Content (RQ2, RQ3).....	116
Table 68: Final Respondent Comments from Org1 (RQ2).....	117
Table 69: Final Respondent Comments from Org2 (RQ2).....	119
Table 70: Thematic analysis of respondent's final comments (RQ2).....	120

Table 71: Gender 121

**Table 72: Q1.a Have you read, heard or seen much about UBE (spam) in the media?
..... 121**

Table 73: Where have you read, heard or seen much about spam in the media?..... 121

**Table 74: Q1.b Has your organisation provided you with any information about
UBE? 121**

Table 75: Q1.c What sort of information has the organisation provided? 122

Table 76: Q1.d How do you think the spammers got your email address? 122

Table 77: Types of spam received by participant in the past (RQ2, RQ3) 123

**Table 78: Q2.b Has the amount of UBE you receive increased or decreased in the past
12 months? 123**

Table 79: How participants feel about the UBE they receive..... 124

Table 80: Q3.d If not, how do you think you might feel in that situation? 125

Table 81: Q4.a.i Ever clicked on the link provided in the email? 125

**Table 82: Q4.b For any other non-financial unsolicited emails, have you ever clicked
on any links included in unsolicited emails you have received? 126**

Table 83: Q4.c If “Yes”, what was the reason you clicked on it?..... 126

Table 84: Q4.e What do you normally do with the unsolicited emails you receive?. 126

**Table 85: Q5.c How well do you think your organisation is doing in controlling the
amount of unsolicited email that you receive? 127**

**Table 86: Q5.d Do you think more could be done by your organisation to control
unsolicited email? 127**

Table 87: Q5.e If “Yes”, what more do you think they could do to control it?	128
Table 88: Q5.f Do you think your organisation could provide you with more information about unsolicited email?	128
Table 89: Q5.g If “Yes”, what information do you think they should provide?.....	128
Table 90: Other emergent participant themes, attributes, attitudes and events	129
Table 91: Cost Analysis with Spam Filters (RQ1).....	131
Table 92: Cost Analysis without Spam Filters (RQ1)	132
Table 93: Organisational UBE filtering techniques comparison (RQ1).....	134

List of Figures

Figure 1. Literature Map 22

Figure 2. Research Framework for Comparative Case Studies using Replication 36

Figure 3. Organisational spam filtering: Model comparison 133

Abbreviations

AUP	Acceptable Use Policy	IT	Information Technology
CBF	Content Based Filter	JES	Job Emotion Scale
HR	Human Resources	ROI	Return On Investment
ISP	Internet Service Provider	UBE	Unsolicited Bulk Email

Definitions

Unsolicited Bulk Email (UBE)

Any substantially identical emails sent to large numbers of email addresses, from a sender unknown to recipients who had not given permission for the email to be sent.

This definition is intended to include Unsolicited Commercial Email (UCE) marketing products or services such as Viagra, job offers or pornographic web sites, fraud or identity-theft emails such as Nigerian scams and "phishing" attempts (that ask you to go to a bank or financial website such as Pay Pal and enter your username and password).

Emails that contained viruses, or emails sent within the organisation to some form of "All Users" distribution list are not included in this definition.

Spam

Unsolicited Bulk Email (UBE) as defined above. This term will be used interchangeably with the abbreviation UBE, as it is the commonly recognised term for UBE.

Chapter 1 - Introduction

1.1 Background

Email is a major part of life on the Internet. For example, the Pew Internet & American Life Project has conducted some 32 polls on a regular basis between April 2000 and February 2005, which consistently show that 90% or more of the respondents have sent or read email at some time (Fallows, 2005, p. 8).

Unfortunately for Internet users with email addresses, the receipt of UBE, or spam, has also become a major part of email life, with significant negative impacts for those who receive it.

According to recent reports (MessageLabs Ltd., 2007, p. 1; Messaging Anti-Abuse Working Group, 2007, p. 2), approximately 70-80% of all current email traffic is spam or “abusive” email, and spammers continue to develop new techniques, such as using email “stationary” or “wallpaper” (Framingham, J. B., 2007), to force their way into the Inboxes of employees in organisations worldwide.

As recently as the time of this writing (June 2007), a disturbing new tactic being used by some spammers, called “spam spikes” (Framingham, G. K., 2007), appears to be deliberately targeting specific domains (and the organisations behind them) with what amounts to a Distributed Denial of Service (DDoS) spam attack, presumably in an attempt to overwhelm the anti-spam systems protecting the organisation.

UBE in the New Zealand context

The sheer volume and persistent onslaught of UBE has meant that some New Zealand ISPs have also been struggling to cope with the increasing load of junk email they must process daily (Saarinen, 2006).

Although a number of surveys and studies have been and continue to be done overseas, little research appears to have been done on its impact on New Zealand organisations, as

noted by Brad Ward from the IT Policy Group, Ministry of Economic Development, who stated “At present there are no detailed statistics on the incidence and effect of spam in New Zealand, so we have to rely on anecdotal evidence and comments and on statistical evidence collected overseas.” (Ward, B., 2003).

At least three surveys have been done in New Zealand, that have asked brief questions about UBE, as their focus has been on Internet Security.

UBE-related questions included in these surveys were:

Small business Internet security survey results (2004)

Q15: Does your business have any of the following security solutions installed?

(Included Spam Filtering as one of the options)

Q18: Approximately how many spam emails do you receive daily?

Q21: What are the two top IT issues impacting your business?

(Spam was listed in third place at 8%)

(Employers and Manufacturers Association (Northern), 2004)

NetSafe Internet security survey (2004)

Q22: How much of an issue is unsolicited junk email, spam?

(47% found it a minor irritant, 22% a major annoyance, and 4% seriously interfering with their business online)

Q23: How much of your daily email traffic is spam?

(The Internet Safety Group & MYOB, 2004)

Symantec and EMA Internet security survey 2005

Q20: Approximately how many spam emails do you receive daily?

Q21: Have you ever been the target of a phishing attempt?

(Approximately 50% had been)

Q24: What are the top two IT issues impacting your business?

(Spam, virus and email threats ranked top of this list, at 14.9%)

(Employers and Manufacturers Association (Northern), 2005)

These surveys have not specifically focused on UBE and its impact in New Zealand, but have at least attempted to quantify respondents’ daily spam levels, and identified that it is definitely impacting on businesses in New Zealand.

Although the surveys noted on the previous page have partially begun to fill in the gap identified by Brad Ward, there is clearly a need to conduct more detailed studies on the effects of UBE in New Zealand.

Little research appears to have been conducted into New Zealand employee's knowledge about UBE, attitudes towards UBE, beliefs about why they or their colleagues are receiving UBE, their behaviour regarding received UBE or any emotional stress some types of UBE may cause them.

This research is therefore concerned with investigating the impact of UBE on organisations and their employees, within a New Zealand context.

1.2 Purpose Statement

After consideration of the current literature and the gaps identified as they relate to New Zealand, the purposes of this research are therefore:

1. To determine how UBE is impacting selected organisations economically
2. To explore the attitudes (knowledge, beliefs, behaviours), possible stress of, and any gender differences between employees regarding UBE they receive
3. To compare the above impacts between organisations with similar levels of UBE blocking/filtering

1.3 Research Questions

RQ1: How is UBE impacting NZ organisations economically?

RQ2: How is UBE impacting employees in NZ organisations (socially)?

RQ3: Are employees impacted differently because of their gender?

(Note: References to research question will use abbreviations: RQ1, RQ2 and RQ3)

1.4 Delimitations

1. The scope of the research was confined to studying two organisations based in Auckland, New Zealand.
2. Because the research is on the impact of UBE, the organisations were required to be receiving UBE, which necessitated purposeful, rather than random, selection of the organisations (and employees) to be studied.
3. The organisations selected were of a size adequate to provide meaningful statistical data from survey responses, comprising approximately 500 and 1,200 employees respectively.
4. The survey participants had email addresses within the organisation's domain, capable of receiving email from the Internet, and have web-browser access to the Internet.

1.5 Limitations

The main limitation of the research is that only two organisations were studied, and therefore the research may not be able to be generalised to other organisations within New Zealand, the majority of which will have far fewer employees.

Conducting a comparative, multiple-case study, however, is regarded as preferred and providing more substantial analytic benefits than a single-case design (Yin, 2003, p. 53).

Also, as some of the research is qualitative, the resulting interpretations may be arguable.

1.6 Significance

The significance of this research is that it will provide economic data that will help fill the gap in our knowledge about how much UBE is costing New Zealand organisations.

The economic data may also help organisations justify further investment in anti-spam technology, to block UBE from entering the organisations email systems, reducing the impact on employee time and productivity.

Equally as important, it is hoped this research will provide an insight into how the contents of UBE can affect the employees who receive it, which could be used to shape Human Resource (HR) policies and Information Technology (IT) policies that recognise the obligations employers have to protect their employees from any objectionable or other potentially harmful content (e.g. fraud) that may be contained in the UBE they receive.

1.7 Summary

This chapter has introduced the problem of UBE as a global issue affecting email users worldwide, highlighting the persistent and aggressive nature of spammers.

UBE in the New Zealand context shows that it has a major impact on ISPs, but as yet no comprehensive research about its impact on New Zealand organisations.

The purpose statement outlined the areas to be explored, and the research questions stated the specific problems to be answered.

The delimitations and limitations set the boundaries and parameters within which this study has taken place, and finally, the significance of the study in terms of the knowledge to be gained about the impact of UBE in a uniquely New Zealand context, and the benefits that it may provide for organisations trying to minimise its impact on their business.

Chapter 2 - Literature Review

2.1 Introduction

Much has been written about spam or UBE since it first became a significant problem at the end of the 1990's. This chapter provides an overview of some of the literature published about UBE (spam), both internationally and within New Zealand.

A review of literature published during the last few years revealed that the majority fell into five main categories, as shown in (Figure 1):

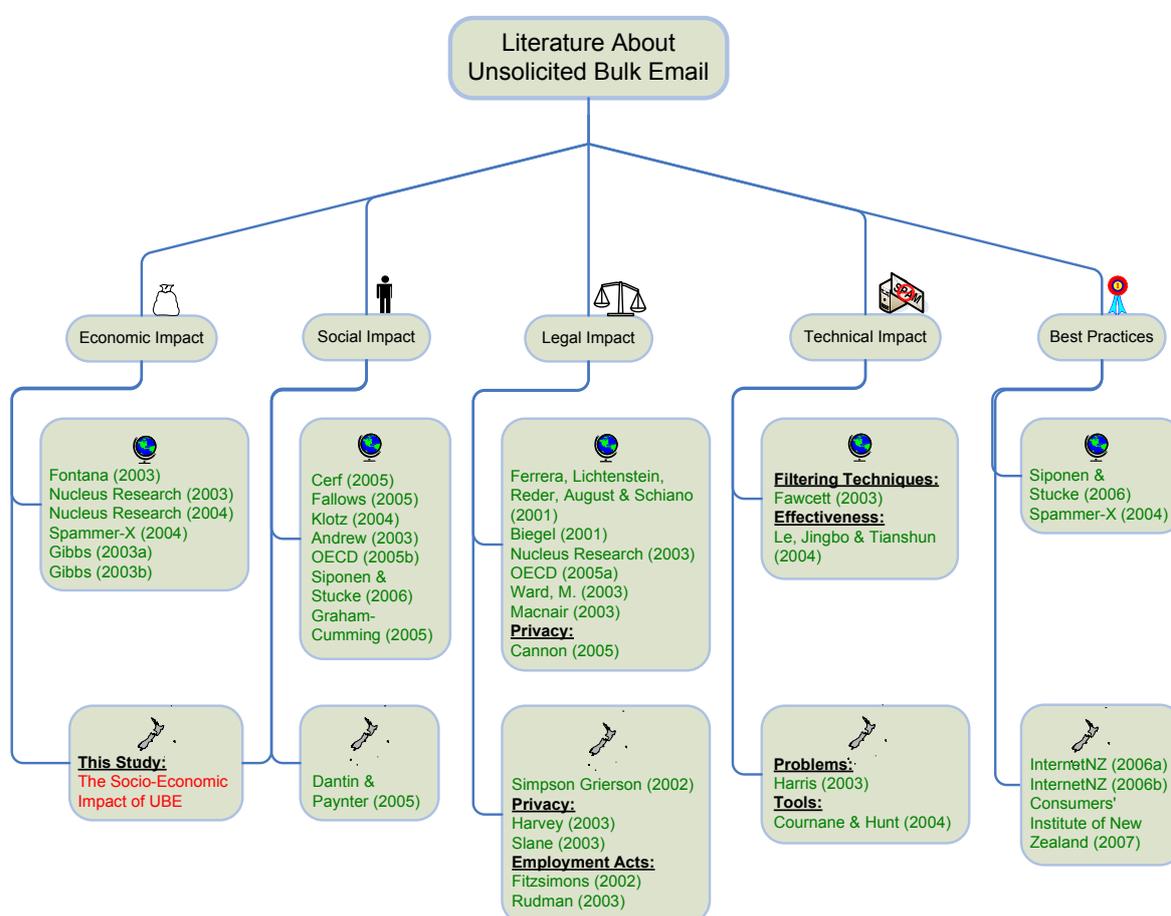


Figure 1. Literature Map

In the Literature Map above, each category has been further separated into two sub-categories:

New Zealand literature (🦘) and non-New Zealand literature (🌐).

2.2 Economic Impact of UBE

Many articles and some research internationally have tended to focus on the economic impact of UBE, in terms of time/productivity losses, and calculating a cost to business derived from this.

The measurements of time wasted tend to vary from seconds to minutes per email, but this can translate into large economic losses depending on employee's salaries. For example, in a 2003 article in *Network World*, it was found that when a legal firm gave 220 of their lawyers a Blackberry mobile phone, they were rendered almost useless because of the amount of UBE forwarded to them. Taking into account the number of spam emails to delete, the time taken to delete them (estimated at 5 seconds/spam), and the average hourly rate of the users (mostly highly-priced lawyers), losses were calculated at \$US300,000/year (Fontana, 2003). This equates to a cost of spam of approximately \$US1,360 per lawyer per year.

Nucleus Research calculated in 2003, based on interviews with 117 employees at 76 US companies, that the economic cost to businesses came to an average 6.5 minutes per day per employee in lost time, and an average cost of spam of \$US874 per employee per year (Nucleus Research Inc., 2003). In 2004, after interviewing employees at 82 Fortune 500 companies Nucleus Research found this cost had increased in 10 months to \$US1,934 per employee per year (Nucleus Research Inc., 2004, p. 1), based on 30 seconds/e-mail and 29 e-mails/day.

By way of contrast, Spammer-X claimed that it took him only 7 seconds to identify and delete 13 spam messages received the morning of writing chapter twelve of his book, therefore costing only about 30 minutes, or \$US15 (@ \$US30/hour) per year (Spammer-X, 2004, p. 321).

While there are still arguments over the actual cost of UBE, there is no argument that UBE has a measurable economic impact on any organisation.

The basis of a good framework for conducting a quantitative study of the economic impact of UBE was found in a Network World article entitled “What Spam Really Costs, Part I” (Gibbs, 2003a). The second article in the series provides a link to download a spreadsheet that can be used to calculate the total costs, based on the “average fully burdened cost of an employee” (Gibbs, 2003b). The calculations did not include the possibility of connectivity charges in forwarding or retrieving UBE on mobile devices, which was significant in the case of the legal firm mentioned above.

2.3 Social Impact of UBE

“I hate spam!”

For people who receive UBE, this highly emotive statement is one they have probably made, or thought, at least once in their online life, but in this particular case it was the opening statement of an article by none other than Vinton Cerf, who is one of the creators of the TCP/IP protocol suite that underlies the Internet, and who is widely regarded as one of the Internet’s founders. He further considers that the reason why spammers try to conceal the real origins of their emails is because of “the public’s widespread hatred of spam” (Cerf, 2005).

The literature about the social impact of UBE examines people’s attitudes and behaviours towards UBE, the impact it has on their online experience and on them personally.

The 2005 Pew Internet survey showed that:

52% of Internet users consider spam a big problem

67% of email users say spam has made being online unpleasant or annoying...

53% of email users say spam has made them less trusting of email
(Fallows, 2005, pp. 1-2)

But the same survey also found that 6% of respondents had at some time “ordered a product or service that was offered in an unsolicited email” (Fallows, 2005, pp. 4-5), and 2% had supplied personal financial details that were requested by an unsolicited email. A recent book examining Internet communication states that ‘Americans have consistently expressed their frustration, if not anger, with spam. Surveys regularly show that most people dislike spam. A Gallup poll shows that Americans are evenly divided between those who “hate” spam, and those who find it merely “annoying”’ (Klotz, 2004).

Other studies have shown similar attitudes towards UBE.

An international survey conducted in 2003, with 21,102 respondents from more than 36 countries, found that in answer to the question: “How do you feel about receiving spam (unsolicited commercial emails)?”, 95% (20,173 people) said that they either hated spam or that it annoyed them, but 1% of respondents indicated that “I like to receive them” (Andrew, 2003, p. 5).

Of the respondents who added comments at the end of the survey, the report also noted that “Many mentioned that spam invaded their personal space and talked about privacy and rights, ‘Spam is an infringement of my privacy and of my right to choose what I use my Internet connection for.’ (New Zealand)” (Andrew, 2003, p. 5).

A recent report by the OECD Task Force on Spam, released in May 2005, acknowledges that UBE has a social impact on users, stating that “Of course, there are other, sometimes less quantifiable but much more substantial costs faced by the user - ... mental anguish caused by spam with objectionable content, loss of life savings when a user falls for a scam that is e-mailed.” (OECD Directorate for Science Technology and Industry, 2005b).

In a recent international study, researchers in Finland found that frustration and anger were also mentioned by respondents, stating that ‘Two Finnish respondents believed that spam

increases frustration and anger among the employees who receive it: “spam messages increase anger among workers.” (Siponen & Stucke, 2006, p. 5).

The strength of people’s negative emotion was probably most notable in survey results presented to a 2005 spam conference, which found that nearly 11% of respondents “would like to physically harm a spammer (women half as violent as men)” (Graham-Cumming, 2005, p. 11)

A recent New Zealand survey that contained only a very small sample of email users (N=28), concluded that the majority of respondents, for the question “Does spam bother you?”, were “more concerned about losing(sic) genuine messages, their overflowing inboxes, and the waste of time than about disturbing content” (Dantin & Paynter, 2005).

The range of emotions expressed by respondents in these surveys is certainly varied, and the emotional reactions seem to arise as either a result of UBE disrupting their working environment, the contents of the UBE, or both.

The respondents’ comments about their feelings towards UBE include highly negative emotional words such as frustration, anger, hate and anguish, which, in an organisational context, are the subject of studies about affective events theory (AET), and how employee emotional states affect employee retention, job performance and job satisfaction (Ashkanasy, 2002; Grandey, Tam, & Brauburger, 2002).

Considering the depth of negative feeling towards spam expressed by many people, it is possible that in an organisational context, employees could express their frustration at the constant flood of spam in their inboxes by initiating legal action against their employer for failing to stop it. This results in spam having a legal impact on organisations.

2.4 Legal Impact of UBE

The legal impact of spam with respect to an organisation generally has two aspects:

- International and national anti-spamming laws
- Potential for lawsuits by employees against their employers for failing to provide a safe working environment

The impact of UBE knows no international boundaries, and has reached such a level that many governments and international organisations have been forced to resort to enacting anti-spam laws, in an attempt to stem the rising tide.

In the U.S.A., the CAN-SPAM Act of 2003 came into force on January 1, 2004. This marked a major milestone in anti-spam legislation, as studies have determined that the majority of UBE originates from the U.S.A. Enforcement of CAN-SPAM is under the jurisdiction of the Federal Trade Commission (FTC), which regulates advertising (Ferrera, Lichtenstein, Reder, August, & Schiano, 2001).

Senders of UBE can be and have been prosecuted under a variety of existing laws in the U.S.A., including: “Crimes Against Property – Physical or Intangible ... trespass, vandalism, theft, data storms, denial of service” (Ferrera et al., 2001), “trespass to chattels” (Biegel, 2001) and fraud (Biegel, 2001; Ferrera et al., 2001).

In the recently released report from the OECD Task Force on Spam, Annex B lists “Cases Brought Under A Specific Anti-Spam Law”, and documents a case from the United States, FTC vs. Global Web Productions, brought under the CAN-SPAM Act. The defendants were charged regarding a fraudulent weight loss patch and anti-aging spray. The report noted that “The defendants reside in Australia and New Zealand, and Global Web is based in Australia” (OECD Directorate for Science Technology and Industry, 2005a). The report lists many other cases brought against spammers in a variety of countries, and notes any cross-border elements, where defendants were in another country.

In a BBC News item entitled “Sexual spam could spark lawsuits”, Dr Brian Bandey, a net law expert, reminded U.K. employers of their responsibility for providing a “safe working environment”, and

The obligation to oversee the welfare of workers extended to policing what reached the e-mail inboxes of workers and tackling sexual spam.... To avoid lawsuits for mental or emotional distress firms had to take all reasonable and practical steps to stop explicit spam....

(Ward, M., 2003)

In a letter to Guardian Unlimited, also in the U.K., Ed Macnair of IT Security vendor NetIQ warned that “...employers need to be aware they will be held responsible for stopping the sexually explicit and offensive spam entering the workplace.... Organisations that do not attempt to stop sexually explicit spam will be facing lawsuits from distressed employees.” (Macnair, 2003)

Employee lawsuits because of spam are also a fear of employers in the U.S.A., as noted in a Nucleus research report:

...productivity and IT impact are not the only concerns of administrators in managing spam. Many companies worry that even with filters, unsolicited e-mail sent to employees may provoke legal action:

According to one IT administrator, “One of the reasons we got into spam filtering is the offensive content lawsuits that could arise. We have to prevent work environment lawsuits.”

(Nucleus Research Inc., 2003)

Spam is also regarded as an invasion of privacy issue, and in the U.S. privacy is regarded as a fundamental “right to be left alone”.

Cannon (2005, p. 80) regards spam as a violation of this right to be left alone, stating that “Spam is considered an invasion of a right that is categorized as communication privacy”.

In New Zealand, many parties have lobbied parliament to enact anti-spam legislation, including the former Privacy Commissioner, Bruce Slane, who, in a letter to the Minister of Communications, stated “Spam can cause consumer protection problems... However, the particular reason that I add my voice to calls for effective responses to spam concerns information privacy. This typically involves using personal information provided for one purpose for another, the marketing purpose of spammers” (Slane, 2003).

New Zealand Judge David Harvey, quoting Lilian Edwards, states that “Spam is an invasion of the privacy of the individual...” (Harvey, 2003, p. 311), and further notes that “Spamming also has economic implications... Employers also suffer additional costs in that spam wastes employee time... spam threatens the efficiency and speed of the internet for all users... Potential civil liability for spam may exist in contract, tort, trademarks, and consumer protection law.” (Harvey, 2003, p. 312).

Under New Zealand law, remedies available for use against spammers include a claim for trespass to goods which could be made in the following situations:

- Spreading viruses;
- Using data robots; and
- Spamming.

(Simpson Grierson x-tech group, 2002, p. 243)

This may now have been superseded, however, with the recent introduction of the “Unsolicited Electronic Messages Act 2007”, which passed into law in February 2007, and comes into effect on September 5, 2007. Designed to prevent spammers operating in New Zealand, it also makes illegal the harvesting of addresses or even the use of harvested addresses, and applies not only to email, but also other forms of electronic messaging, and

is policed by the Department of Internal Affairs, who have setup a website at <http://www.spam.govt.nz> to provide businesses and individuals with information about the new requirements of the Act which states that “The Act defines spam as ‘unsolicited commercial electronic messages’” (The New Zealand Department of Internal Affairs, 2007)

With respect to the previously noted social impact caused by UBE to recipients in the form of stress, some reports and articles warn that employees might pursue legal action as a result of repeatedly receiving, for example, pornographic spam.

Based on overseas experiences, New Zealand organisations may need to consider that this type of UBE might result in a sexual harassment case by employees under the Employment Relations Act 2000, either against their employer, or even against another employee, as noted by Fitzsimons, who stated “Some recent complaints have included unwelcome exposure to internet sex, as when someone walks by another person’s computer and observes offensive materials.” (Fitzsimons, 2002).

New Zealand legislation that may apply, as in the previously mentioned warnings about lawsuits from U.K. and U.S. publications, is the Health and Safety in Employment Act. The 2003 edition of the New Zealand Employment Law Guide notes that: “Stress has also been identified as a hazard that employers must manage... It confirmed that employers have a duty to provide a working environment and management processes that will not cause employees undue stress.” (Rudman, 2003, p. 178).

2.5 Technical Impact of UBE

UBE has had a substantial impact in the development of technology designed to prevent it, much of it focusing on content filtering and sophisticated statistical detection techniques.

A recent paper on spam filtering states “The problem is popular enough that it has been the subject of a Data Mining Cup contest... Bayesian analysis has been very popular, but researchers have also used SVMs, decision trees, memory and case-based reasoning, rule learning and even genetic programming.” (Fawcett, 2003).

Other researchers have examined the effectiveness of spam filtering techniques (e.g. Le, Jingbo, & Tianshun, 2004), and there have also been contributions from New Zealand researchers with “An analysis of the tools used for the generation and prevention of spam” (Courmane & Hunt, 2004).

In addition, however, it is acknowledged that technical solutions to preventing UBE always come at a price, and that price includes a level of “false positives”, as noted by Harris, who stated,

Invariably any computer system that attempts to distinguish between spam and legitimate mail is going to be wrong some of the time... It is almost impossible to overemphasize how crucial the issue of false positives can be: for businesses, a single false positive may mean the loss of thousands of dollars in missed sales. For emergency services, it is conceivable that a false positive could even result in loss of life. (Harris, 2003, p. 22)

When considered in the light of the dangers presented by false positives, and compared with the losses faced by an organisation or the stress caused to employees, this places organisations in a “damned if you do, damned if you don’t” type of situation.

2.6 Organisational Best Practices to Minimise the Impact of UBE

The final area that is frequently found in the literature is that of best practice to avoid addresses being harvested and detecting and blocking UBE.

The practices that are typically found include technical solutions that can be implemented by the organisation, such as those mentioned in the previous Technical Impact section, and also education and awareness is of particular importance for both the organisation and its employees. Both parties play a role in how UBE can be minimised, because of the methods used to “harvest” email addresses, and in discouraging the spammers.

In the Siponen and Stucke (2006) study, the researchers examined a number of factors to try and determine the effectiveness of various anti-spam strategies in companies.

When asked which anti-spam techniques they would prefer to use as part of their future strategy, the majority favoured Filters (38%) and Blacklists (20%), while the least-favoured techniques were “Letting the users themselves delete spam messages manually” (6%) and “Complaining to the spammers” (4%) (Siponen & Stucke, 2006, p. 8).

A number of the study’s respondents indicated caution was necessary with the use of filters, due to the problem of sometimes filtering legitimate emails, which they said “occurs with international emails in particular”, and that “the balance between blocking spam and creating false positives is difficult to achieve” (Siponen & Stucke, 2006, p. 7).

In New Zealand, the Consumers’ Institute publish a helpful list of best practices for both individuals and organisations on their website, providing advice about:

- [**Eight ways to block spam**](#)
(Some techniques for fighting back)
- [**Six mistakes to avoid**](#)
(Don't try this at home!)
- [**How they find you**](#)
(How spammers get your email address)

(Consumers' Institute of New Zealand, 2007)

The website run by InternetNZ (<http://www.stopspam.net.nz>) contains information about spam relevant to the New Zealand context, and also includes best practices.

In particular, they provide best practice information on:

- [Reducing Spam](#)
- [Golden rules](#)
- [Technical](#)

For example, the page on “Reducing Spam” includes a section about “What can businesses do about spam?” which covers the organisations web server, mail server and employee education, noting for education specifically that “Teaching your staff how to handle spam is probably the most important, and yet under-rated thing you can do to reduce the effect it has on your organization.” (InternetNZ, 2006b).

The bottom line for how to stop UBE globally, as stated by a spammer them self, is “if you want to stop spam, don’t buy products from spam e-mails!” (Spammer-X, 2004, p. 10).

2.7 Summary

This chapter has highlighted four areas of impact that UBE has in relation to organisations and email users, and also some solutions and recommendations that have emerged as a response to the problem.

The chapter also highlights the limited amount of research that has been done in New Zealand surrounding the impact UBE has on organisations from an operational perspective, and that virtually no research has yet been done on the impact it has on employees.

The lack of knowledge in these areas provides the theoretical basis to build the methodological framework for this study, and placing it within a socio-economic context.

Chapter 3 - Research Design

3.1 Introduction

This chapter focuses on how the research design was developed, detailing why the specific methodological approach and methods were used that resulted in the research framework. It will also detail the various data collection design components, including the sampling design and the instruments used, particularly why and how the questions and special scales were developed to measure employees attitudes. The data collection methods used and the treatment and analyses of the resulting quantitative and qualitative data are also described.

3.2 Methodology

Comparative, Embedded Case Study Design

Using case study methodology, “the researcher explores in depth a program, an event, an activity, a process, or one or more individuals” (Creswell, 2003, p. 15), and is normally associated with a qualitative approach. It is particularly appropriate when asking “how” and “why” questions (Yin, 2003, p. 22).

When considering case study methodology, however, Yin (2003, p. 53) also strongly advises that a multiple-case study, even if only two-case, is much preferred over a single-case study, as the researcher must use replication logic, analogous to replicating experiments, producing evidence that is more “compelling”, and a more “robust” study overall (Yin, 2003, pp. 46-47). In a two-case study, the design employs literal (as opposed to theoretical) replication, and is used to predict similar results.

Further, Bryman states that multiple-case studies are a form of comparative design methodology, and that “in certain social science fields, like organization studies, this has become a common research design in its own right” (Bryman, 2004, p. 55).

When associated with a quantitative approach, Bryman describes its typical form as “Survey research in which there is a direct comparison between two or more cases...”, and

with a qualitative approach as including "...qualitative interview research on two or more cases" (Bryman, 2004, p. 56).

Yin describes the above forms as an "embedded" design, whereby "each individual case study may in fact include the collection and analysis of highly quantitative data, including the use of surveys within each case." (Yin, 2003, p. 53).

Typically, a comparative design seeks to highlight contrasts and differences between cases; however, the reverse is also true in that it can also highlight similarities between them.

Another important component of the research design is the unit of analysis. Yin (2003, p. 23) states that as a guide, the unit(s) of analysis are related to the research questions, and so there were two units of analysis embedded into the design: the organisation as an economic unit, and the employees as a "social" unit.

This research therefore used a comparative, two-case research design methodology as suggested by (Yin, 2003, pp. 52-53) and (Bryman, 2004, p. 56), incorporating an embedded survey, and using two embedded units of analysis (organisation, employees).

3.3 Methods

Mixed Methods Approach

A qualitative approach is normally associated with case study research, however, due to the use of an embedded design (survey) that is associated with quantitative methods, the resulting approach is therefore one of mixed methods. Additionally, in order to provide some triangulation with the quantitative results from the survey, interviews were incorporated, also resulting in a mixed methods approach. Creswell describes this type of mixed methods approach as a "concurrent nested strategy" that is appropriate when the researcher utilises "different methods to study different groups or levels. For example, if an organization is being studied, then employees could be studied quantitatively, managers

could be interviewed qualitatively, entire divisions could be analyzed with quantitative data, and so forth.” (Creswell, 2003, p. 218).

For this research design, data was obtained from multiple sources:

- Quantitative data from survey(s) (employee wage/salary costs, server/software costs, quantity of and time taken to delete spam emails)
- Qualitative data (employer and employee survey and interviews re: knowledge, beliefs, attitudes, behaviours about UBE)
- Secondary data (literature review)

3.4 Research Framework

The diagram in (Figure 2) below shows the resulting research framework based on (COSMOS Corporation, cited in Yin, 2003, p. 40), that was employed for this study:

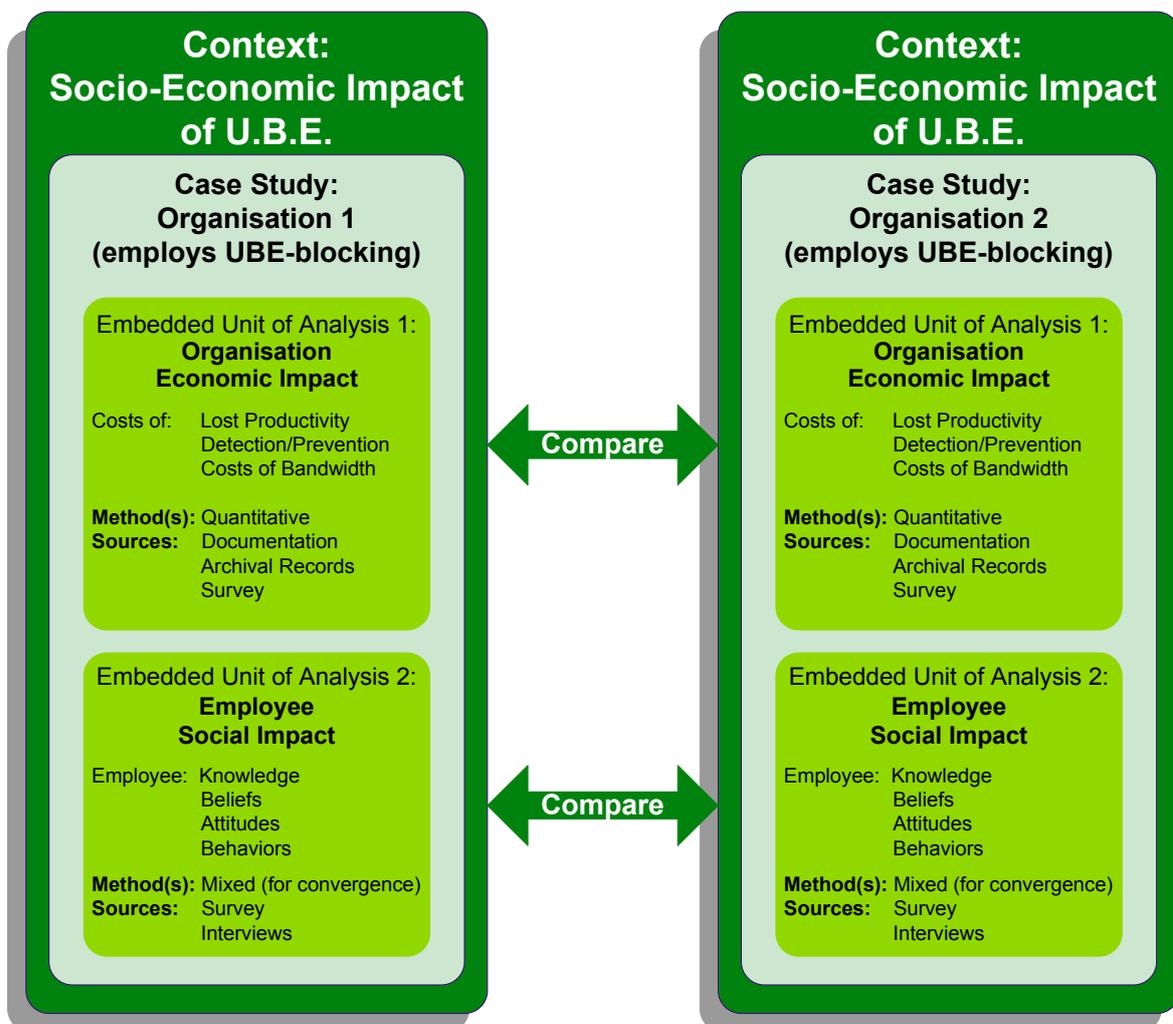


Figure 2. Research Framework for Comparative Case Studies using Replication

3.5 Data Collection Design

3.5.1 Sampling Design

3.5.1.1 Organisations

Selection of the organisations was done in cooperation with the Employers and Manufacturers Association (EMA) Northern, who have conducted security/spam surveys of their members for the past two years.

The sampling design used for organisation selection was a non-probabilistic judgement sample. Antonius (2003, p. 116) defines a judgement sample as resulting “from judgement that makes us believe that analysis of certain specific units is more likely to give us a better idea of the problem we are examining”.

For this research, an EMA Northern staff member was advised that the selection criteria for each organisation were that they were to be:

- Currently receiving spam
- Between 500-1,500 employees in size

The EMA Northern staff member then contacted a number of local companies, and found two that were receiving spam, within the size range, and willing to participate in the study. Each organisation was then contacted by the researcher, and after confirming willingness to participate, each sent a confirmation e-mail for ethics approval.

3.5.1.2 Survey Participants

The survey sampling design was a non-probabilistic sample of volunteers, which is defined by Antonius as being “composed of people who respond to a general appeal, without any selection.” (Antonius, 2003, p. 116). The IT Managers sent out several emails at intervals to all staff at their respective organisations, requesting participation in the survey, and providing the URL link to the survey website. The survey results are derived from people who responded to that appeal.

3.5.1.3 *Interview Participants*

Four participants from each organisation were chosen by their respective IT Manager to participate in a recorded interview.

The sampling used was again a judgement sample. The IT Managers were advised that the criteria for selection were that the participants must be receiving UBE, and that they should include male and female participants, ideally two of each gender. Any other selection criteria used by the IT Managers is unknown.

3.5.2 *Instruments*

Data was collected using the following survey instruments:

- Organisational questionnaires and archive data
- Online web-based employee survey
- Individual employee interviews

The survey instruments were critical for providing answers to the socio-economic research questions regarding the impact of UBE on organisations and employees. A considerable amount of time was therefore spent on designing questionnaire, survey and interview questions that would hopefully answer the research questions.

3.5.2.1 *Question Design*

When constructing the question content, de Vaus (1995, p. 81) citing (Dillman, 1978), states that there are “four distinct types of question content: behaviour, beliefs, attitudes and attributes”. Each question type is further defined as:

- Behaviour – what people *do*
 - Beliefs – what people *believe* is true or false
 - Attitudes – what people believe is *desirable*
 - Attributes – *characteristics* of the respondent (e.g. gender, ethnicity, salary)
- (de Vaus, 1995, p. 82)

A better approach, however, may be one suggested by Zikmund (2003) in his chapter on “Attitude Measurement”, where he defines attitude as “an enduring disposition to respond consistently in a given manner to various aspects of the world, including persons, events, and objects”. He further describes attitude as consisting of three components:

- Affective – person’s general feelings or emotions towards an object
- Cognitive – person’s awareness of and knowledge about an object
- Behavioural – person’s intentions and expectations, predisposition to action (Zikmund, 2003, p. 308)

Using Zikmund’s definition, it could be argued that two of de Vaus’s question types are actually sub-types of attitude measurement:

- Behaviour - Behavioural
- Beliefs - Cognitive

Re-defining de Vaus’s question types using Zikmund’s definition, it could be argued that there are only two distinct question types, one of which has several components:

Table 1

Question Type Model, based on (de Vaus, 1995) and (Zikmund, 2003)

Question Type	Component	Measurement
Attributes		person’s characteristics
Attitudes	<i>Affective</i>	person’s general feelings or emotions
	<i>Behavioural</i>	person’s actions or intended/expected actions
	<i>Cognitive</i>	person’s beliefs or knowledge

3.5.2.2 Organisational Questionnaires

The organisational questionnaires were in two parts, with the first part containing several attribute, cognitive and behavioural questions (what do they know or believe about the impact of UBE, and what do they do about it), and the second part requested only information used for the economic calculations.

Table 2***Question Design for Organisational Questionnaire, OQx.1 (RQ1, RQ2)***

Q.	Purpose	Type	Scale (MR = Multiple Responses)
1	UBE Knowledge	Cognitive	Open-ended, entered text
2	UBE Knowledge	Cognitive	Open-ended, entered text
3	UBE Behaviour	Behavioural	MR: Open-ended, entered text, two measures (useful, effective) using scale: Not at all <-> Extremely
4	UBE Behaviour	Attribute	Open-ended, entered text (expect Yes/No)
5	UBE Behaviour	Behavioural	MR: Open-ended, entered text
6	UBE Behaviour	Attribute	Open-ended, entered text (expect Yes/No +)
7	UBE Belief	Cognitive	MR: Open-ended, entered text
8	UBE Knowledge	Attribute	Open-ended, entered text (expect Yes/No)

The second part of the questionnaire (OQx.2) for each organisation's IT Departments was data required for the economic calculations (*RQ1*), and included employee information and costs, IT costs for hardware, software, Internet connection and administration (support) time for dealing with UBE.

Additional archive information was later requested from both organisations, regarding actual email and spam statistics, so that this could also be incorporated into the economic analysis for comparison.

The questionnaires and responses from each organisation can be found in Appendix A.

3.5.2.3 Online web-based employee survey

The employee survey consisted mostly of closed-ended questions using a variety of scales, including simple "yes/uncertain/no" choices, and Likert rating scales (e.g. ranging from "strongly agree" to "strongly disagree").

A special scale, derived from the Job Emotions Scale (JES) used in other studies (Ashkanasy, 2002; Grandey et al., 2002), was created to measure the affective component of respondents attitude towards the types of UBE they receive.

Table 3***Question Design for Web-based Employee Survey (RQ2, RQ3)***

Q.	Purpose	Type	Scale (MR = Multiple Responses)
1	Demographics	Attribute	Gender
2	Demographics	Attribute	Ethnicity
3	Demographics	Attribute	Salary/Wage range
4	Demographics	Attribute	Years, months
5	UBE Statistics	Attribute	Yes/Uncertain/No
6	UBE Statistics	Attribute	Yes/No
7-8	UBE Statistics	Attribute	Entered numeric variables
9	UBE Statistics	Attribute	Entered numeric variable
10	UBE Statistics	Attribute	a.) Entered numeric variable b) Hour/Day/Week/Month
11	UBE Statistics	Attribute	Likert 5-point: Less <-> More
12	UBE Belief	Cognitive	MR: Closed-ended, open-ended entered text
13	UBE Filters	Cognitive	Likert 5-point: Str. Agree <-> Str. Disagree
14	UBE Filters	Attribute	Yes/Uncertain/No
15	UBE Behaviour	Behavioural	Yes/Uncertain/No
16	UBE Behaviour	Behavioural	Yes/Uncertain/No
17	UBE Behaviour	Behavioural	Entered text
18	UBE Behaviour	Behavioural	Yes/Uncertain/No
19	UBE Behaviour	Behavioural	Entered text
20	UBE Behaviour	Behavioural	Yes/Uncertain/No
21	UBE Behaviour	Attribute	Yes/Uncertain/No
22	UBE Behaviour	Behavioural	Yes/Uncertain/No
23	UBE Emotions	Affective	MR: JES (modified)
24	UBE Emotions	Affective	MR: JES (modified)
25	UBE Attitudes	All Attitude	Likert 5-point: Str. Agree <-> Str. Disagree
-	Final Comments	All Attitude	Entered text

The questions about respondent's reactions to different spam types, which used the JES scale modified for this study, allowed for multiple responses i.e. mixed emotions by the respondent, but included a "Don't Care" option, intended originally to override any other

selections the respondents might make. However, it became obvious from both the results, and the comments of interview participants, that many believed that mixed emotions could, in fact *include* a “Don’t Care” attitude towards spam, in combination with the other emotional responses such as anger and frustration.

As a result, the analysis did not try to eliminate the other responses when the “Don’t Care” option was chosen, which also helped simplify the analysis.

Once the questions had been decided, a web-based survey questionnaire was developed using Apian SurveyPro 3.0i (a professional survey package owned by the Unitec School of Management) with the NetCollect plug-in. To prevent unauthorised entry to the survey, but also to enable identification of which organisation survey respondents were from, two security PIN numbers were also enabled in SurveyPro, and the respective PIN number included with the email sent to staff at each organisation.

To ensure the informed consent of all participants, the initial login page also included statements of the purpose of the research and that the survey was both voluntary, anonymous, and secure (via https://). Also included on the login page was a link to an additional page which provided the participants with a definition of spam for the purposes of the survey. This definition was also sent with the email to staff.

The full survey (see Appendix C) was submitted to the Unitec Research Ethics Committee (UREC), but some questions were later changed, requiring UREC approval again.

A Linux server was then installed and setup to host the completed HTML survey pages and the PERL scripts required by SurveyPro for the survey to run.

An SSL certificate was also purchased for 12 months from Comodo and installed on the server, and the complete survey was then made available via the Internet with the URL:

<https://surveys.unitec.ac.nz/spam> .

The survey was piloted first by the researcher, the researcher's supervisor, and the IT Manager from organisation 1, to discover any issues with use of, or responses to, the online survey and questions, and to determine an average time taken to complete the survey (10-15 minutes).

The IT managers at each organisation sent out a succession of emails to all employees, requesting them to participate in the survey, as per the sampling design.

3.5.2.4 Individual Employee Interviews

To provide some triangulation of information and gain any additional insights to answer *RQ2* and *RQ3*, semi-structured interviews were conducted, with four participants (employees) from each organisation who are currently receiving spam, using open questions to determine various attributes and attitudes towards the UBE they receive and how their organisation responds to it.

The interview questions were not piloted first to discover any issues with the questions or responses.

Each participant was e-mailed a copy of the "Invitation to Participate" and "Interview Consent" forms to read prior to the interviews, and before commencing each interview, confirmation was obtained that they understood the nature of the research and the purpose of the interview, and the consent form was then signed by the participant and researcher.

Samples of each form, as approved by UREC, are included in Appendix D.

Each interview was recorded on an Olympus WS-100 digital voice recorder, and the resulting file transferred to a PC, labelled (e.g. Org1_Interview1.WMA), then transcribed to a MS Word .DOC file of the same name (e.g. Org1_Interview1.DOC).

3.6 Data Analysis

3.6.1 Quantitative Data

3.6.1.1 Employee Survey Socio-economic Data

Software packages used during the conversion and analysis phases were:

- Microsoft Office Access 2003 SP2
- SPSS for Windows v14.0.0

Phase 1 – SurveyPro Cleanup and Export

SurveyPro uses its own database system, and creates a NetCollect database file (.SDH) for each page of the web survey, so the eight .SDH database files were batch imported into SurveyPro, which included error-checks as it matched questions with answers.

Of the records (forms) in the imported data table, 10 were deleted initially, as 8 records showed initial login only before exiting, 1 record was a test record, and 1 record seemed to be a deliberately bogus entry (ethnicity was “Droid” and answers to other questions were clearly meant to be a joke).

The resulting survey data was exported from SurveyPro to an MS Access database using the following options:

- Multiple response checkbox answers exported as separate fields
- Checkbox answers exported as indexes starting from 1

This resulted in the database field names labelled as question numbers, for example:

Q003, Q003O – Question 3, and Question 3 “Other” option

Q15M001, Q15M002 – Question 15/Checkbox 1, Question 15/Checkbox 2 etc.

Phase 2 – SPSS Import, Data Editing and Coding

The Access database was imported into SPSS, and the original SurveyPro field names were edited to match the actual question numbers, as, for example, the PIN login field was labelled Q001, and the survey Q1 was named Q002 etc. At this point, the Q001 PIN login field, which indicated which organisation the respondent was from, was renamed “org”, and the survey data was edited, replacing each organisation’s PIN number with 1 and 2 respectively, and the “org” variable values changed to reflect this (1=“Org1”, 2=“Org2”). Remaining variables values were then also coded according to the values used in the survey (e.g. for gender, 1=“Male”, 2=“Female” etc).

During this process, it was found that for Q2 (ethnic group), five respondents entered “New Zealander” in the “Other” category, so a new code value was created for these cases, 6=“New Zealander”, and their records were edited and replaced with this code.

Phase 3 – Compute New Variables

Several questions required more than one variable to be entered, which were:

- Q4 Experience using email – Years, Months
- Q7-8 Spam emails received (Q7), over a number of days (Q8)
- Q10 Deleting spam emails (Q10a) times per Hour/Day/Week/Month (Q10b)

Two of these (Q4 & Q7-8) required a new, computed variable to be created so the data could be analysed, so the following new variables were computed with the formula shown:

email_experience = $\text{SUM}(\text{email_years},0) + (\text{SUM}(\text{email_months},0) / 12)$

spam_perday = $\text{SUM}(\text{spam_in},0) / \text{SUM}(\text{spam_days},0)$

Also, as these new variables were scale variables, they required grouping into “bands”, similar to the salary/wage data, so the results could be analysed in tables, so SPSS’s

Transorm/Visual Bander function was used to create the following new variables:

email_experience_banded 24 bands (in years): <1.0, 1.0-1.9 ... 22.0-22.9, 23.0+

spam_perday_banded 91 bands: <1.00, 1.00-1.99 ... 89.00-89.00, 90.00+

For Q10, there were only two responses for the “times per hour” entry (1 and 2 times per hour respectively), so these were changed to “times per day” instead (8 and 15 times per day respectively, as organisation 1 used a 7.5 hour day).

Phase 4 – Define Multiple Response Sets

Three of the questions used multiple response checkboxes: Q12, Q23a-m and Q24.

During the export from SurveyPro (phase 1), each of the checkboxes in these questions became a variable with a dichotomous value, either zero for unchecked (not counted) or one for checked (counted), so before analysis, each question required defining an SPSS Multiple Response Set containing all of the checkbox variables for each question.

In total, 15 multiple response sets were created.

Phase 5 - Descriptive Analysis

Zikmund (2003, p. 473) states that “Descriptive analysis refers to the transformation of raw data into a form that will make them easy to understand and interpret. . . . Calculating averages, frequency distributions, and percentage distributions are the most common ways of summarizing data.”

To answer the research questions, the results from each organisation need to be presented in a simple, common format that allows easy comparison.

For this reason, percentage cross-tabulation is the primary method of presentation for the results, because “When data from a survey are cross-tabulated, percentages help the researcher understand the nature of the relationship by allowing relative comparison.”

(Zikmund, 2003, p. 477).

To meet the requirements of the comparative research framework, which will answer the research questions about the organisation and any gender differences, the basic cross-tabulation needs to be further refined into another level of subgroup, resulting in three

variables (the dependent, organisation, and gender), which, according to Zikmund (2003, p. 478), is a form of elaboration analysis.

Percentages shown in the results (male, female, and total) are calculated by SPSS using the valid responses of their respective organisations (cases) as the base, presented side-by-side in columns, for direct organisational comparison, as required by the framework.

Statistical terms and abbreviations used in his study:

N	The number of <i>valid</i> responses in each case
Nr	The number of <i>valid</i> responses in a multiple-response question
%	The proportion of people in each case that gave a <i>valid</i> response
Outlier	An extreme value
Mean	The arithmetic mean, or average
5% Trimmed Mean	The arithmetic mean after excluding the 5% lowest and 5% highest values, making the mean less sensitive to outliers
Median	The middle value after sorting all values from smallest to largest
Mode	The most frequently occurring value in the data

“Don’t Care” inclusive with other multiple-response selections

Of special note for the Job Emotion Scale (JES) results, was that originally it was intended that should a survey respondent or interview participant select “Don’t Care” as a response, this would then exclude other multiple-response selections for that question item.

However, during examination of the survey results, and also during discussion with some of the interview participants, it became clear that some people felt that selecting both “Don’t Care” AND other responses (e.g. “Frustrated”, “Angry”) were perfectly valid in their minds, therefore the resulting analyses included ALL responses, even if “Don’t Care” was one of the selections.

3.6.1.2 Economic Data

The economic data from the organisational questionnaire and archival records was combined with the UBE statistics (average number of spam emails per day, average time to delete a spam) and entered into a spreadsheet spam cost analysis model originally developed by Mark Gibbs in Network World (Gibbs, 2003b).

3.6.2 Qualitative Data – Thematic Analysis

All qualitative text data from survey respondents and interview participants was manually analysed for themes that emerged, grouped for frequency counts where appropriate, and then interpreted and compared.

3.7 Follow-up Discussions

After the cost analysis, some unexpected results emerged, and it was necessary to contact the IT Manager at each organisation to clarify and confirm organisational information provided, and discuss the results of the analysis.

A meeting to discuss the results and possible recommendations for best practice was also held with a representative of Marshal Software NZ, as both organisations are using their anti-spam software.

3.8 Ethics Issues

The web-based survey was anonymous, with no personally identifying information entered, neither was any attempt made to record the source IP address of the respondent. No ethnic group was specifically targeted by this research, but one question did request the ethnic group the respondent identified with.

Several employees were directly interviewed; therefore every effort was made to ensure anonymity of these participants, and no personal details other than gender were recorded. The raw data obtained from the survey and interviews will be kept archived on DVD, in a secure location known by the Unitec Postgraduate Division and accessible only by this researcher and supervisors, for a period of five (5) years post-study.

3.9 Summary

This chapter has described in detail the choices of methodology and methods used in this study, and provided a research framework for the theoretical underpinnings.

The researcher has supported the choices used, particularly in the design of the survey instruments' questions and scales used, and discussed an issue that arose with the use of this that required modifying the statistical analysis.

The sampling methods, univariate statistical analysis methods, thematic analysis and the use of a previously developed spam cost analysis spreadsheet model were discussed, and also the necessity of post-analysis follow-up discussions with both the organisations and one of the anti-spam vendors as a result of the findings.

Chapter 4 - Results and Descriptive Analysis

4.1 Introduction

This chapter presents the results of the quantitative and qualitative methods used in the study. A descriptive analysis or interpretation accompanies the numerous tables resulting from the statistical and thematic analyses from the survey and interviews, and the economic calculations are based on a modified spreadsheet model. These results provide the basis for further discussion and inferential analysis in the following chapter.

Each section title or table title includes, in parentheses following it, the relevant research question(s) (RQ1, RQ2 or RQ3) that link(s) to it.

A table linking the methods used, analysis performed, research question(s) and section reference can be found in section 4.3.

4.2 Organisation Backgrounds

The background of each organisation assists in explaining the impact UBE has on each organisation by placing it within the organisational context.

The backgrounds provided here are based on the organisational questionnaire results which can be found in Appendix A, and discussions both pre and post-analysis of the results.

4.2.1 Organisation 1 Background

Organisation 1 is part of a multi-national company, based primarily in the Auckland CBD, with three divisions and 1,200 local staff with 1,000 email accounts, located at 26 sites across New Zealand at most major cities, ranging from 500 staff in Auckland and 200 staff in Wellington to (for example) 5 staff in Levin.

Economic costs are based on *7.5 hours/day*.

They have been using MailMarshal since September 2000, and were running v6.14.441, released about mid 2006, at the time of the study. They added a Barracuda Spamware appliance as the first layer of defence two years ago, in mid 2005, running v3.4.10.102. The two layers of anti-spam systems are configured to use one Real-time Block List (RBL) on the Barracuda appliance, the Spamhaus SBL-XBL list, as recommended by Barracuda. The systems are configured to block positively identified spam, but tag and pass through to the recipient emails that had high scores and so were possible spam, but could not be positively identified by the systems. They consider the combined anti-spam systems to be very effective at blocking most spam.

The IT department considers spam to be a moderate problem, and uses several policies, processes and techniques to try and control it.

Besides the above-mentioned technical solutions, they also provide a “Public Folder” for staff to forward missed spam to, which they find to be also very effective, and send out occasional email reminders about spam, and have a policy statement on their Intranet.

Their “Acceptable Use” (email) policy covers netiquette only, however, and is not specifically for spam, and they do not currently cover spam as a topic during staff induction or training.

They regard the main reasons employees are being spammed to be because of email addresses on their own (public) website, and because employees leave email addresses on other websites when subscribing etc.

4.2.2 Organisation 2 Background

Organisation 2 was originally two multi-national sister companies based in South Auckland, with about 500 local staff, and about 210 email accounts. In December 2005 the companies were sold to two different owners, and their domain names were changed at

this time due to the business ownership change, but they retained their joint IT department and IT infrastructure. Economic cost is based on *8.0 hours/day*.

Organisation 2 has been using MailMarshal since the beginning of 2001, and was using v5.5.7 (over three years old) at the time the study was conducted. Immediately following the domain name changes in 2005, spam levels dropped to virtually zero for a time.

The system is configured to use the Spamhaus RBL, as recommended by MailMarshal, but all emails detected as spam are quarantined, and original recipients are sent an individual email notification for every email that is quarantined.

Emails destined for invalid recipient names are dropped, but no notification is given to the sender to prevent directory harvesting attacks.

Recipients of the quarantine notification emails must check each email and determine if it looks like spam, then request it to be released if it is not.

IT staff proactively check through the quarantine folders also, checking for legitimate emails, releasing them if they are, and adding them to a “whitelist” that is their approved business list of specific email addresses and domains.

Due to the huge worldwide increase of image spam in 2006, organisation 2 found that much of this was passing undetected through their anti-spam system, and resorted to using custom filters to try and identify specific features they found in the spam.

This practice has continued up to the present, but is now found to be creating problems of its own; as the rate of false-positives has increased as a result of the ratings given to specific words they have found to be common in the missed spam.

Spam within organisation 2 is considered a significant problem, and all management, the Human Resources department and the IT department are aware of it.

They also use a number of policies, processes and techniques, which overall they believe to be only somewhat effective in controlling spam, including the previously mentioned

MailMarshal, Anti-virus scanning on the server and clients, Microsoft Outlook “Harmful Attachment Protection”, and their SMTP configuration.

They do have an Acceptable Use, or Email Policy, which advises employees that they monitor and intercept spam emails, and that employees should not reply to it. This policy is not currently part of any staff induction or other training, however.

They regard the main reasons employees are being spammed to be because they leave their email addresses on public websites while engaging in Internet shopping, discussion groups and other website logons, and also as a result of their address being forwarded to harvesters through malicious software (trojans/viruses) that infect the computers of friends and associates who have their addresses in their contacts lists.

4.3 Results Question Map

The following table provides a summary of the mapping between the research method, data source, results table(s), data analysis method(s) and the relevant research question(s) answered by each table.

Table 4

Research Method/Question/Results Table map

Research Method	Data Source	Results Table(s)	Data Analysis Performed	Relevant Research Question(s)	Section
Quantitative	SQ1, SQ2	5	Univariate	RQ2, RQ3	4.4
Quantitative	SQ3	6	Univariate	RQ1	4.4
Quantitative	SQ4	7	Univariate	RQ2, RQ3	4.4
Quantitative	SQ5	8	Univariate	RQ1, RQ2, RQ3	4.4
Quantitative	SQ6	9	Univariate	RQ1, RQ2, RQ3	4.4
Quantitative	SQ7, SQ8	10, 11	Univariate	RQ1, RQ2	4.4
Quantitative	SQ9	12, 13	Univariate	RQ1	4.4
Quantitative	SQ10a,b	14	Univariate	RQ1, RQ2	4.4
Quantitative	SQ11	15	Univariate	RQ1	4.4
Mixed	SQ12	16 - 19	Univariate, Content	RQ2	4.4
Quantitative	SQ13a-d	20 - 23	Univariate	RQ1, RQ2, RQ3	4.4
Quantitative	SQ14	24	Univariate	RQ1, RQ2	4.4
Quantitative	SQ15	25	Univariate	RQ1, RQ2	4.4
Quantitative	SQ16	26	Univariate	RQ1, RQ2	4.4
Mixed	SQ17	27 - 29	Content, Univariate	RQ1, RQ2	4.4
Quantitative	SQ18	30	Univariate	RQ2, RQ3	4.4
Qualitative	SQ19	31	Content	RQ2	4.4
Quantitative	SQ20	32	Univariate	RQ2, RQ3	4.4
Quantitative	SQ21	33	Univariate	RQ2, RQ3	4.4
Quantitative	SQ22	34	Univariate	RQ2, RQ3	4.4
Quantitative	SQ23a-m	35 - 47	Univariate	RQ2, RQ3	4.4
Quantitative	SQ24	48	Univariate	RQ2, RQ3	4.4
Quantitative	SQ25a-s	49 - 67	Univariate	RQ2, RQ3	4.4
Qualitative	SFC	68 - 70	Content	RQ2	4.4
Mixed	IQ1	71 - 76	Content, Univariate	RQ2	4.5
Mixed	IQ2	77, 78	Univariate	RQ2	4.5
Mixed	IQ3	79, 80	Univariate, Content	RQ2	4.5
Mixed	IQ4	81 - 84	Univariate, Content	RQ2	4.5
Mixed	IQ5	85 - 90	Content, Univariate	RQ2	4.5
Quantitative	OQx.2	91 - 93	Univariate	RQ1	4.6

Note 1. SQx = Survey Question x, SFC = Survey Final Comments, IQx = Interview Question, OQx.2 = Organisational Questionnaire part 2

4.4 Survey Socio-Economic Results and Descriptive Analysis

Table 5

Gender/Ethnicity (RQ2, RQ3)

	Org1 (N=129)			Org2 (N=45)		
	Male	Female	Total	Male	Female	Total
	%	%	%	%	%	%
NZ European	38.8	47.3	86.0	33.3	33.3	66.7
NZ Maori	.0	3.9	3.9	8.9	2.2	11.1
Pacific Islander	.0	.8	.8	.0	11.1	11.1
Asian	.0	1.6	1.6	4.4	.0	4.4
New Zealander	1.6	.8	2.3	2.2	2.2	4.4
Other	3.1	1.6	4.7	2.2	.0	2.2
Prefer not to say	.8	.0	.8	.0	.0	.0
Total	44.2	55.8	100.0	51.1	48.9	100.0

Gender/Ethnicity

In organisation 1, more than half of the respondents (55.8%) were female, and in organisation 2, slightly more than half of the respondents (51.1%) were male.

In both organisations, a clear majority of respondents (86% and 67% respectively) identified their ethnicity as NZ European.

In organisation 1, small numbers of respondents identified with other ethnic groups, but in organisation 2, one in five respondents (22.2%) identified as either Maori or Pacific Islander.

The ethnic bias towards NZ European, and the higher numbers of Maori/Pacific Island respondents in organisation 2, may be dependent on a number of factors, including:

- The nature of the organisations' business
- The location of the business (organisation 1 – Auckland CBD primarily, organisation 2 – Manukau)
- Disinclination to participate in the online survey (between 9-15% from each organisation participated)

Table 6***Wage/Salary Range (RQ1)***

	Org1 (N=129)			Org2 (N=45)		
	Male	Female	Total	Male	Female	Total
	%	%	%	%	%	%
\$0 - \$9,999	.0	.0	.0	.0	.0	.0
\$10,000 - \$19,999	.8	2.3	3.1	.0	2.2	2.2
\$20,000 - \$29,999	4.7	7.0	11.6	2.2	4.4	6.7
\$30,000 - \$39,999	7.8	10.9	18.6	2.2	13.3	15.6
\$40,000 - \$49,999	9.3	10.9	20.2	11.1	17.8	28.9
\$50,000 - \$59,999	7.0	5.4	12.4	8.9	8.9	17.8
\$60,000 - \$69,999	1.6	3.1	4.7	8.9	.0	8.9
\$70,000 - \$79,999	2.3	1.6	3.9	11.1	2.2	13.3
\$80,000 - \$89,999	3.1	7.0	10.1	.0	.0	.0
\$90,000 - \$99,999	.0	1.6	1.6	.0	.0	.0
\$100,000+	7.8	6.2	14.0	6.7	.0	6.7
Total	44.2	55.8	100.0	51.1	48.9	100.0
Mean	\$51,400			\$48,000		
5% Trimmed Mean	\$50,800			\$46,900		

Wage/Salary Range

For both organisations, the majority (53.5% and 53.4% respectively) earned less than \$50,000 pa, and a clear majority (66% and 71% respectively) earned less than \$60,000 pa. In organisation 1, however, one in four respondents (25.7%) earned more than \$80,000 pa. For organisation 1 the IT/HR supplied average employee cost (\$55,000 pa) was about 7% higher than the SPSS calculated mean of the respondents (\$51,400), but is consistent with the range of \$50,000-\$59,999. For organisation 2, the IT/HR supplied average employee cost (\$41,000 pa) was about 15% lower than the SPSS calculated mean of the respondents (\$48,000 pa), but is also consistent with the range of \$40,000-\$49,999.

Table 7***Experience Using Email (years) (RQ2, RQ3)***

	Org1 (N=129)			Org2 (N=45)		
	Male	Female	Total	Male	Female	Total
	%	%	%	%	%	%
<1.0	.0	3.1	3.1	.0	2.2	2.2
1.0 - 1.9	.8	.8	1.6	.0	.0	.0
2.0 - 2.9	.0	.8	.8	4.4	2.2	6.7
3.0 - 3.9	1.6	1.6	3.1	4.4	6.7	11.1
4.0 - 4.9	1.6	.8	2.3	.0	.0	.0
5.0 - 5.9	4.7	9.3	14.0	4.4	6.7	11.1
6.0 - 6.9	3.1	4.7	7.8	6.7	2.2	8.9
7.0 - 7.9	1.6	7.8	9.3	4.4	4.4	8.9
8.0 - 8.9	7.0	8.5	15.5	6.7	.0	6.7
9.0 - 9.9	6.2	1.6	7.8	4.4	2.2	6.7
10.0 - 10.9	12.4	12.4	24.8	2.2	6.7	8.9
11.0 - 11.9	.0	.8	.8	.0	2.2	2.2
12.0 - 12.9	.8	.0	.8	2.2	.0	2.2
13.0 - 13.9	2.3	.8	3.1	.0	2.2	2.2
14.0 - 14.9	.0	.0	.0	2.2	.0	2.2
15.0 - 15.9	.8	2.3	3.1	2.2	8.9	11.1
16.0 - 16.9	.8	.8	1.6	.0	.0	.0
17.0 - 17.9	.0	.0	.0	.0	.0	.0
18.0 - 18.9	.0	.0	.0	2.2	.0	2.2
19.0 - 19.9	.0	.0	.0	.0	.0	.0
20.0 - 20.9	.8	.0	.8	4.4	2.2	6.7
21.0+	.0	.0	.0	.0	.0	.0
Total	44.2	55.8	100.0	51.1	48.9	100.0

Experience using email

For both organisations, the majority of respondents (57.5% and 55.6% respectively) had less than nine years experience using email, and a significant majority (90% and 71% respectively) had less than 11 years experience.

Table 8***Have Ever Received Any Spam Emails in Work Account (RQ1, RQ2, RQ3)***

	Org1 (N=127)			Org2 (N=45)		
	Male	Female	Total	Male	Female	Total
	%	%	%	%	%	%
Yes	35.4	49.6	85.0	42.2	40.0	82.2
Uncertain	.8	2.4	3.1	2.2	.0	2.2
No	7.9	3.9	11.8	6.7	8.9	15.6
Total	44.1	55.9	100.0	51.1	48.9	100.0

Table 9***Have Received Spam Email in the Past Two Weeks (RQ1, RQ2, RQ3)***

	Org1 (N=127)			Org2 (N=45)		
	Male	Female	Total	Male	Female	Total
	%	%	%	%	%	%
Yes	34.6	45.7	80.3	35.6	33.3	68.9
No	9.4	10.2	19.7	15.6	15.6	31.1
Total	44.1	55.9	100.0	51.1	48.9	100.0

Spam email received by respondents

For both organisations, a clear four-fifths majority of respondents (85% and 82% respectively) indicated they had at some time received spam in their work email accounts.

A clear majority of respondents from both organisations (80% and 69% respectively) further indicated that they had received spam in the past two weeks approximately.

There were no significant gender differences in either organisation.

The probable reason for there being fewer respondents in organisation 2 having received spam in the last two weeks compared to having ever received it is because of their domain name change, as spam levels had dropped for a while to almost zero, so some email accounts with the new domain name had not yet been “discovered” again by spammers.

Table 10***Spam email Received (per day) (RQ1, RQ2)***

	Org1 (N=86)			Org2 (N=31)		
	Male	Female	Total	Male	Female	Total
	%	%	%	%	%	%
<1.00	7.0	15.1	22.1	25.8	16.1	41.9
1.00 - 1.99	9.3	9.3	18.6	3.2	3.2	6.5
2.00 - 2.99	4.7	11.6	16.3	6.5	.0	6.5
3.00 - 3.99	7.0	2.3	9.3	.0	3.2	3.2
4.00 - 4.99	5.8	1.2	7.0	.0	.0	.0
5.00 - 5.99	4.7	3.5	8.1	6.5	3.2	9.7
6.00 - 6.99	1.2	2.3	3.5	3.2	3.2	6.5
7.00 - 7.99	2.3	2.3	4.7	.0	.0	.0
8.00 - 8.99	1.2	.0	1.2	.0	3.2	3.2
9.00 - 9.99	.0	.0	.0	.0	.0	.0
10.00 - 10.99	1.2	4.7	5.8	3.2	3.2	6.5
11.00 - 11.99	.0	.0	.0	.0	.0	.0
12.00 - 12.99	1.2	.0	1.2	.0	.0	.0
13.00 - 13.99	.0	.0	.0	.0	3.2	3.2
14.00 - 15.99*	.0	.0	.0	.0	.0	.0
16.00 - 16.99	1.2	.0	1.2	.0	.0	.0
17.00 - 20.99*	.0	.0	.0	.0	.0	.0
21.00 - 21.99	.0	.0	.0	.0	3.2	3.2
22.00 - 34.99*	.0	.0	.0	.0	.0	.0
35.00 - 35.99	.0	1.2	1.2	.0	.0	.0
36.00 - 43.99*	.0	.0	.0	.0	.0	.0
44.00 - 44.99	.0	.0	.0	.0	3.2	3.2
45.00 - 54.99*	.0	.0	.0	.0	.0	.0
55.00 - 55.99	.0	.0	.0	3.2	.0	3.2
56.00 - 85.99*	.0	.0	.0	.0	.0	.0
86.00 - 86.99	.0	.0	.0	.0	3.2	3.2
87.00+	.0	.0	.0	.0	.0	.0
Total	46.5	53.5	100.0	51.6	48.4	100.0

(* Ranges of zeros combined to reduce table length)

Table 11***Descriptive statistics for: Spam email received (per day) (RQ1, RQ2)***

		Statistic		Std. Error	
		Org1 (N=87)	Org2 (N=32)	Org1 (N=87)	Org2 (N=32)
Mean		3.8	9.5	.5	3.3
95% Confidence Interval for Mean	Lower Bound	2.8	2.7		
	Upper Bound	4.8	16.2		
5% Trimmed Mean		3.2	6.4		
Median		2.7	2.5		
Minimum		.1	.1		
Maximum		35.0	86.4		
Skewness		4.1	3.1	.3	.4
Kurtosis		24.3	9.9	.5	.8

Spam emails received per day

For both organisations, the majority of respondents (57% and 54.9% respectively) are receiving less than three spam emails per day.

For respondents receiving less than one spam email per day, there was a significant difference between organisations (22.1% and 41.9% respectively).

As the number of spam emails per day increased to 10.00-10.99 per day, the percentage of respondents receiving spam in organisation 1 declined almost uniformly.

For organisation 2, after the initial 41.9% receiving less than one spam email per day, the number received by respondents became intermittent (e.g. no one received 4.00-4.99), but remained generally the same (about 6.5%, or 2 respondents) up to 10 spam emails per day.

Of those receiving 11 or more spam emails per day, 3 respondents (2 male, 1 female) were from organisation 1 and received about 12, 16 and 35 spam emails per day respectively.

From organisation 2, there were 5 respondents (1 male, 4 female), who received about 13, 21, 44, 55 and 86 spam emails per day respectively.

Table 12***Time to Identify and Delete One Spam Email (RQ1)***

Seconds	Org1 (N=89)			Org2 (N=31)		
	Male	Female	Total	Male	Female	Total
	%	%	%	%	%	%
1	4.5	1.1	5.6	.0	.0	.0
2	10.1	15.7	25.8	3.2	12.9	16.1
3	6.7	6.7	13.5	6.5	9.7	16.1
4	2.2	2.2	4.5	.0	.0	.0
5	10.1	19.1	29.2	35.5	16.1	51.6
6	1.1	.0	1.1	.0	3.2	3.2
7	.0	1.1	1.1	.0	.0	.0
8	1.1	.0	1.1	.0	.0	.0
10	7.9	4.5	12.4	6.5	3.2	9.7
15	1.1	2.2	3.4	.0	.0	.0
20	1.1	.0	1.1	.0	.0	.0
30	.0	1.1	1.1	.0	3.2	3.2
Total	46.1	53.9	100.0	51.6	48.4	100.0

Most respondents believe they can identify and delete a spam email within 5 seconds

For both organisations, a clear majority of respondents (78.6% and 83.8% respectively) believe that they can identify and delete a single spam email in 5 seconds or less.

There were a total of 6 respondents (5 from Org1 and 1 from Org2) who believed it took them more than 10 seconds on average to identify and delete a single spam email.

Further, there were 2 respondents, 1 from each organisation, who believed it took 30 seconds to identify and delete a single spam email.

These values seem to be rather extreme; especially considering the 2 respondents who entered 30 seconds also claimed their number of years experience using email to be 7 years and 20 years respectively.

Table 13

Descriptive Statistics for: Time to Identify and Delete One Spam Email (Seconds, all Respondents) (RQ1)

Statistic				Std. Error			
		Org1	Org2	Total	Org1	Org2	Total
Mean		5.13	5.66	5.27	.471	.885	.417
95% Confidence Interval for Mean	Lower Bound	4.20	3.85	4.45			
	Upper Bound	6.07	7.46	6.10			
5% Trimmed Mean		4.57	4.92	4.64			
Median		4.50	5.00	5.00			
Variance		20.004	25.072	21.191			
Skewness		2.781	3.950	3.121	.254	.414	.219
Kurtosis		11.008	18.722	13.071	.503	.809	.435

Average time to identify and delete one spam email

For the purposes of the economic calculations, there is a need to determine the average time it takes to identify that an email is actually spam, and then delete it.

From the descriptive statistics table above, it can be seen that the mean time taken when both organisations were combined, was 5.27 seconds, however, as just discussed, there were six extreme outliers that will have skewed the mean, as can be seen by the positive skew value of 3.121, and in such cases, the median is a better indicator of the average value than the mean.

The highly positive kurtosis value also indicates that the majority of responses are clustered around a central value, and as the median is 5 seconds, this is therefore the value that will be used in economic calculations. Although there may be some bias towards this value, as it was used as an example value on the survey page, sufficient numbers of respondents have chosen values less than or greater than this to justify using this as the average time.

Table 14***Frequency of deleting Spam Email (RQ1, RQ2)***

		Org1 (N=87)			Org2 (N=31)		
		Times per			Times per		
		Day %	Week %	Month %	Day %	Week %	Month %
Spam emails are deleted	1	16.1	0	1.1	16.1	3.2	3.2
	2	25.3	1.1	1.1	16.1	9.7	0
	3	21.8	5.7	1.1	9.7	3.2	0
	4	8.0	2.3	0	3.2	3.2	0
	5	6.9	0	0	9.7	6.5	0
	6	0	0	0	3.2	0	0
	7	0	1.1	0	0	0	0
	8	2.3	0	0	3.2	0	0
	10	0	0	0	3.2	0	0
	12	1.1	0	0	0	0	0
	15	1.1	1.1	0	3.2	0	0
	20	0	0	0	3.2	0	0
	25	0	1.1	0	0	0	0
	30	1.1	0	0	0	0	0
Total		83.9	12.6	3.4	71.0	25.8	3.2

Most respondents delete emails daily

For both organisations, a clear majority of respondents (83.9% and 71% respectively) are deleting spam on a daily basis. For both organisations also, a majority of respondents (78.2% and 54.8% respectively) are deleting spam up to five times a day, which suggests *spam is a frequent distraction and time waster* for employees in both organisations.

There were several extreme cases in each organisation, with 1 respondent from organisation 1 claiming to be deleting 30 times per day, when they were receiving about 17 spam emails per day on average, and another respondent from organisation 1 selected two times per *hour* (converted to 15 times per day), when they received only 10 spam emails in 7 days, suggesting this may be a mistake, and should have been two times per *week*.

Table 15***Do You Believe You Are Receiving Less or More Spam Now Than a Year Ago? (RQ1)***

	Org1 (N=88)			Org2 (N=31)		
	Male	Female	Total	Male	Female	Total
	%	%	%	%	%	%
Less	4.5	3.4	8.0	22.6	16.1	38.7
Somewhat Less	3.4	3.4	6.8	6.5	.0	6.5
About the Same	3.4	4.5	8.0	6.5	6.5	12.9
Somewhat More	11.4	11.4	22.7	6.5	19.4	25.8
More	23.9	30.7	54.5	9.7	6.5	16.1
Total	46.6	53.4	100.0	51.6	48.4	100.0

Compared to a year ago, organisation 1 respondents believe they receive more spam, organisation 2 respondents believe they receive less

For organisation 1, a clear majority of respondents (77.2%) believe they are receiving more spam now than a year ago. Only 14.8% believe they are receiving less.

For organisation2, however, a slight majority of respondents (45.2%) believe they are receiving less spam now than a year ago, compared to the number of respondents (41.9%) who believe they are receiving more spam now.

As discussed previously, the most probable reason for respondents from organisation 2 believing they are receiving less spam now is related to the change of domain name, in that their new email addresses are not yet “known” to spammers, so they are currently enjoying a “spam holiday”.

Table 16***Why Am I Receiving Spam? (RQ2)***

	Org1 (N=87)			Org2 (N=31)		
	Male	Female	Total	Male	Female	Total
	N _r =56	N _r =71	N _r =127	N _r =24	N _r =18	N _r =42
	%	%	%	%	%	%
I don't really know	26.4	28.7	55.2	25.8	22.6	48.4
My email address is on our organisational website	9.2	20.7	29.9	25.8	6.5	32.3
My email address is on someone's website	4.6	10.3	14.9	9.7	3.2	12.9
I registered my email address on a suspect website	5.7	1.1	6.9	3.2	3.2	6.5
I posted my email address online	4.6	4.6	9.2	3.2	.0	3.2
I replied to a spam email at least once	1.1	2.3	3.4	3.2	3.2	6.5
I accidentally visited an inappropriate website	1.1	2.3	3.4	.0	.0	.0
Other	11.5	11.5	23.0	6.5	19.4	25.8
Total (N%)	46.0	54.0	100.0	51.6	48.4	100.0

(For multiple-response questions, N=number of respondents, N_r= number of responses)

Most respondents don't really know how spammers got their email address, but many believe it is because it is on their own organisation's or someone else's website

For each of the multiple-response choices, the percentages of responses for each choice showed a high degree of similarity between the two organisations.

The majority of respondents in both organisations (55.2% and 48.4% respectively) indicated that they didn't really know how spammers had found their email address, which is not surprising, as spammers use a wide variety of address harvesting techniques.

It may also be an indication though, that many Internet users are not as aware as they should be of the “trails” they may leave behind, including their email addresses, when chatting, shopping or subscribing on the Internet.

Of those respondents in both organisations who chose one or more reasons for how spammers may have found their email address, almost one-third of respondents (29.9% and 32.3% respectively) believe it is because their email address is on their organisational website. As harvesting addresses from organisational websites is a very popular method used by spammers, this choice was deliberately placed further down the list in the survey (in 4th position), so that it would be less likely to be chosen as a result of order bias.

For organisation 1, more than twice as many female respondents chose this reason than males (9.2% and 20.7% respectively). By way of contrast, in organisation 2, about four times as many male respondents as female chose this reason (25.8% and 6.5% respectively).

The next most popular choice by respondents from both organisations was the open-ended “Other” choice (23.0% and 25.8% respectively), and these responses will be discussed after the thematic summary further on.

A smaller number of respondents from both organisations (14.9% and 12.9% respectively) believed their email addresses were found on someone else’s website, or that they had registered their email address on a suspect website (6.9% and 6.5% respectively).

Only 3 respondents, all from organisation 1, believed their email addresses had been found because of accidentally visiting an inappropriate website.

Although the numbers of respondents who chose specific ways they believed spammers may have found their email address is small, it does provide an indication that some are aware of the possible consequences that Internet activity can have.

Table 17

Other Reasons why I may be Receiving spam (Org1) (RQ2)

	Reason
Org1	1 I use out of office a lot which replies to spam that comes through.
	2 Automatic ' Out Of Office ' reply
	3 I replied but through an out of office assistant - so not deliberately
	4 Out of office assistant replies to spam
	5 [#] Some comes through our <i>abc@xyz.co.nz</i> * site we use for our <i>department</i> *. In terms of replying to spam this only occurs when I have my out of office assistant on if I am away for a period of time.
	6 My email address was on an email sent by a colleague to a harvester .
	7 I believe that it's because they use pictures instead of text to get past the SPAM blockers
	8 Static isp so it's somewhat uncontrolled.
	9 A few years ago I did reply to a spam email to give them a piece of my mind - not sure what the outcome was though!
	10 One of the first spam emails I received I replied to & asked that they didn't email me again. Was told later that I shouldn't have done that as it confirms my email address.
	11 From searching & subscribing on net for <i>work</i> * prep
	12 I have submitted by email address when joining a membership
	13 Think someone sent me a chain e mail that I sent on and it picked up my email address
	14 Chain letters sent to me
	15 Giving business cards to suppliers at trade shows
	16 My e-mail address is on my business cards
	17 Internet shopping
	18 I've only had 1 or 2 'actual' spam emails, the rest were from contacts of mine but the subject line came up with 'spam' in it ????
	19 Other peoples bad habit of CC my email address rather than display name
	20 There are news reports confirming far more spammail is out there. Now getting a dozen emails from same source where previously one source.

(* actual words replaced to protect anonymity of organisation; [#] two reasons given)

Table 18***Other Reasons why I may be Receiving spam (Org2) (RQ2)***

Reason	
Org2	1 It has been on forwarded with out being deleted by someone else
	2 I got forwarded a spam email from another workmate whilst on holiday...
	3 Out of office assistant when away
	4 Purchasing items over the internet
	5 Bebo website /Oldfriends website
	6 Emails coming through as ' Spam ' are from identified sources , jokes or 'banned' by company and need to request their release
	7 Email address has been harvested by a worm from someone's contacts/address book.
	8 Not really sure how they get my email address

Table 19***Thematic Summary of Respondent's Reasons why they may be Receiving spam (RQ2)***

Theme	Frequency		
	Org1	Org2	Total
Out of Office Assistant	5	1	6
Technical reason (e.g. forwarded to spammer by colleague/worm, using pictures in spam, 'static isp')	3	1	4
Subscribing/registering on a website	2	1	3
Specifically replying to spam	2	0	2
Chain letter emails	2	0	2
Email address is on Business Card	2	0	2
Forwarded on from someone else	0	2	2
Internet shopping	1	1	2
False positives (legitimate emails tagged/quarantined as spam)	1	1	2
Email address on organisation website	1	0	1
Other or Don't Know	2	1	3
Total	21	8	29

Thematic Analysis of Respondent's Reasons why they may be Receiving spam

The reason mentioned most frequently by respondents of "Other" reasons, mainly by organisation 1, was that they believe spammers found their email address because of "Out of Office Assistant" auto-replies.

Four respondents gave "technical" reasons for how spammers found their email address, although 1 respondent misinterpreted the question and gave a reason for why spam was able to pass through the filters to them (using pictures instead of text).

Six respondents repeated reasons that were already in the closed-ended responses (subscribing/registering on a website, replying to spam, address on organisational website).

Internet shopping was mentioned by 2 respondents, 1 from each organisation, and was a good reason that had been overlooked for inclusion in the closed-ended responses.

Chain letters, mentioned by 2 respondents, was also a good possible explanation.

Email addresses on business cards, given as the reason by 2 respondents who were both from organisation 1, raises the question of what they believe spam emails to be. The survey included a definition of spam that stated they were "from a sender unknown to recipients who had not given permission for the email to be sent". If the respondents had given their business cards to someone, they would certainly not be unknown, and they have also implicitly given consent to be emailed by voluntarily giving them their email address.

There were two other themes that were misinterpretations of the question:

- Two respondents from organisation 2 gave specific instances of receiving spam forwarded on from someone else, rather than how spammers found their email address.
- Two respondents, 1 from each organisation, wrote that "spam" they are receiving is from contacts known to them, but their emails were being tagged as spam by their organisation's anti-spam system (known as "false positives").

Spam Filters in My Organisation:**Table 20*****Generally Block Spam Quite Well (RQ1, RQ2, RQ3)***

	Org1 (N=86)			Org2 (N=31)		
	Male	Female	Total	Male	Female	Total
	%	%	%	%	%	%
Strongly Agree	8.1	9.3	17.4	22.6	16.1	38.7
Agree	19.8	24.4	44.2	25.8	29.0	54.8
Neutral	11.6	12.8	24.4	3.2	3.2	6.5
Disagree	4.7	5.8	10.5	.0	.0	.0
Strongly Disagree	2.3	1.2	3.5	.0	.0	.0
Total	46.5	53.5	100.0	51.6	48.4	100.0

Table 21***Let Too Many Spam Emails Through (RQ1, RQ2, RQ3)***

	Org1 (N=86)			Org2 (N=26)		
	Male	Female	Total	Male	Female	Total
	%	%	%	%	%	%
Strongly Agree	4.7	1.2	5.8	.0	.0	.0
Agree	11.6	26.7	38.4	.0	3.8	3.8
Neutral	16.3	15.1	31.4	11.5	11.5	23.1
Disagree	7.0	10.5	17.4	19.2	23.1	42.3
Strongly Disagree	5.8	1.2	7.0	19.2	11.5	30.8
Total	45.3	54.7	100.0	50.0	50.0	100.0

Spam filters generally block spam quite well

A clear majority of respondents from both organisations (61.6% and 93.5% respectively) agree that the spam filters in their organisation generally block spam quite well, with a small percentage of respondents from organisation 2 (14%) disagreeing, and no disagreement from organisation 1 respondents.

Opinions divided about too many spam emails being let through

Despite agreement with the previous statement, a small majority of respondents from organisation 1 (44.2%) still believe their organisation's spam filters let too many spam emails through, with only one in four (24.4%) in disagreement. A quite high percentage, nearly one in three (31.4%), took a neutral stance.

In contrast, a clear majority of respondents from organisation 2 (73.1%) believe that their organisation's spam filters do not let too many spam emails through, although almost one in four (23.1%) took a neutral stance.

Putting these two differing opinions in perspective though, organisation 1 is receiving about 60 times more email, and detecting more than 560 times more spam per day than organisation 2, and levels of spam in organisation 2 have apparently not yet returned to those experienced prior to their domain name change. Given the current conditions in organisation 2, it is possible that the respondent's belief that the filters are not letting too many spam emails is actually due to the domain name change.

Spam Filters in My Organisation:**Table 22*****Block Unsolicited Emails (Spam) I Want (RQ1, RQ2, RQ3)***

	Org1 (N=85)			Org2 (N=27)		
	Male	Female	Total	Male	Female	Total
	%	%	%	%	%	%
Strongly Agree	2.4	.0	2.4	.0	.0	.0
Agree	5.9	7.1	12.9	18.5	25.9	44.4
Neutral	17.6	15.3	32.9	18.5	14.8	33.3
Disagree	15.3	23.5	38.8	7.4	7.4	14.8
Strongly Disagree	4.7	8.2	12.9	7.4	.0	7.4
Total	45.9	54.1	100.0	51.9	48.1	100.0

Table 23***Block Good Emails (Non-Spam) I Want (RQ1, RQ2, RQ3)***

	Org1 (N=85)			Org2 (N=30)		
	Male	Female	Total	Male	Female	Total
	%	%	%	%	%	%
Strongly Agree	1.2	1.2	2.4	10.0	3.3	13.3
Agree	5.9	18.8	24.7	33.3	30.0	63.3
Neutral	16.5	18.8	35.3	3.3	10.0	13.3
Disagree	16.5	14.1	30.6	6.7	3.3	10.0
Strongly Disagree	5.9	1.2	7.1	.0	.0	.0
Total	45.9	54.1	100.0	53.3	46.7	100.0

Some agreement that filters block spam that respondents want

The intention of the question was to determine if respondents liked to receive some types of spam, but may have been misinterpreted by some respondents.

The results indicate that a small percentage of respondents from organisation 1, and a majority of respondents from organisation 2 (15.3% and 44.4% respectively) believe the filters block spam they want to receive. The majority of respondents from organisation 1 (51.7%) did not agree that the filters block spam they want.

A small percentage of respondents wanting to receive certain types of spam might be expected, and is confirmed by later results about how respondents feel about spam they receive, but the large majority percentage from organisation 2 was not expected.

There are two possible explanations for this percentage of responses of agreement from organisation 2 respondents:

- Respondents were confused by the wording of the statement
- Respondents from organisation 2 may be interpreting this statement according to the level of “false positives” (legitimate email falsely tagged as spam) that they receive. Several respondents from organisation 2 have noted, both in a previous question and in their final comments, that legitimate, and even business-related emails often get blocked or tagged as “spam”, although it is actually “email I want”.

Opinions divided about filters blocking legitimate email

Respondents from organisation 1 were divided about whether filters blocked good emails, with a small majority (37.7%) disagreeing, and one in four respondents (27.1%) agreeing.

As with the previous three statements, a high percentage of respondents from organisation 1 (35.3%) took a neutral stance.

A clear majority of respondents from organisation 2 (76.6%) agreed the filters blocked good emails, which may indicate the “false positive” reason for the previous statement is valid.

Table 24***Other Organisations Have Ever Bounced-back Your Email as Spam (RQ1, RQ2)***

	Org1 (N=86)			Org2 (N=31)		
	Male	Female	Total	Male	Female	Total
	%	%	%	%	%	%
Yes	20.9	30.2	51.2	22.6	12.9	35.5
Uncertain	9.3	12.8	22.1	12.9	22.6	35.5
No	15.1	11.6	26.7	16.1	12.9	29.0
Total	45.3	54.7	100.0	51.6	48.4	100.0

Table 25***Have Ever Accidentally Deleted Good Emails While Deleting Spam (RQ1, RQ2)***

	Org1 (N=87)			Org2 (N=31)		
	Male	Female	Total	Male	Female	Total
	%	%	%	%	%	%
Yes	23.0	16.1	39.1	16.1	19.4	35.5
Uncertain	8.0	10.3	18.4	9.7	3.2	12.9
No	14.9	27.6	42.5	25.8	25.8	51.6
Total	46.0	54.0	100.0	51.6	48.4	100.0

Table 26***Have Ever Opened Untagged Emails That Looked Like Possible Spam (RQ1, RQ2)***

	Org1 (N=87)			Org2 (N=31)		
	Male	Female	Total	Male	Female	Total
	%	%	%	%	%	%
Yes	17.2	28.7	46.0	22.6	22.6	45.2
Uncertain	9.2	9.2	18.4	6.5	9.7	16.1
No	19.5	16.1	35.6	22.6	16.1	38.7
Total	46.0	54.0	100.0	51.6	48.4	100.0

A majority of respondents may have had emails they sent bounced-back as spam

For both organisations, a small majority of respondents (51.2% and 35.5% respectively) believe they have had emails they sent rejected by other organisations as spam.

This result may be of some concern to both organisations, as it could mean that their email servers have been “blacklisted” as a spam source on occasions.

This result should be interpreted with care, however, as spammers (and viruses) do forge or “spoof” email “From:” addresses that are legitimate, which would mean that the bounce-backs may actually be the result of spammers sending spam using their forged “From:” address, which the recipient anti-spam system may then bounce back to them.

One in three respondents have accidentally deleted good emails while deleting spam

For both organisations, a small majority of respondents (42.5% and 51.6% respectively) have never accidentally deleted good emails while deleting spam emails.

Both organisations may have cause to be concerned though, as more than one in three respondents (39.1% and 35.5% respectively) reported that they have deleted good emails.

In fact, during informal discussion prior to their interview, one participant related how they had deleted a customer’s order along with some spam, but was fortunately able to retrieve it from the “Trash” after being contacted by the customer a week later when enquiring why they had not had a response to it.

A small majority of respondents have opened untagged emails that looked like spam

For both organisations, a small majority of respondents (46.0% and 45.2% respectively) have opened untagged emails, even though they looked like they were probably spam emails. Perhaps to avoid a scenario like the previous question, most respondents may be “erring on the side of caution”, and opening emails even though they could be spam, simply because they passed through the anti-spam systems undetected. The main reasons given for opening the emails are in the thematic summary in the following pages.

Table 27***Reasons for Opening (possible) Spam Email (Org1) (RQ1, RQ2)***

Org1		
1	First item on row and immediately	opened it without wanting to
2	In case it was a legitimate email	
3	It had a name on it I recognised	
4	Was not 100% sure it was not spam and needed to check, Subject line	seemed like it might be real.
5	Wasn't sure what it was.	
6	In case it was a legitimate email	
7	Not clear if it was spam, I receive many legitimate emails through my work that are from unfamiliar addresses	
8	In case it was a legitimate email	
9	It wasn't tagged as spam	
10	I thought it might be an old friend , or someone who knows me but I don't know them	
11	Spam is sometimes quite a laugh	
12	The title in the subject line led me to believe that they were genuine work emails.	
13	Wanted to see if the email was from a (potential business contact*)	
14	In case it was a legitimate email but it clearly wasn't!!	
15	To forward to our spam address for logging	
16	Thought it could be a remittance form from a client	
17	Preview Pane	
18	Curious and to ascertain it was in fact SPAM.	
19	Looked legit	
20	In case it was not spam	
21	In case it was legitimate	
22	In case it was legitimate email	
23	I have my email set to open the email highlighted , and also I was curious to see what the email was about seeing as I couldn't identify the sender	
24	Assumed it was a legitimate email	
25	The main reason was the Subject was 'Hi (my first name)'	
26	In case it was a legitimate email.	
27	Just in case it was legitimate . I usually open to delete them	
28	To see if it was legitimate mail.	
29	In case it was a work related email	
30	Couldn't tell it was spam without opening it	

- 31 **Name of addressee** did not look like spam
- 32 **Legitimate mail**...had to look at it...
- 33 **To see if** it was a **legitimate email**
- 34 I get a lot of unsolicited email in my job and **potentially it was work related**
- 35 Not tagged as [Spam]... **to check** if it was **legit**
- 36 No specific reason
- 37 I use **preview pane** on my outlook - if it don't have any cause to open it I delete it.
- 38 **In case** it was a **legitimate email** from a **person requesting information regarding (our organisation*)**.
- 39 **Seemed to be** a **legitimate** email
- 40 **Uncertain as to legitimacy** of the e-mail

Note 1. Actual words replaced to protect anonymity of organisation

Table 28***Reasons for Opening (possible) Spam Email (Org2) (RQ1, RQ2)***

Org2	1	Curious
	2	In case it was legitimate - looked like it was from someone I know
	3	It looked legitimate from the sender & subject line (only one)
	4	Description / subject of email
	5	Email address could have meant something to me
	6	It is the first email on my list and the other pane (viewing pane) is also open so it automatically opens the spam .
	7	Dunno. didn't open
	8	In case it was a legitimate email
	9	To check whether legitimate email .
	10	In case it was a legitimate email .
	11	It had a heading that looked like it could have been for work
	12	To see what the email was about
	13	In case it was a legitimate email
	14	No indication it was spam

Table 29**Thematic Summary of Reasons for Opening (possible) Spam Email (RQ1, RQ2)**

Theme	Frequency		
	Org1	Org2	Total
Checking "just in case" it was a legitimate email	16	5	21
Thought it was legitimate	6	2	8
Subject line looked legitimate	3	3	6
Receive unsolicited email as part of job	6	0	6
Thought the sender name might be someone they knew	3	2	5
Opened automatically by "preview pane"	3	1	4
Curious	2	2	4
Unsure what it was	3	0	3
No specific reason given	1	1	2
Opened by accident (first item on row)	1	0	1
Amusement	1	0	1
Total	45	16	61

Thematic Analysis of Reasons for Opening (possible) Spam Email

The examples given for this survey question were “in case it was a legitimate email”, and “wanted to see what it was selling”, and the choice of words from the first example have probably introduced some bias into the choice of words used by respondents in giving reasons for opening possible spam. It is possible that this may also have biased the reasons, but as there was a second example reason respondents could have also used, but did not, it is more likely respondents were stating a genuine reason, but just using the choice of words supplied in the example.

For both organisations, the major reason given by respondents (16 and 5 respectively) for opening a possible spam email was as per the example just discussed: “in case it was a legitimate email”. This doubt or uncertainty about the nature of the email was also expressed slightly differently by 3 respondents who were not “sure” or it was not “clear”. Respondents from both organisations thought the email *looked* legitimate in some way (6 and 2 respectively), and 3 respondents from each organisation thought the Subject line specifically looked legitimate.

Two primary goals of any spammer are to evade spam filters and to get the recipient to read the spam. Both of these goals can often be accomplished simultaneously simply by making the spam look as closely as possible like a legitimate email (Spammer-X, 2004, p. 216), so it is not surprising that the top three reasons given relate to the email looking legitimate.

For both organisations, 2 respondents from each stated that their reason for opening the email was because they were curious. As mentioned above, one of the spammer’s goals is to get the recipient to read it, and doing so often includes using marketing or social engineering techniques that will arouse enough curiosity in the recipient that they will open the email.

Deserving of sympathy are those respondents who receive unsolicited email as part of their job, usually as a point of contact for an organisation or a department within it. Six respondents from organisation 1 gave the reason that it could have been work related, and 2 respondents specifically mentioned that receiving unsolicited email or email from unfamiliar addresses was part of their job.

A few respondents from both organisations (3 and 2 respectively) thought the name on the email looked familiar, and might be someone they knew. Statistically it is quite possible that as spammers' software cycles through any possible combinations of forged sender first names and surnames, a particular combination will occur that will look like a familiar name to the recipient, and they will open it as a result.

For both organisations a few respondents (3 and 1 respectively) had the spam automatically opened for them by their email client's "preview pane", so for these respondents it was somewhat unintentional.

Three respondents from organisation 1 were not sure of the nature of the email, although this could probably also be classified as a "just in case" reason.

One respondent from organisation opened a spam by accident (accidents do happen)!

One respondent from organisation 1 also stated there was amusement value to be found in some spam emails which could be "a laugh". The respondent may be referring in this case to spam emails that employ software to generate random sentences, which often generate long paragraphs of prose that almost make sense, but are in fact generated with the previously mentioned goal of beating the recipient's spam filters.

Table 30***Have Ever Clicked on a Graphic or Link within a Spam Email (RQ2, RQ3)***

	Org1 (N=84)			Org2 (N=31)		
	Male	Female	Total	Male	Female	Total
	%	%	%	%	%	%
Yes	6.0	1.2	7.1	3.2	.0	3.2
Uncertain	4.8	11.9	16.7	9.7	6.5	16.1
No	35.7	40.5	76.2	38.7	41.9	80.6
Total	46.4	53.6	100.0	51.6	48.4	100.0

Table 31***Reason Given for Clicking on Link within a Spam Email (RQ2)***

Org1	1	Wasn't certain of whether the email was spam
	2	By accident
	3	Curiosity
	4	It was a Bank hoax and I wanted to supply the bank with as much info as poss.
	5	I wasn't sure if it was spam, it could've been from (...a potential contact*)
	6	I thought it was rather obscure and curiosity got to me...
Org2	1	Curious

Note 1. Actual words replaced to protect anonymity of organisation

Most Respondents Have Not Clicked on Links within Spam

A clear majority of respondents from both organisations (76.2% and 80.6% respectively)

say they have never clicked on a (URL) link within a spam email.

All but one of those who did were men.

Curiosity the Main Reason When They Did

Of those who stated they had clicked on a link, curiosity was the main reason given.

Of the remainder, uncertainty of whether the email was spam (2 respondents) was the next main reason, 1 respondent clicked by accident, and 1 respondent was trying to “do the right thing” when they received a bank phishing scam, and provide details to the bank.

Table 32***Have Ever Purchased a Product or Service Offered in a Spam Email (RQ2, RQ3)***

	Org1 (N=87)			Org2 (N=31)		
	Male	Female	Total	Male	Female	Total
	%	%	%	%	%	%
Yes	.0	.0	.0	.0	.0	.0
Uncertain	1.1	.0	1.1	.0	.0	.0
No	44.8	54.0	98.9	51.6	48.4	100.0
Total	46.0	54.0	100.0	51.6	48.4	100.0

No one has purchased anything from a spam email

With the exception of one uncertain male from organisation 1, no respondent stated they have ever purchased anything from a spam email.

As previously indicated by Spammer-X (2004, p. 10), the best way to stop spam is not to purchase anything advertised in it, so this result from employees hopefully indicates a responsible attitude towards reducing the problem of spam.

This is also one of the four “Four Golden Rules” advocated by Internet NZ, and in fact is “Rule 1: Never buy anything advertised in a spam” (InternetNZ, 2006a).

Table 33***Have Ever Received a "Phishing" Type Email for a Bank, PayPal etc. (RQ2)***

	Org1 (N=86)			Org2 (N=30)		
	Male	Female	Total	Male	Female	Total
	%	%	%	%	%	%
Yes	19.8	19.8	39.5	16.7	20.0	36.7
Uncertain	2.3	4.7	7.0	.0	3.3	3.3
No	24.4	29.1	53.5	33.3	26.7	60.0
Total	46.5	53.5	100.0	50.0	50.0	100.0

A Majority Have Never Received a Phishing Email

A clear majority of respondents from both organisations (53.5% and 60% respectively) have never received phishing emails, but more than one in three respondents from both organisations *have* received one of these scam emails, which may be cause for concern.

Table 34***Have Ever Clicked on Link in Phishing Email and Logged-in (RQ2)***

	Org1 (N=34)			Org2 (N=11)		
	Male	Female	Total	Male	Female	Total
	%	%	%	%	%	%
Yes	.0	.0	.0	.0	.0	.0
Uncertain	.0	.0	.0	.0	.0	.0
No	50.0	50.0	100.0	45.5	54.5	100.0
Total	50.0	50.0	100.0	45.5	54.5	100.0

Of the respondents who had received a phishing email, none had ever clicked on the link in it and logged in. From the previous section, "Reason Given for Clicking on Link Within a Spam Email", one respondent (from organisation 1, #5) indicated they had clicked on the link inside one of these emails, but only to provide the bank with information about it, so the indication is that respondents are clearly aware of the threat posed by these scams.

How Do You Really Feel About the Unsolicited Emails You Receive?

Table 35

Selling Cheap Software (RQ2, RQ3)

	Org1 (N=76)			Org2 (N=28)		
	Male (N _r =41)	Female (N _r =45)	Total (N _r =86)	Male (N _r =15)	Female (N _r =16)	Total (N _r =31)
	%	%	%	%	%	%
Like it	1.3	.0	1.3	.0	.0	.0
Happy	.0	.0	.0	.0	.0	.0
Angry	10.5	5.3	15.8	7.1	3.6	10.7
Frustrated	18.4	28.9	47.4	3.6	14.3	17.9
Disgusted	.0	.0	.0	.0	.0	.0
Worried	.0	1.3	1.3	.0	3.6	3.6
Embarrassed	.0	.0	.0	.0	3.6	3.6
Don't Care	23.7	23.7	47.4	42.9	32.1	75.0
Total (N%)	48.7	51.3	100.0	53.6	46.4	100.0

Note 1. In multiple-response question: N=number of respondents, N_r= number of responses

Organisational Differences

In organisation 1, slightly more respondents expressed composite anger than those who didn't care, but in organisation 2 this was the opposite, where a clear majority (75%) didn't care about it, compared to those who expressed composite anger about it. One person from organisation 1 (male) *liked to receive spam about cheap software*, and 1 respondent from each organisation (both female) expressed anxiety (worry) about it.

Gender Similarities

Response	Org1			Org2		
	Male	Female	Ratio	Male	Female	Ratio
Angry	10.5%	5.3%	2:1	7.1%	3.6%	2:1
Frustrated	18.4%	28.9%	1:1.6	3.6%	14.3%	1:4
Don't Care	23.7%	23.7%	1:1	42.9%	32.1%	1.3:1

In both organisations, *women expressed more frustration than men* with this spam, and *twice as many men expressed anger about it than women*. Similar ratios of men and women from both organisations didn't care about it.

Table 36***Sexual Performance Drugs (RQ2, RQ3)***

	Org1 (N=82)			Org2 (N=29)		
	Male (N _r =52)	Female (N _r =61)	Total (N _r =113)	Male (N _r =15)	Female (N _r =21)	Total (N _r =36)
	%	%	%	%	%	%
Like it	.0	.0	.0	.0	.0	.0
Happy	.0	.0	.0	.0	.0	.0
Angry	14.6	13.4	28.0	6.9	13.8	20.7
Frustrated	13.4	31.7	45.1	3.4	17.2	20.7
Disgusted	8.5	12.2	20.7	3.4	27.6	31.0
Worried	1.2	1.2	2.4	3.4	.0	3.4
Embarrassed	3.7	7.3	11.0	.0	6.9	6.9
Don't Care	22.0	8.5	30.5	34.5	6.9	41.4
Total (N%)	47.6	52.4	100.0	51.7	48.3	100.0

Note 1. In multiple-response question: N=number of respondents, N_r= number of responses

Organisational Similarities and Differences

A majority of respondents from both organisations expressed one of the composite anger forms (angry, frustrated, or disgusted) as used by Grandey et al.(2002, p. 41), but almost one in three from organisation 1, and two out of five from organisation 2 (30.5% and 41.4% respectively) didn't care about it. A small percentage from both organisations expressed some form of composite anxiety (13.4% and 10.3% respectively).

Gender Similarities

Response	Org1			Org2		
	Male	Female	Ratio	Male	Female	Ratio
Angry	14.6%	13.4%	1:1	6.9%	13.8%	1:2
Frustrated	13.4%	31.7%	1:2.4	3.4%	17.2%	1:5
Disgusted	8.5%	12.2%	1:1.4	3.4%	27.6%	1:8
Don't Care	22.0%	8.5%	2.6:1	34.5%	6.9%	5:1

In both organisations, *women expressed more composite anger than men* for spam about sexual performance drugs, *particularly frustration and disgust*, while *men were much more likely not to care about it* than women.

Table 37***Weight Loss Drugs/Programmes (RQ2, RQ3)***

	Org1 (N=78)			Org2 (N=28)		
	Male (N _r =41)	Female (N _r =51)	Total (N _r =92)	Male (N _r =15)	Female (N _r =14)	Total (N _r =29)
	%	%	%	%	%	%
Like it	.0	.0	.0	7.1	3.6	10.7
Happy	.0	.0	.0	.0	.0	.0
Angry	9.0	14.1	23.1	7.1	7.1	14.3
Frustrated	16.7	30.8	47.4	.0	14.3	14.3
Disgusted	2.6	7.7	10.3	3.6	3.6	7.1
Worried	1.3	1.3	2.6	.0	3.6	3.6
Embarrassed	1.3	2.6	3.8	.0	.0	.0
Don't Care	21.8	9.0	30.8	35.7	17.9	53.6
Total (N%)	47.4	52.6	100.0	53.6	46.4	100.0

Note 1. In multiple-response question: N=number of respondents, N_r= number of responses

Organisational Similarities and Differences

The majority of respondents from organisation 1 expressed composite anger, with almost half (47.4%) being frustrated. By comparison, the majority of respondents on organisation 2 (53.6%) did not care about it, along with nearly one in three (30.8%) in organisation 1 also. A small number of respondents from organisation 2 (2 male, 1 female) *liked to receive UBE about weight loss drugs and programmes.*

Gender Similarities

Response	Org1			Org2		
	Male	Female	Ratio	Male	Female	Ratio
Angry	9.0%	14.1%	1:1.6	7.1%	7.1%	1:1
Frustrated	16.7%	30.8%	1:1.8	0%	14.3%	~
Disgusted	2.6%	7.7%	1:3	3.6%	3.6%	1:1
Don't Care	21.8%	9.0%	2.4:1	35.7%	17.9%	2:1

From both organisations *women expressed more composite anger than men, particularly frustration*, with only women in organisation2 expressing frustration. For both organisations *men were again much more likely to not care about it than women.*

Table 38***Male Enhancement/Enlargement Products (RQ2, RQ3)***

	Org1 (N=81)			Org2 (N=28)		
	Male (N _r =47)	Female (N _r =59)	Total (N _r =106)	Male (N _r =14)	Female (N _r =21)	Total (N _r =35)
	%	%	%	%	%	%
Like it	.0	.0	.0	.0	.0	.0
Happy	.0	.0	.0	.0	.0	.0
Angry	12.3	16.0	28.4	7.1	17.9	25.0
Frustrated	16.0	28.4	44.4	3.6	10.7	14.3
Disgusted	7.4	13.6	21.0	10.7	25.0	35.7
Worried	.0	1.2	1.2	.0	3.6	3.6
Embarrassed	1.2	6.2	7.4	.0	10.7	10.7
Don't Care	21.0	7.4	28.4	28.6	7.1	35.7
Total (N%)	48.1	51.9	100.0	50.0	50.0	100.0

Note 1. In multiple-response question: N=number of respondents, N_r= number of responses

Organisational Similarities and Differences

A majority of respondents from both organisations expressed some form of composite anger, but more than one in four from organisation 1 and one in three from organisation 2 (28.4% and 35.7% respectively) didn't care about it. In both organisations a small percentage expressed some form of composite anxiety (8.6% and 14.3% respectively).

Gender Similarities

Response	Org1			Org2		
	Male	Female	Ratio	Male	Female	Ratio
Angry	12.3%	16.0%	1:1.3	7.1%	17.9%	1:2.5
Frustrated	16.0%	28.4%	1:1.8	3.6%	10.7%	1:3
Disgusted	7.4%	13.6%	1:1.8	10.7%	25.0%	1:2.3
Don't Care	21.0%	7.4%	2.8:1	28.6%	7.1%	4:1

In both organisations, *women expressed more composite anger than men* for spam about male enhancement/enlargement products, *particularly frustration and disgust*, while *men were much more likely not to care about it* than women. In both organisations, *women also expressed much more composite anxiety than men*.

Table 39***Mortgage/Loan Financing (RQ2, RQ3)***

	Org1 (N=82)			Org2 (N=27)		
	Male (N _r =42)	Female (N _r =50)	Total (N _r =92)	Male (N _r =13)	Female (N _r =16)	Total (N _r =29)
	%	%	%	%	%	%
Like it	.0	.0	.0	7.4	.0	7.4
Happy	.0	.0	.0	.0	.0	.0
Angry	12.2	12.2	24.4	11.1	11.1	22.2
Frustrated	17.1	31.7	48.8	3.7	18.5	22.2
Disgusted	1.2	1.2	2.4	3.7	.0	3.7
Worried	.0	2.4	2.4	.0	3.7	3.7
Embarrassed	.0	.0	.0	.0	.0	.0
Don't Care	20.7	13.4	34.1	22.2	25.9	48.1
Total (N%)	46.3	53.7	100.0	48.1	51.9	100.0

Note 1. In multiple-response question: N=number of respondents, N_r= number of responses

Organisational Similarities and Differences

In organisation 1 the *majority of respondents expressed composite anger, particularly frustration*, whereas the *majority of respondents in organisation 2 didn't care about it*.

Two respondents from organisation 2 (both male) *liked to receive mortgage/loan spam*.

Gender Similarities and Differences

Response	Org1			Org2		
	Male	Female	Ratio	Male	Female	Ratio
Angry	12.2%	12.2%	1:1	11.1%	11.1%	1:1
Frustrated	17.1%	31.7%	1:1.8	3.7%	18.5%	1:5
Disgusted	1.2%	1.2%	1:1	3.7%	0%	~
Don't Care	20.7%	13.4%	1.5:1	22.2%	25.9%	1:1.2

Men and women in both organisations were *equally angry* about this spam, but again, *women expressed more frustration than men*. More men than women didn't care about this spam in organisation 1, whereas slightly more women than men didn't care about it in organisation 2.

Table 40***Job/Employment Offers (RQ2, RQ3)***

	Org1 (N=78)			Org2 (N=26)		
	Male (N _r =41)	Female (N _r =44)	Total (N _r =85)	Male (N _r =13)	Female (N _r =13)	Total (N _r =26)
	%	%	%	%	%	%
Like it	1.3	1.3	2.6	7.7	.0	7.7
Happy	.0	2.6	2.6	3.8	3.8	7.7
Angry	9.0	7.7	16.7	3.8	7.7	11.5
Frustrated	17.9	25.6	43.6	3.8	15.4	19.2
Disgusted	1.3	.0	1.3	.0	.0	.0
Worried	.0	1.3	1.3	.0	.0	.0
Embarrassed	.0	.0	.0	.0	.0	.0
Don't Care	23.1	17.9	41.0	30.8	23.1	53.8
Total (N%)	48.7	51.3	100.0	50.0	50.0	100.0

Note 1. In multiple-response question: N=number of respondents, N_r= number of responses

Organisational Similarities and Differences

The majority of respondents from organisation 1 expressed composite anger, whereas the majority of respondents in organisation 2 didn't care about it. Two out of five respondents (41%) in organisation 1 also didn't care about it, and 1 respondent expressed some anxiety.

Four respondents from each organisation *liked receiving spam about job offers*.

Gender Similarities and Differences

Response	Org1			Org2		
	Male	Female	Ratio	Male	Female	Ratio
Angry	9.0%	7.7%	1.2:1	3.8%	7.7%	1:2
Frustrated	17.9%	25.6%	1:1.4	3.8%	15.4%	1:4
Disgusted	0%	1.3%	~	0%	0%	~
Don't Care	23.1%	17.9%	1.3:1	30.8%	23.1%	1.3:1

Men expressed slightly more anger than women in organisation 1, whereas women expressed more anger in organisation 2.

In both organisations, women expressed more frustration than men, and men were more likely to not care about it than women.

Table 41***Adult Pornography Websites (RQ2, RQ3)***

	Org1 (N=73)			Org2 (N=27)		
	Male (N _r =47)	Female (N _r =54)	Total (N _r =101)	Male (N _r =17)	Female (N _r =28)	Total (N _r =45)
	%	%	%	%	%	%
Like it	.0	.0	.0	.0	.0	.0
Happy	.0	.0	.0	.0	.0	.0
Angry	19.2	16.4	35.6	11.1	25.9	37.0
Frustrated	12.3	26.0	38.4	3.7	11.1	14.8
Disgusted	9.6	17.8	27.4	18.5	40.7	59.3
Worried	.0	2.7	2.7	7.4	7.4	14.8
Embarrassed	4.1	6.8	11.0	3.7	14.8	18.5
Don't Care	19.2	4.1	23.3	18.5	3.7	22.2
Total (N%)	49.3	50.7	100.0	51.9	48.1	100.0

Note 1. In multiple-response question: N=number of respondents, N_r= number of responses

Organisational Similarities and Differences

A majority of respondents from both organisations expressed composite anger, with more than one in three expressing anger, and nearly three out of five (59.3%) from organisation 2 expressing disgust. Respondents expressed higher levels of composite anxiety (worried, embarrassed) than for previous types of spam, but more than one in five from both organisations still didn't care about it.

Gender Similarities and Differences

Response	Org1			Org2		
	Male	Female	Ratio	Male	Female	Ratio
Angry	19.2%	16.4%	1.2:1	11.1%	25.9%	1:2.3
Frustrated	12.3%	26.0%	1:2	3.7%	11.1%	1:3
Disgusted	9.6%	17.8%	1:1.8	18.5%	40.7%	1:2.2
Don't Care	19.2%	4.1%	4.7:1	18.5%	3.7%	5:1

In both organisations, *women generally expressed more frustration, anger and disgust than men* about this type of spam, and *men were much more likely to not care about it* than women. Organisation 1 men were the exception, being *slightly angrier than women*.

Table 42***Child Pornography Websites (RQ2, RQ3)***

	Org1 (N=69)			Org2 (N=27)		
	Male (N _r =56)	Female (N _r =62)	Total (N _r =118)	Male (N _r =17)	Female (N _r =27)	Total (N _r =44)
	%	%	%	%	%	%
Like it	.0	.0	.0	.0	.0	.0
Happy	.0	.0	.0	.0	.0	.0
Angry	23.2	21.7	44.9	18.5	29.6	48.1
Frustrated	13.0	15.9	29.0	.0	7.4	7.4
Disgusted	30.4	39.1	69.6	33.3	44.4	77.8
Worried	2.9	8.7	11.6	3.7	7.4	11.1
Embarrassed	4.3	1.4	5.8	3.7	7.4	11.1
Don't Care	7.2	2.9	10.1	3.7	3.7	7.4
Total (N%)	47.8	52.2	100.0	51.9	48.1	100.0

Note 1. In multiple-response question: N=number of respondents, N_r= number of responses

Organisational Similarities and Differences

A clear majority of respondents from both organisations expressed composite anger, particularly anger and disgust, for this type of spam. There was also some composite anxiety expressed, and significantly fewer respondents didn't care about it.

Gender Similarities and Differences

Response	Org1			Org2		
	Male	Female	Ratio	Male	Female	Ratio
Angry	23.2%	21.7%	1:1	18.5%	29.6%	1:1.6
Frustrated	13.0%	15.9%	1:1.2	0%	7.4%	~
Disgusted	30.4%	39.1%	1:1.3	33.3%	44.4%	1:1.3
Don't Care	7.2%	2.9%	2.5:1	3.7%	3.7%	1:1

Again, *women in both organisations generally expressed more anger, frustration and disgust than men*, and though the percentages of those who didn't care in both organisations were quite small, slightly more men than women from organisation 1 didn't care about this type of spam.

Table 43***Dating Websites (RQ2, RQ3)***

	Org1 (N=74)			Org2 (N=27)		
	Male (N _r =38)	Female (N _r =46)	Total (N _r =84)	Male (N _r =13)	Female (N _r =16)	Total (N _r =29)
	%	%	%	%	%	%
Like it	1.4	.0	1.4	.0	.0	.0
Happy	.0	.0	.0	.0	.0	.0
Angry	10.8	12.2	23.0	7.4	11.1	18.5
Frustrated	14.9	28.4	43.2	11.1	14.8	25.9
Disgusted	1.4	5.4	6.8	3.7	7.4	11.1
Worried	.0	2.7	2.7	.0	3.7	3.7
Embarrassed	1.4	4.1	5.4	.0	3.7	3.7
Don't Care	21.6	9.5	31.1	25.9	18.5	44.4
Total (N%)	48.6	51.4	100.0	48.1	51.9	100.0

Note 1. In multiple-response question: N=number of respondents, N_r= number of responses

Organisational Similarities and Differences

Although nearly one in three and two out of five respondents from each organisation (31.1% and 44.4% respectively) didn't care about this spam, a majority from organisation 1 and significant numbers from organisation 2 also expressed composite anger. One respondent from organisation 1 (male) *liked to receive spam about dating websites*.

Gender Similarities and Differences

Response	Org1			Org2		
	Male	Female	Ratio	Male	Female	Ratio
Angry	10.8%	12.2%	1:1.1	7.4%	11.1%	1:1.5
Frustrated	14.9%	28.4%	1:1.9	11.1%	14.8%	1:1.3
Disgusted	1.4%	5.4%	1:3.8	3.7%	7.4%	1:2
Don't Care	21.6%	9.5%	2.3:1	25.9%	18.5%	1.4:1

Again, women in both organisations generally expressed more anger, frustration and disgust than men, and men were more likely not to care about it than women.

Table 44***Stock Market "Tips" (RQ2, RQ3)***

	Org1 (N=79)			Org2 (N=28)		
	Male (N _r =43)	Female (N _r =47)	Total (N _r =90)	Male (N _r =16)	Female (N _r =15)	Total (N _r =31)
	%	%	%	%	%	%
Like it	.0	.0	.0	3.6	.0	3.6
Happy	.0	.0	.0	7.1	.0	7.1
Angry	13.9	11.4	25.3	3.6	10.7	14.3
Frustrated	16.5	31.6	48.1	14.3	17.9	32.1
Disgusted	1.3	.0	1.3	3.6	.0	3.6
Worried	1.3	.0	1.3	.0	3.6	3.6
Embarrassed	.0	.0	.0	.0	.0	.0
Don't Care	21.5	16.5	38.0	25.0	21.4	46.4
Total (N%)	46.8	53.2	100.0	53.6	46.4	100.0

Note 1. In multiple-response question: N=number of respondents, N_r= number of responses

Organisational Similarities and Differences

The majority of respondents in organisation 1 expressed composite anger, with *almost half being frustrated*, whereas most respondents in organisation 2 didn't care about stock market spam, but one in three (32.1%) were still frustrated by it. Three respondents from organisation 2 *liked to receive stock market spam*.

Gender Similarities and Differences

Response	Org1			Org2		
	Male	Female	Ratio	Male	Female	Ratio
Angry	13.9%	11.4%	1.2:1	3.6%	10.7%	1:3
Frustrated	16.5%	31.6%	1:1.9	14.3%	17.9%	1:1.3
Disgusted	1.3%	0%	~	3.6%	0%	~
Don't Care	21.5%	16.5%	1.3:1	25.0%	21.4%	1.2:1

Slightly more men expressed anger in organisation 1, but more women expressed anger in organisation 2. In both organisations, *women expressed more frustration than men*, and *more men didn't care about it*. All 3 respondents in organisation 2 *who liked to receive this spam were men*.

Table 45**Online Casino Websites (RQ2, RQ3)**

	Org1 (N=71)			Org2 (N=27)		
	Male (N _r =40)	Female (N _r =40)	Total (N _r =80)	Male (N _r =14)	Female (N _r =18)	Total (N _r =32)
	%	%	%	%	%	%
Like it	1.4	.0	1.4	3.7	.0	3.7
Happy	.0	.0	.0	.0	.0	.0
Angry	12.7	9.9	22.5	3.7	14.8	18.5
Frustrated	16.9	31.0	47.9	7.4	22.2	29.6
Disgusted	2.8	1.4	4.2	7.4	3.7	11.1
Worried	.0	1.4	1.4	.0	3.7	3.7
Embarrassed	1.4	.0	1.4	.0	.0	.0
Don't Care	21.1	12.7	33.8	29.6	22.2	51.9
Total (N%)	49.3	50.7	100.0	51.9	48.1	100.0

Note 1. In multiple-response question: N=number of respondents, N_r= number of responses

Organisational Similarities and Differences

As with the “stock market” spam, the majority of respondents in organisation 1 expressed composite anger, particularly frustration, and the majority of respondents in organisation 2 didn’t care. Three respondents expressed anxiety, and *1 respondent from each organisation liked to receive online casino spam.*

Gender Similarities and Differences

Response	Org1			Org2		
	Male	Female	Ratio	Male	Female	Ratio
Angry	12.7%	9.9%	1.3:1	3.7%	14.8%	1:4
Frustrated	16.9%	31.0%	1:1.8	7.4%	22.2%	1:3
Disgusted	2.8%	1.4%	2:1	7.4%	3.7%	2:1
Don’t Care	21.1%	12.7%	1.7:1	29.6%	22.2%	1.3:1

Again, the men in organisation 1 expressed slightly more anger, whereas the women in organisation 2 expressed more anger. In both organisations, *women expressed more frustration than men, and again slightly more men than women didn’t care about it. Both of the respondents who liked to receive casino website spam were men.*

Table 46**"Nigerian" Fraud (RQ2, RQ3)**

	Org1 (N=76)			Org2 (N=28)		
	Male (N _r =46)	Female (N _r =54)	Total (N _r =100)	Male (N _r =17)	Female (N _r =21)	Total (N _r =38)
	%	%	%	%	%	%
Like it	1.3	.0	1.3	.0	.0	.0
Happy	1.3	.0	1.3	.0	.0	.0
Angry	18.4	21.1	39.5	32.1	25.0	57.1
Frustrated	21.1	31.6	52.6	7.1	14.3	21.4
Disgusted	2.6	9.2	11.8	.0	7.1	7.1
Worried	1.3	2.6	3.9	7.1	10.7	17.9
Embarrassed	.0	.0	.0	.0	3.6	3.6
Don't Care	14.5	6.6	21.1	14.3	14.3	28.6
Total (N%)	47.4	52.6	100.0	53.6	46.4	100.0

Note 1. In multiple-response question: N=number of respondents, N_r= number of responses

Organisational Similarities and Differences

For both organisations, the *majority of respondents expressed composite anger*, mainly frustration for organisation 1, and anger for organisation 2. There were more people expressing composite anxiety for this type of spam, with higher levels in organisation 2. Of some concern may be that 2 respondents in organisation 1 *liked* to receive this spam!

Gender Similarities and Differences

Response	Org1			Org2		
	Male	Female	Ratio	Male	Female	Ratio
Angry	18.4%	21.1%	1:1.1	32.1%	25.0%	1.3:1
Frustrated	21.1%	31.6%	1:1.5	7.1%	14.3%	1:2
Disgusted	2.6%	9.2%	1:3.5	0%	7.1%	~
Don't Care	14.5%	6.6%	2.2:1	14.3%	14.3%	1:1

Slightly more women expressed anger in organisation 1, whereas slightly more men did so in organisation 2. In both organisations *women were more frustrated or disgusted by it than men*. More men than women didn't care in organisation 1, but in organisation 2 the respondents who didn't care were evenly divided between genders.

Table 47***Selling Other General Products/Services (RQ2, RQ3)***

	Org1 (N=78)			Org2 (N=30)		
	Male (N _r =41)	Female (N _r =47)	Total (N _r =88)	Male (N _r =17)	Female (N _r =16)	Total (N _r =33)
	%	%	%	%	%	%
Like it	.0	.0	.0	.0	.0	.0
Happy	.0	.0	.0	3.3	.0	3.3
Angry	10.3	9.0	19.2	3.3	20.0	23.3
Frustrated	16.7	34.6	51.3	13.3	13.3	26.7
Disgusted	1.3	.0	1.3	3.3	.0	3.3
Worried	.0	1.3	1.3	.0	.0	.0
Embarrassed	1.3	.0	1.3	.0	.0	.0
Don't Care	23.1	15.4	38.5	33.3	20.0	53.3
Total (N%)	47.4	52.6	100.0	53.3	46.7	100.0

Note 1. In multiple-response question: N=number of respondents, N_r= number of responses

Organisational Similarities and Differences

The majority of respondents in organisation 1 expressed composite anger, particularly frustration, whereas the majority in organisation 2 didn't care about spam selling other general types of products and services. *One respondent in organisation 2 liked it.*

Gender Similarities and Differences

Response	Org1			Org2		
	Male	Female	Ratio	Male	Female	Ratio
Angry	10.3%	9.0%	1.1:1	3.3%	20.0%	1:6.1
Frustrated	16.7%	34.6%	1:2.1	13.3%	13.3%	1:1
Disgusted	1.3%	0%	~	3.3%	0%	~
Don't Care	23.1%	15.4%	1.5:1	33.3%	20.0%	1.7:1

Men and women were about equally angry in organisation 1, but in organisation 2 more women expressed anger than men. *Women in organisation 1 expressed more frustration than men, but in organisation 2 they were evenly divided.* In both organisations, *more men than women didn't care about spam selling general products and services.*

Table 48***Spam in General (RQ2, RQ3)***

	Org1 (N=83)			Org2 (N=31)		
	Male (N _r =54)	Female (N _r =54)	Total (N _r =108)	Male (N _r =20)	Female (N _r =26)	Total (N _r =46)
	%	%	%	%	%	%
Like it	.0	.0	.0	.0	.0	.0
Happy	.0	.0	.0	.0	.0	.0
Angry	19.3	14.5	33.7	9.7	19.4	29.0
Frustrated	33.7	42.2	75.9	25.8	32.3	58.1
Disgusted	2.4	1.2	3.6	6.5	9.7	16.1
Worried	2.4	2.4	4.8	6.5	6.5	12.9
Embarrassed	1.2	.0	1.2	.0	6.5	6.5
Don't Care	6.0	4.8	10.8	16.1	9.7	25.8
Total (N%)	47.0	53.0	100.0	51.6	48.4	100.0

Note 1. In multiple-response question: N=number of respondents, N_r= number of responses

Organisational Similarities and Differences

For both organisations, *a clear majority expressed composite anger about spam in general, with the highest percentage feeling frustrated about it (75.9% and 58.1% respectively), and the next highest percentage feeling angry about it.* Smaller percentages from each organisation (10.8% and 25.8% respectively) don't care about spam generally, but a small percentage from each organisation also expressed some composite anxiety about it.

Gender Similarities and Differences

Response	Org1			Org2		
	Male	Female	Ratio	Male	Female	Ratio
Angry	19.3%	14.5%	1.3:1	9.7%	19.4%	1:2
Frustrated	33.7%	42.2%	1:1.3	25.8%	32.3%	1:1.3
Disgusted	2.4%	1.2%	2:1	6.5%	9.7%	1:1.5
Don't Care	6.0%	4.8%	1.3:1	16.1%	9.7%	1.7:1

Men from organisation 1 and women from organisation 2 expressed more anger about it than their opposite gender. In both organisations, *women were more frustrated by it than men*, and slightly more men than women don't care about it.

When I Receive Spam...**Table 49*****It is a Waste of my Time at Work (RQ2, RQ3)***

	Org1 (N=83)			Org2 (N=31)		
	Male	Female	Total	Male	Female	Total
	%	%	%	%	%	%
Strongly Agree	27.7	39.8	67.5	25.8	25.8	51.6
Agree	16.9	12.0	28.9	22.6	19.4	41.9
Neutral	1.2	1.2	2.4	.0	.0	.0
Disagree	.0	1.2	1.2	3.2	3.2	6.5
Strongly Disagree	.0	.0	.0	.0	.0	.0
Total	45.8	54.2	100.0	51.6	48.4	100.0

Almost all agree that receiving spam is a waste of their time at work

A clear majority of respondents from both organisations (96.4% and 93.5% respectively) agree that spam wastes their time at work.

Three respondents, however, did not believe it wasted their time at work. After cross-checking their reported spam per day, they were all receiving minimal amounts, with 1 respondent receiving about 1.3 spam per day, and the other 2 respondents less than 1 spam per day, so because of these very low levels, they may have considered that it had very little impact on their work time.

Only 2 respondents, both from organisation 1, were neutral or undecided about this statement, so the strong agreement with this statement from respondents at both organisations shows that most are well aware of the disruption that spam causes to their work.

Table 50***I Worry that Fellow Employees Might see it (RQ2, RQ3)***

	Org1 (N=82)			Org2 (N=31)		
	Male	Female	Total	Male	Female	Total
	%	%	%	%	%	%
Strongly Agree	3.7	2.4	6.1	3.2	3.2	6.5
Agree	1.2	2.4	3.7	12.9	3.2	16.1
Neutral	15.9	22.0	37.8	12.9	25.8	38.7
Disagree	17.1	18.3	35.4	12.9	9.7	22.6
Strongly Disagree	8.5	8.5	17.1	9.7	6.5	16.1
Total	46.3	53.7	100.0	51.6	48.4	100.0

Most respondents were not worried fellow employees might see it

More than half of the respondents from organisation 1 (52.5%) and more than one in three respondents from organisation 2 (38.7%) were not worried that fellow employees might see the spam they received. This result could have at least two possible interpretations:

- A degree of knowledge about the origins of spam, and confidence their fellow employees are also aware of it
- They just don't care about it

More than one in three respondents from both organisations (37.8% and 38.7% respectively) were undecided about whether they were worried or not, for reasons unknown.

Some respondents were worried

About one in ten from organisation 1 and more than one in five from organisation 2 (9.8% and 22.6% respectively) agreed that they were worried about it.

As low as these figures may be, it does indicate that there are measurable levels of anxiety amongst employees, who may be concerned about what others may think about the spam they receive, and why they may be receiving it.

Table 51***It Makes me Angry (RQ2, RQ3)***

	Org1 (N=81)			Org2 (N=31)		
	Male	Female	Total	Male	Female	Total
	%	%	%	%	%	%
Strongly Agree	11.1	13.6	24.7	6.5	19.4	25.8
Agree	16.0	22.2	38.3	12.9	9.7	22.6
Neutral	14.8	13.6	28.4	25.8	16.1	41.9
Disagree	3.7	4.9	8.6	6.5	3.2	9.7
Strongly Disagree	.0	.0	.0	.0	.0	.0
Total	45.7	54.3	100.0	51.6	48.4	100.0

Spam does make most respondents angry

A majority of respondents from organisation 1, and almost half of the respondents in organisation 2 (63% and 48.4% respectively) get angry about spam.

The lower figure of agreement from organisation 2 respondents did not translate into definite disagreement with the statement, but instead resulted in a higher degree of neutrality or indecision about whether it made them angry.

Women more angry about spam than men

Comparing the gender differences for this question shows that similar to the previous questions about how respondents feel about specific types of spam, where men typically expressed how they felt about the different types of spam as “don’t care”, women also appear to be proportionally slightly angrier than men about receiving spam.

Table 52***I Enjoy Receiving it (RQ2, RQ3)***

	Org1 (N=82)			Org2 (N=31)		
	Male	Female	Total	Male	Female	Total
	%	%	%	%	%	%
Strongly Agree	.0	.0	.0	.0	.0	.0
Agree	1.2	.0	1.2	6.5	.0	6.5
Neutral	.0	1.2	1.2	3.2	6.5	9.7
Disagree	17.1	19.5	36.6	25.8	12.9	38.7
Strongly Disagree	28.0	32.9	61.0	16.1	29.0	45.2
Total	46.3	53.7	100.0	51.6	48.4	100.0

Most respondents do not enjoy receiving spam, but some men do!

A clear majority of respondents from both organisations disagreed that they enjoy receiving spam (97.6% and 83.9% respectively).

However, 1 respondent from organisation 1 and several from organisation 2 agreed that *they do enjoy receiving spam!* These respondents were *all men*.

Responses to the previous questions about the different types of spam indicated that there were particular types of spam that some respondents *liked* to receive, e.g. online casinos, dating websites, job/employment offers etc, so this result is not unexpected.

Table 53***It is an Intrusion on my Privacy (RQ2, RQ3)***

	Org1 (N=83)			Org2 (N=31)		
	Male	Female	Total	Male	Female	Total
	%	%	%	%	%	%
Strongly Agree	15.7	16.9	32.5	9.7	12.9	22.6
Agree	16.9	20.5	37.3	25.8	19.4	45.2
Neutral	12.0	8.4	20.5	9.7	6.5	16.1
Disagree	1.2	2.4	3.6	3.2	3.2	6.5
Strongly Disagree	.0	6.0	6.0	3.2	6.5	9.7
Total	45.8	54.2	100.0	51.6	48.4	100.0

Many respondents believe spam is an intrusion on their privacy

A majority of respondents from both organisations agreed that spam is an intrusion on their privacy (69.8% and 67.8% respectively).

However, a small percentage of respondents from each organisation disagree that it is (9.6% and 16.2% respectively), with more women than men in disagreement.

If those in disagreement had been all or mostly men, then this result may have been explainable due to previous responses indicating that some men like receiving spam, and may therefore not regard them as an intrusion on their privacy. However, as more women disagreed, this result is unexplainable without further research.

Table 54***I Delete them Immediately (RQ2, RQ3)***

	Org1 (N=83)			Org2 (N=31)		
	Male	Female	Total	Male	Female	Total
	%	%	%	%	%	%
Strongly Agree	32.5	42.2	74.7	16.1	29.0	45.2
Agree	9.6	9.6	19.3	35.5	9.7	45.2
Neutral	1.2	.0	1.2	.0	6.5	6.5
Disagree	1.2	1.2	2.4	.0	.0	.0
Strongly Disagree	1.2	1.2	2.4	.0	3.2	3.2
Total	45.8	54.2	100.0	51.6	48.4	100.0

Almost all respondents delete spam immediately

A clear majority of respondents from both organisations agreed that they delete the spam they receive immediately (94% and 90.4% respectively).

This will help the IT departments at each organisation in respect of keeping email storage requirements under control, but only if the Trash is regularly emptied.

Potential problems with false-positives

A negative impact to this practice occurs if the “spam” deleted actually happens to be a false-positive, which a number of respondents have commented about, and which one interview participant stated had happened with a customer order, which fortunately was successfully recovered from the Trash, as it had not been emptied.

Table 55***They are Sometimes Interesting to read (RQ2, RQ3)***

	Org1 (N=82)			Org2 (N=31)		
	Male	Female	Total	Male	Female	Total
	%	%	%	%	%	%
Strongly Agree	1.2	.0	1.2	.0	3.2	3.2
Agree	1.2	1.2	2.4	6.5	9.7	16.1
Neutral	6.1	2.4	8.5	9.7	3.2	12.9
Disagree	13.4	25.6	39.0	25.8	9.7	35.5
Strongly Disagree	24.4	24.4	48.8	9.7	22.6	32.3
Total	46.3	53.7	100.0	51.6	48.4	100.0

Some respondents find spam interesting to read

The majority of respondents from both organisations do not find spam interesting to read (87.8% and 67.8% respectively), but a number of respondents agreed that it sometimes can be interesting to read.

As some respondents have previously indicated that they *like* to receive certain types of spam, it may also explain why some respondents to this question have also indicated they find it interesting to read. The comment of one respondent from organisation 1, in the question as to why they opened possible spam may also be a factor: “Spam is sometimes quite a laugh”. Most respondents who agreed with this question were from organisation 2.

Table 56*The email was sent by the Person it says it is "From:" (RQ2, RQ3)*

	Org1 (N=82)			Org2 (N=31)		
	Male	Female	Total	Male	Female	Total
	%	%	%	%	%	%
Strongly Agree	1.2	2.4	3.7	.0	6.5	6.5
Agree	3.7	8.5	12.2	9.7	16.1	25.8
Neutral	18.3	20.7	39.0	19.4	19.4	38.7
Disagree	11.0	3.7	14.6	12.9	3.2	16.1
Strongly Disagree	12.2	18.3	30.5	9.7	3.2	12.9
Total	46.3	53.7	100.0	51.6	48.4	100.0

Many respondents unsure who spam is "From:"

Almost two out of five respondents from both organisations (39% and 38.7% respectively) chose "neutral" as their answer, which is almost the majority of respondents in organisation 1, and was the majority of respondents in organisation 2.

One of the most common features about spam is that it usually uses a false and often invalid "From:" or reply-to address, as:

...during the process of sending spam, any reply address can be specified in the message header, and only rarely does spam contain a legitimate or nonfalsified address.... More times than not, the person who appears to be sending the spam doesn't even exist.

(Spammer-X, 2004, p. 338)

The exception to these is usually the "Nigerian Fraud" spam, where the scammer actually *does* want the recipient to reply to them, as part of a bigger deception.

That the majority of respondents from both organisations either believe the sender is who they claim to be or are unsure (54.9% and 71% respectively) indicates that employees need more education about the deliberately deceptive nature of the spam they receive.

Table 57***I Sometimes Forward it on to Colleagues or Friends (RQ2, RQ3)***

	Org1 (N=81)			Org2 (N=31)		
	Male	Female	Total	Male	Female	Total
	%	%	%	%	%	%
Strongly Agree	.0	.0	.0	.0	.0	.0
Agree	.0	.0	.0	3.2	6.5	9.7
Neutral	1.2	.0	1.2	3.2	3.2	6.5
Disagree	8.6	9.9	18.5	22.6	6.5	29.0
Strongly Disagree	37.0	43.2	80.2	22.6	32.3	54.8
Total	46.9	53.1	100.0	51.6	48.4	100.0

Very few respondents forward on spam

A clear majority of respondents from both organisations (98.7% and 83.8% respectively) do not forward on their spam to colleagues or friends.

Of the few who indicated they sometimes had, and while the actual reason is unknown from this survey, some possible reasons might be that the friends or colleagues:

- Had similar interests to the advertised products or services (casinos, dating etc)
- Were auto-forwarded by some sort of rule
- Might also consider that the spam was “quite a laugh”

Table 58***It Makes me Frustrated (RQ2, RQ3)***

	Org1 (N=83)			Org2 (N=31)		
	Male	Female	Total	Male	Female	Total
	%	%	%	%	%	%
Strongly Agree	22.9	33.7	56.6	12.9	25.8	38.7
Agree	19.3	14.5	33.7	19.4	16.1	35.5
Neutral	2.4	1.2	3.6	16.1	6.5	22.6
Disagree	1.2	1.2	2.4	3.2	.0	3.2
Strongly Disagree	.0	3.6	3.6	.0	.0	.0
Total	45.8	54.2	100.0	51.6	48.4	100.0

Spam frustrates the majority of respondents

A clear majority of respondents from both organisations (90.3% and 74.2% respectively) feel frustrated when they receive spam.

There appears to be very little gender difference for this general question however, compared to the previous questions about more specific types of spam, with both genders appearing to be approximately equally frustrated by spam for organisation 1, and women slightly more frustrated than men in organisation 2.

Table 59***I Believe they are Mostly Deceptive or Fraudulent (RQ2, RQ3)***

	Org1 (N=83)			Org2 (N=31)		
	Male	Female	Total	Male	Female	Total
	%	%	%	%	%	%
Strongly Agree	30.1	37.3	67.5	9.7	16.1	25.8
Agree	10.8	14.5	25.3	22.6	22.6	45.2
Neutral	4.8	2.4	7.2	12.9	6.5	19.4
Disagree	.0	.0	.0	6.5	3.2	9.7
Strongly Disagree	.0	.0	.0	.0	.0	.0
Total	45.8	54.2	100.0	51.6	48.4	100.0

Most respondents believe spam is deceptive or fraudulent

A clear majority of respondents from both organisations (92.8% and 71% respectively) believe that spam is mostly deceptive or fraudulent.

Since the majority, if not all of the spam industry is based on deception and fraud (e.g. fake sender addresses, trying to hide the email's true source, phishing, "Nigerian" scams etc), it is encouraging that most respondents also believe this to be true, with men and women in almost equal agreement.

Some respondents, however, were either not sure (neutral) or disagreed with this statement. Nearly one in five respondents from organisation 2 (19.4%) were not sure, and several respondents (two men and one woman) disagreed. One of these male respondents had also indicated in the previous questions about the various spam types that he liked to receive them. This attitude should be of some concern to organisations, and should ideally be countered with improved employee education about the nature of and risks associated with spam.

Table 60***I have Sometimes Replied to them (RQ2, RQ3)***

	Org1 (N=82)			Org2 (N=31)		
	Male	Female	Total	Male	Female	Total
	%	%	%	%	%	%
Strongly Agree	.0	.0	.0	.0	.0	.0
Agree	3.7	.0	3.7	.0	6.5	6.5
Neutral	1.2	.0	1.2	3.2	.0	3.2
Disagree	8.5	17.1	25.6	38.7	12.9	51.6
Strongly Disagree	31.7	37.8	69.5	9.7	29.0	38.7
Total	45.1	54.9	100.0	51.6	48.4	100.0

Most respondents have not replied to spam

A clear majority of respondents from both organisations (95.1% and 90.3% respectively) disagree that they have sometimes replied to spam.

Despite most email addresses being faked (with the exception of Nigerian scams, as mentioned before), there is still an element of risk involved in replying to a spam email, and if the spammer has faked a *real* email address, the reply will be sent to a completely innocent party.

Even worse, if the content of the spam is included in the reply, there is a risk that the person replying will trigger the recipient's anti-spam systems and result in their reply being submitted to anti-spam vendors or RBLs as spam.

Not replying is Rule 2 of InternetNZ's "Four Golden Rules" (InternetNZ, 2006a), and although only a few respondents have replied at some time, the response suggests further reminders to employees about never doing so may be necessary.

Table 61***I Sometimes Report it to my Manager or IT Dept (RQ2, RQ3)***

	Org1 (N=81)			Org2 (N=31)		
	Male	Female	Total	Male	Female	Total
	%	%	%	%	%	%
Strongly Agree	9.9	14.8	24.7	3.2	6.5	9.7
Agree	21.0	22.2	43.2	16.1	16.1	32.3
Neutral	7.4	7.4	14.8	9.7	12.9	22.6
Disagree	4.9	8.6	13.6	19.4	9.7	29.0
Strongly Disagree	2.5	1.2	3.7	3.2	3.2	6.5
Total	45.7	54.3	100.0	51.6	48.4	100.0

Many respondents have reported spam to their manager or the IT Department

Respondents from both organisations (67.9% and 42% respectively) are reporting spam they receive.

Organisation 1 provides a public folder for employees to forward spam to, and interview participants from organisation 2 indicated they have also forwarded spam to the IT Department, so both organisations provide some sort of mechanism for employees to report spam that has slipped through the filters, and the response to this question shows that employees are doing this to some degree.

Table 62***I Sometimes find the Content of the Email is Objectionable (RQ2, RQ3)***

	Org1 (N=83)			Org2 (N=31)		
	Male	Female	Total	Male	Female	Total
	%	%	%	%	%	%
Strongly Agree	12.0	18.1	30.1	9.7	9.7	19.4
Agree	14.5	20.5	34.9	22.6	22.6	45.2
Neutral	16.9	13.3	30.1	12.9	12.9	25.8
Disagree	2.4	2.4	4.8	6.5	3.2	9.7
Strongly Disagree	.0	.0	.0	.0	.0	.0
Total	45.8	54.2	100.0	51.6	48.4	100.0

Many respondents have received spam with objectionable content

A majority of respondents from both organisations (65% and 64.6% respectively) have received spam with objectionable content.

In organisation 1 a higher proportion of women than men had received objectionable content, whereas proportions were about equal for organisation 2.

Although what people find “objectionable” is subjective, in the survey results on how respondents feel about specific types of spam they have received, the highest number of “disgusted” responses were received for spam of a sexual nature, i.e. sexual performance drugs, male enhancement products, adult and child pornography websites.

The highest percentages of “disgusted” responses (69.6% and 77.8% respectively) were recorded by those who had received spam relating to child pornography.

Table 63***I am Concerned I Might Accidentally Delete good Emails with spam (RQ2, RQ3)***

	Org1 (N=83)			Org2 (N=31)		
	Male	Female	Total	Male	Female	Total
	%	%	%	%	%	%
Strongly Agree	1.2	16.9	18.1	6.5	12.9	19.4
Agree	26.5	18.1	44.6	22.6	22.6	45.2
Neutral	10.8	8.4	19.3	9.7	3.2	12.9
Disagree	4.8	9.6	14.5	9.7	6.5	16.1
Strongly Disagree	2.4	1.2	3.6	3.2	3.2	6.5
Total	45.8	54.2	100.0	51.6	48.4	100.0

Most respondents are concerned about accidentally deleting good emails

A majority of respondents from both organisations (62.7% and 64.6% respectively) are concerned they might accidentally delete good emails when deleting spam. Slightly more women than men were concerned about it.

During the interviews with participants from each organisation, two participants who were specifically asked whether they had, indicated they had accidentally deleted either a customer order or a customer enquiry when deleting spam.

The indication was that this had either occurred because the email was a false-positive and had been tagged as spam, or else it was because there were a number of spam emails on either side of it and it was accidentally selected for deletion along with them.

Although about one in five (18.1% and 22.6% respectively) were not concerned, this is nevertheless a serious issue that affects organisations who use email as a main method of communication within their business.

Table 64***I wish the IT Dept would do more to stop it (RQ2, RQ3)***

	Org1 (N=83)			Org2 (N=31)		
	Male	Female	Total	Male	Female	Total
	%	%	%	%	%	%
Strongly Agree	7.2	10.8	18.1	.0	6.5	6.5
Agree	18.1	22.9	41.0	19.4	16.1	35.5
Neutral	18.1	16.9	34.9	12.9	19.4	32.3
Disagree	2.4	3.6	6.0	19.4	6.5	25.8
Strongly Disagree	.0	.0	.0	.0	.0	.0
Total	45.8	54.2	100.0	51.6	48.4	100.0

Many respondents want their IT Departments to do more to stop spam

Not surprisingly, many respondents from both organisations (59.1% and 42% respectively) would like their IT Department to do more to stop spam.

Surprisingly, a small percentage of respondents from organisation 1 and one in four respondents from organisation 2 (6% and 25% respectively) *did not* wish their IT Department would do more to stop it.

About one in three respondents from each organisation (34.9% and 32.3% respectively) were undecided or had no opinion about this.

Table 65***I am Worried I am Receiving it Because I may have Accidentally Visited a Website with Similar Content (RQ2, RQ3)***

	Org1 (N=81)			Org2 (N=31)		
	Male	Female	Total	Male	Female	Total
	%	%	%	%	%	%
Strongly Agree	2.5	6.2	8.6	3.2	3.2	6.5
Agree	7.4	7.4	14.8	12.9	12.9	25.8
Neutral	13.6	9.9	23.5	9.7	12.9	22.6
Disagree	17.3	21.0	38.3	19.4	12.9	32.3
Strongly Disagree	4.9	9.9	14.8	6.5	6.5	12.9
Total	45.7	54.3	100.0	51.6	48.4	100.0

Most respondents are *not* worried they are receiving spam because of accidentally visiting a website with similar content

A small majority of respondents from both organisations (53.1% and 45.2% respectively) do not believe they are receiving spam as the result of accidentally visiting a website.

This may be because they know they have not visited a similar website, or they know that spammers employ a wide variety of techniques to harvest addresses, and usually tend to spam indiscriminately to lists they have harvested or purchased.

Despite this, there were a high proportion of respondents from both organisations (23.4% and 32.3% respectively) who *are* worried that this is the reason they are receiving certain types of spam.

About one in five from each organisation (23.5% and 22.6% respectively) was not sure.

Further education about how spammers get their email addresses may help alleviate employee concerns regarding this belief.

Table 66***I Hate Receiving it (RQ2, RQ3)***

	Org1 (N=83)			Org2 (N=31)		
	Male	Female	Total	Male	Female	Total
	%	%	%	%	%	%
Strongly Agree	18.1	30.1	48.2	9.7	25.8	35.5
Agree	18.1	15.7	33.7	25.8	12.9	38.7
Neutral	9.6	7.2	16.9	12.9	6.5	19.4
Disagree	.0	1.2	1.2	3.2	3.2	6.5
Strongly Disagree	.0	.0	.0	.0	.0	.0
Total	45.8	54.2	100.0	51.6	48.4	100.0

The majority of respondents hate receiving spam

A clear majority of respondents from each organisation (81.9% and 74.2% respectively) agreed that they hate receiving spam.

Less than one in five (16.9% and 19.4% respectively) were neutral or had no strong feelings about this, so possibly didn't care, and only a few respondents disagreed.

Of note for this result is that a much higher proportion of respondents than usual in each organisation chose to "Strongly Agree" with this statement, which is indicative that there is a greater depth of feeling associated with this statement, and a greater proportion of women than men chose this option.

Table 67***I Worry my Colleagues or Manager Might see me Reading it, if it is Objectionable Content (RQ2, RQ3)***

	Org1 (N=83)			Org2 (N=31)		
	Male	Female	Total	Male	Female	Total
	%	%	%	%	%	%
Strongly Agree	1.2	4.8	6.0	.0	9.7	9.7
Agree	4.8	6.0	10.8	9.7	3.2	12.9
Neutral	14.5	19.3	33.7	19.4	22.6	41.9
Disagree	16.9	15.7	32.5	19.4	9.7	29.0
Strongly Disagree	8.4	8.4	16.9	3.2	3.2	6.5
Total	45.8	54.2	100.0	51.6	48.4	100.0

Most Respondents not worried they might be seen reading spam with objectionable content

This question was highly speculative, as the respondents may never have been in the proposed situation of having opened a spam email with objectionable content, and had a colleague or manager observe them do so. The purpose was to try and gauge any levels of anxiety the respondents might have about being placed in such a situation.

Although many respondents chose the neutral option (33.7% and 41.9% respectively), probably because they were undecided how they might feel, most other respondents decided they would not be worried (49.4% and 35.5% respectively).

This result could be interpreted that many employees understand that receiving a certain type of spam does not mean they asked for it (it was unsolicited), and they have the expectation that others understand this also.

About one on five respondents from each organisation (16.8% and 22.6% respectively) were worried, with women slightly more worried than men, which may indicate a need for further education and reassurance by employers.

Table 68

Final Respondent Comments from Org1 (RQ2)

Org1	I get only occasional spam via my (<i>work*</i>) email address...would be good to have an easy way to notify IT about it as it usually sits in my Junk email box with me not knowing where to direct it
	No SPAM at work, but am receiving about 20 a day on my home email account - managed by XTRA.
	In the interests of preventing false positives my organisation chooses to have more relaxed spam filtering leading to more spam getting in - frustrating.
	Spam is all shit and doesn't work for the spammers so why bother, plus I think IT could do more to stop it coming into my inbox!
	I think I've only had about 3 spam emails in the 7 months I've been here.
	Spam is a pain, and was a complete pain when lhug went down due to spam. Due to their inability to deal with it. I still haven't received emails people had said they sent to me.
	It interrupts your train of thought and wastes time. It raises concerns about the safety of our company and personal information that is stored on company servers.
	It's really annoying in general and it loses you time and if I accidentally happen to open one e.g. Job opportunity!! I know this is all fake and would never follow these things up! This stupid Spam needs to be stopped.
	Thanks for this. I think you have omitted one emotion and that is "bewildered". Most of the spam I receive is indecipherable, with weird references to the bible, sometimes codes and bizarre subject lines. These do not embarrass, or worry me particularly, nor do they make me angry... they just make no sense and I wonder who came up with them, and why?? The "science of spam" is actually quite fascinating... but I would still rather do without it!!
	Many emails are in foreign languages and or look corrupt and/or unreadable
	IT'S AN INVASION OF PERSONAL SPACE AND IT IS DELIBERATELY MISLEADING. OUR IT TEAM AREN'T AT FAULT. PEOPLE WITHIN THE SPAM INDUSTRY ARE OBVIOUSLY CLUED UP ON WHAT THEY DO AND ALWAYS TRY TO STAY ONE STEP AHEAD. THERE NEEDS TO BE MORE INTERNATIONAL PRESSURE, BETTER TRACKING OF WHERE IT'S COMING FROM AND HARSHER PENALTIES. ALSO BETTER EDUCATION ON NOT RESPONDING TO IT.
	They really annoy me, it is so time consuming, I forward them to our IT Dept then delete straight away. I spend enough time clearing legitimate emails without receiving all this garbage and it concerns me that I don't know how they get my email address
	Nervous about the possibility of virus / tracking / ongoing distribution of email. Delete it before it does anything to my system.
	I don't really care about SPAM. I just accept that it is a part of having an email account. I always ignore it.
	Spam is an incredible waste of time - I never read them once I identify they are "spam"
	Spammers should be prosecuted!!
	People who send spam need their heads looked at!

I answered this survey based on my work email address. I also have my own website which has a catch all email address attached to it. I will delete anywhere from 10 to 100 emails 2 to 5 times a day. Thank you for the survey and good luck.

SOME OF YOUR QUESTIONS HAVE STRONG EMOTIONS ATTACHED TO THE ANSWERS. SPAM IS ANNOYING, BUT NOT ENOUGH FOR ME TO DWELL ON IT OR SEEK PSYCHIATRIC HELP

I have had spam emails in the past on personal email accounts, but never any on a work email account. I don't really have a problem with spam emails as they are quite easy to block, and identifying then deleting them does not use up much time or effort. Hope my answers to this survey helped. :)

It's a pain in the you know what, I understand our IT dept stop hundreds of these things each day.....it's almost a part of our daily lives now when using email.....

Frustration is probably caused more by the waste of time it takes everyone to prevent, monitor and delete spam. Not to mention trying to decide exactly what spam emails are (and telling that to an automated blocking filter!)

I find it annoying more than anything else. I never open them in case they link to sites that contain viruses or encourage the spammer to continue to send spam. It is another unfortunate timewaster and misuse of a great work tool.

On a lot of the questions about how it makes me feel, I hit frustrated and don't care. I realise this is somewhat of an oxymoron, but what I meant by that was, although it is annoying, I don't really care too much - it doesn't really affect my life. The only thing I worry about is whether it has viruses etc and if it could potentially crash my computer or allow others to see my personal details. Thank you for your work on this

In general, spam at my workplace is not an issue for me...As indicated...I only receive an average 5 or 6 a week, easily identified and deleted...therefore I can afford to be apathetic and tolerant.

It would be great not receive anymore scam emails.

My mailbox on this domain has only been active a month, and I have no business cards. There is little chance this address would have found its way to any SPAM database as of yet.

Who really opens spam reads it and believes it. That's crap - everyone in our building deals with spam it's not an issue cause who reads it?? Not me. It's frustrating that we have to deal with it - and IT should do more to cut it out.

It's definitely an issue... but I realise there's no simple answer except to reintroduce hanging for spamming.

I don't feel that passionate about spam, it is annoying but doesn't really impact my work duties.

The amount of spam that our office has received in the past few months has increased 10 fold. I honestly don't remember getting any spam a year ago but the past few months it has been crazy! It was reported to our IT department and they have done a good job so far as we aren't getting as much but we are still getting at least a couple a day. It's annoying and a complete waste of my time.

My main personal concern is that they waste time. For others I worry that they will get caught out by phishing emails or the ones that say "your order has been processed" or to that effect so that people will think I didn't order that, and click on the link.

Basically it is a pain in the **** and it would be great if there was a way of stopping it

Table 69

Final Respondent Comments from Org2 (RQ2)

Org2	I have never had a problem with spam in my work email account. The one irritating problem is that ordinary emails often get blocked as spam.
	I think spam was created by computer companies so they could develop software to generate revenue.
	I only get 4/5 a day, mostly ones that don't make sense, so its not hard to deal with them
	The only problem I have is that the company block about every e-mail even if it is business related. Spam filters are good in the use of real spam and not on work related matter.
	I really don't like to receive any spam at all it is a total waste of time. If I want a product or service I will do the research myself.
	I actually had help from IT set up a junk mail box for spam to go into directly so I don't receive in my main inbox which means I don't have to go through and delete everyday, maybe everyone in company set 1 up at least it is separated until IT can work out how to divert before it gets to us.
	The only spam received by me is the occasional joke or email from someone known to me. No advertising etc
	Since switching to (<i>new domain*</i>) address from (<i>old domain*</i>) address, SPAM has decreased considerably. Used to receive upwards of 140 a week.
	It is more frustrating when - not only do I receive my own spam emails but I also receive spam auto forwarded from other workmates email accounts when on leave or away.
	Spam is like junk mail through the letter box at home - totally unsolicited, we provide our letter boxes at home for the use of the Official Postal system, and not the junk. Likewise, the Company provides e-mail to service its business functions and not to have its employee's attention diverted by junk.
	Receiving SPAM is time consuming, and I feel that it also affects your purpose of any person's job. Any and all companies are trying to run a business and make money, and this can't happen when there are un-necessary emails coming through all the time. If on an occasional basis a SPAM email pops up, that I feel is generally OK, but to have to deal with them all the time is a waste of my time, and company time!!!
	In the workplace we should be able to accept e-mails from people in our contact list. At present even most of these are labelled Spam when in fact they are just something passed on - not to be confused with chain letters. We should have the option to accept e-mails from these people if we choose
	Spam mails are a real pain. You have to spend time in the mornings deleting them and there is always a chance they contain virus's It would be great if spam mail could be stopped completely.

Note 1. Final comments have been edited for spelling or to protect anonymity

Table 70***Thematic analysis of respondent's final comments (RQ2)***

Theme	Org1	Org2	Total
Spam wastes time	8	3	11
Spam frustrating	7	1	8
Spam annoying	6	0	6
Don't care about spam	6	0	6
Security concerns about spam	3	1	4
False positives a problem	0	4	4
Concerned about invasion of privacy of personal information	4	0	4
Spam a misuse of email	1	2	3
Receive very little spam	1	2	3
Believes spam is deceitful	3	0	3
Wants legal action to try to stop spam	3	0	3
IT should do more to stop spam	2	0	2
Spam needs to be stopped	1	1	2
Wants scam emails stopped	2	0	2
Spam a distraction	1	1	2
Deletes spam	2	0	2
Spam contents bewildering (foreign language or random text)	2	0	2
Doesn't receive any spam at work	2	0	2

Note 1. Only comments with more than one response are shown

Majority believe spam wastes time and is frustrating or annoying

In their final comments before exiting the survey, the majority of respondents believe that spam is a waste of time, and that it is frustrating or annoying for them.

From the remainder, many didn't really care about spam, but others had concerns about security, privacy and the number of false positives.

A number of respondents stated that spam and scam emails should be stopped, that legal action should be used to stop it, or that their IT department should do more to stop it.

A few also believe that spam is a misuse of email, is deceitful, or is a distraction at work.

Some also receive very little or no spam at work.

Finally, two respondents found the contents of the spam to be somewhat bewildering, containing either random text or in a foreign language.

4.5 Analysis of Employee Interviews (RQ2)

Table 71

Gender

	Org1	Org2	Total
Male	2	1	3
Female	2	3	5

Q1 What do you know about Unsolicited Bulk Emails

Table 72

Q1.a Have you read, heard or seen much about UBE (spam) in the media?

	Org1	Org2	Total
Yes	4	2	6
No	0	2	2

Table 73

Where have you read, heard or seen much about spam in the media?

Participant has:	Org1	Org2	Total
Heard about spam in Print media	2	1	3
Been advised about spam by ISP	2	0	2
Seen an item about spam on TV	1	0	1
Been warned about spam through faxes	0	1	1

Table 74

Q1.b Has your organisation provided you with any information about UBE?

	Org1	Org2	Total
Yes	3	2	5
No	1	2	3

Table 75***Q1.c What sort of information has the organisation provided?***

Organisation (IT department):	Org1	Org2	Total
Sends spam alerts	1	2	3
Has given general (non-specified) information	0	2	2
Advised what to do with spam	1	1	2
Advised IT is working hard to stop spam	1	0	1
Advised them to delete spam	1	0	1
Sent emails to advise about spam	0	1	1
Uses the Intranet to advise about spam	0	1	1
Has not given much information	1	0	1
Assumes they already know about	1	0	1

Table 76***Q1.d How do you think the spammers got your email address?***

Spammers got their address because:	Org1	Org2	Total
Their generic email address attracts spam	1	2	3
It was from an auto-reply	0	1	1
It was harvested from external email contacts	1	0	1
They visited a website	1	0	1
It is on external databases	1	0	1
It is on organisational website	1	0	1
They made bookings with an overseas company	0	1	1
Don't know how they get address	0	1	1

Most participants had read or heard something about spam in the media or been advised by their own personal ISP about it, and more than half had received some sort of information from the organisation, mainly spam alerts and advice on what to do with it. Having a generic email address was the most popular reason for how spammers found their address.

Q2 What can you tell me about the Unsolicited Bulk Emails you receive**Q2.a Which of the following types of UBE have you received in the past?****Table 77*****Types of spam received by participant in the past (RQ2, RQ3)***

	Gender		Total
	Male	Female	
Sexual Performance Drugs (Viagra, Cialis etc)	3	5	8
"Nigerian" Fraud	2	4	6
Male Enhancement/Enlargement Products	3	2	5
Online Casino Websites	1	4	5
Selling Cheap Software	0	4	4
Mortgage/Loan Financing	1	3	4
Stock Market "Tips"	1	3	4
Selling Other General Products/Services	1	3	4
Weight Loss Drugs/Programmes	0	3	3
Job/Employment Offers	2	1	3
Dating Websites	0	2	2
Child Pornography Websites	0	1	1
Adult Pornography Websites	1	0	1

Note 1. As participant numbers were small, frequency counts are by gender only

Note 2. Spam types rearranged from original in order of total frequency, highest to lowest

Table 78***Q2.b Has the amount of UBE you receive increased or decreased in the past 12 months?***

Spam has in the past 12 months:	Org1	Org2	Total
Decreased	1	1	2
Remained about the same	0	0	0
Increased	3	3	6

All participants had received spam about sexual performance drugs at some time, and more than half had received "Nigerian" fraud, male enhancement/enlargement product and online casino spam. Exactly half, the majority of who were the women participants had received software, mortgage/loan, stock market, and other general types of spam.

Q3 How do you feel about Unsolicited Bulk Emails

Q3.a What emotions from the following list best describe how you feel about each type of UBE you have received?

Table 79

How participants feel about the UBE they receive

UBE Type	Composite Positive		Composite Anger		Composite Anxiety		D.C.		P.O.	
	M	F	M	F	M	F	M	F	M	F
Selling Cheap Software				2		1		2		
Sexual Performance Drugs			1	3			2	2		1
Weight Loss Drugs/Programmes				1				3		
Male Enhancement/Enlargement Products			1	2			2			1
Mortgage/Loan Financing				1		1		2		
Job/Employment Offers			1				1	1		
Adult Pornography Websites							1			
Child Pornography Websites										1
Dating Websites				1				1		
Stock Market "Tips"			1	2				2		
Online Casino Websites				2		1	1	1		
"Nigerian" Fraud			1	2		1	1	1		1
Selling Other General Products/Services				1		1		1		
Spam in General?			2	3						2
Total by Gender			7	20	1	5	7	16		6
Total by Composite Emotion			27		6		23		6	

Note 1. M=Male, F=Female, D.C.=Don't Care, P.O.=Particularly Offensive

Female participants seemed to receive a wider range of spam than males, often seven or eight types, compared to the males who received only four or five types, and they were most often angry or frustrated by it, and/or didn't care about it, as shown by the high scores in the female column for the composite anger and "don't care" responses.

Q3.b If you found any of the unsolicited emails you received offensive or objectionable, have you ever opened any of these emails when your work colleague(s) or manager(s) were present, or able to see your computer screen?

None of the 8 participants had ever had this situation occur

Q3.c If so, how did you feel in this situation?

Not Applicable

Table 80

Q3.d If not, how do you think you might feel in that situation?

Participant felt that:	Org1	Org2	Total
Offensive emails would cause embarrassment	2	3	5
Offensive emails would cause anger	0	1	1
Offensive emails would cause disgust	1	0	1
Offensive emails would cause distress	1	0	1
They would be offended at opening offensive emails	0	1	1
Management should be understanding about it	1	1	2
People might think I'm surfing offensive sites	1	0	1
They were concerned IT Dept would find out	1	0	1
They weren't worried about opening offensive emails	0	1	1

Q4 What do you do with Unsolicited Bulk Emails

Q4.a For any of the unsolicited emails you indicated you have received that requested you provide login/password information for a bank or other online financial website, have you:

Table 81

Q4.a.i Ever clicked on the link provided in the email?

	Org1	Org2	Total
Never received one	0	2	2
Yes	0	0	0
No	4	2	6

Q4.a.ii Ever entered your login ID and password?

Not applicable

Table 82

Q4.b For any other non-financial unsolicited emails, have you ever clicked on any links included in unsolicited emails you have received?

	Org1	Org2	Total
Yes	1	1	2
No	3	3	6

Table 83

Q4.c If “Yes”, what was the reason you clicked on it?

Participant clicked on the link:	Org1	Org2	Total
For weight loss drugs or programme information	0	1	1
Thinking it was from someone in same business	1	0	1

Q4.d Have you at any time ever purchased any products or services offered in an unsolicited email?

None of the participants had ever purchased any products or services from spam

Table 84

Q4.e What do you normally do with the unsolicited emails you receive?

Participant normally:	Org1	Org2	Total
Deletes spam emails received	4	3	7
Forwards spam to the IT Dept	3	2	5

From Q3.d, Table 80, the majority of participants believed their response would be anxiety (embarrassed, distressed) if they opened an offensive email with someone else present.

One participant confessed to deliberately clicking on links in the messages for weight loss spam, but most participants delete and/or forward their spam to the IT department.

Q5 What are your opinions about Unsolicited Bulk Emails

Q5.a Do you think that unsolicited emails waste your time at work?

All participants agreed that spam wastes their time at work

Q5.b Do you think they are a waste of your organisation's time and money?

All participants agreed that spam is a waste of their organisation's time and money

Table 85

Q5.c How well do you think your organisation is doing in controlling the amount of unsolicited email that you receive?

The organisation (IT department) is doing:	Org1	Org2	Total
A good job	0	3	3
The best they can do to stop spam	3	0	3
A poor job controlling spam at the moment	1	1	2

Table 86

Q5.d Do you think more could be done by your organisation to control unsolicited email?

Participant believes:	Org1	Org2	Total
Yes, IT could do more to control spam	1	2	3
Not much more can be done by IT to control spam	3	0	3
They don't know what more could be done to control spam	0	2	2

The majority of participants thought that their organisation was doing a good job or the best they could in controlling spam, but 1 respondent from each organisation thought they were doing a poor job.

Several participants thought that more could be done to control spam, but the majority thought not much more could be done or else didn't know.

Table 87*Q5.e If “Yes”, what more do you think they could do to control it?*

Suggested that the organisation (IT department) could:	Org1	Org2	Total
Delete obvious spam, don't tag it and send it through	0	2	2
Increase the spam threshold level	1	0	1
Trade-off increase in false-positives for reduction in spam volume	1	0	1

Table 88*Q5.f Do you think your organisation could provide you with more information about unsolicited email?*

	Org1	Org2	Total
Yes	1	0	1
No	3	4	7

Table 89*Q5.g If “Yes”, what information do you think they should provide? (NB: some suggestions came from other interview questions)*

The organisation (IT department) should provide:	Org1	Org2	Total
Newer employees with more information about spam	1	0	1
Sessions/tips on how to identify spam	1	0	1
Regular reminders	1	0	1

Two participants, both from organisation 2, suggested that the organisation should delete the obvious spam instead of tagging it and sending it (notifications) through. One participant, who was being swamped with spam in a generic account, wanted the threshold changed to bring spam quantities down, and would trade-off this for increased false positives.

Only 1 participant thought the organisation could provide them with more information about spam, although two other suggestions were made during other questions, with information for new employees, sessions and tips on identifying spam and regular reminders being suggested.

Table 90***Other emergent participant themes, attributes, attitudes and events***

Theme, attribute, attitude or event	Org1	Org2	Total
False-positives causing problems	3	1	4
Participant accidentally deleted good email with spam	0	2	2
Received offensive email	2	0	2
Offensive email caused distress	1	0	1
Concerned clicking on links would confirm email address	1	0	1
Worried about Nigerian fraud	0	1	1
IT Dept not reactive enough in dealing with forwarded spam	1	0	1
Company monitors email activity of employees	0	1	1
Phoned IT Dept about amount of spam	0	1	1
Opening offensive spam breach of company rules	0	1	1
Quarantining and notifying employees	0	1	1
Spam filters were loosened up	1	0	1
More spam but easily identified because of 'tagging'	0	1	1
Unsubscribed from 'Old Friends' over Nigerian fraud harvesting rumour	1	0	1
Both 'frustrated' and 'don't care' responses	1	0	1

During discussions with the participants, a number of other facts, opinions and attitudes emerged as tabled above, with the problem of false positives most prominent, followed by receiving offensive emails, and accidentally deleting legitimate email with spam.

4.6 Economic Analysis

4.6.1 Introduction

The economic analysis of the cost of UBE to each organisation was done using a modified version of a “Spam Cost Analysis Model” MS Excel spreadsheet, developed by Mark Gibbs for a Network World article (Gibbs, 2003b), and used with his permission.

The original spreadsheet can be downloaded from the Network World website at:

<http://www.nwfusion.com/downloads/spamcost.xls>

Entered values are in Yellow, derived values are in Green, group results are in Orange, and the conclusion results are in Red. The exposed cell formulae can be found in Appendix D.

A spam filtering model is presented following the tables to better visualise the anti-spam technique chosen by each organisation, and the levels of received email and spam.

4.6.2 Comparative Cost Analysis and Filtering Return on Investment

The following two tables provide comparative cost analyses based on the measured and calculated survey results, documentation, and archival email data for each organisation.

To estimate the Return On Investment (ROI) from filtering spam, and therefore give some indication of the value filtering provides an organisation, a “no filter” comparison is calculated in the second table. To simplify the filter/no filter comparison, the following factors were imposed on the spreadsheet model:

- The calculated spam per user per day was the greater of detected spam or measured spam
- All filtering costs were set to \$0 to remove filtering from the equation
- Support costs were not adjusted at all, although in practice they should increase
- The “bandwidth used by email” could not easily be estimated by organisation 2, so the same value provided by organisation 1 was used, and was also not adjusted when removing the filters, assuming the entire email is received by the filter

The 5% trimmed mean value for spam per user per day for each organisation (3.2 and 6.4 respectively), which had been calculated in SPSS based on the results entered by survey respondents, was about twice as much for Organisation 2 than for Organisation 1.

Table 91

Cost Analysis with Spam Filters (RQ1)

Basics	Org1-Filters	Org2-Filters
Number of email accounts	1,000	210
Average fully loaded annual salary per employee	\$55,000	\$41,000
Average number of working days per person per year	230	240
Total number of emails received per day	140,647	3,557
Total number of detected spam blocked/tagged per day	127,710	363
Average employee cost per hour	\$32	\$21
Total percentage of email that is detected as spam	90.8%	10.2%
Filtering costs		
Hardware cost (per year)	\$2,400	\$6,667
Software/Licensing cost (per year)	\$4,495	\$4,000
Appliance cost (per year)	\$1,400	\$0
Total cost of spam filtering per year	\$8,295	\$10,667
Lost Productivity costs		
Measured spam per user per day (mean)	3.2	6.4
Average time to handle a spam (seconds)	5	5
Calculated spam per user per day	3.2	6.4
Average time to handle spam per user per day (minutes)	0.27	0.53
Average cost to handle spam per user per day	\$0.14	\$0.19
Total cost to handle spam per year	\$32,593	\$9,567
Connectivity costs		
Cost of office Internet connectivity per month	\$5,850	\$3,000
Cost of remote connectivity per month	\$0	\$0
Bandwidth used by e-mail	5%	5%
Total cost of Internet connectivity per month	\$5,850	\$3,000
Cost of bandwidth used by spam per year	\$3,187	\$184
Support costs		
Average cost of user support per user per year	\$66	\$560
Percentage of support time re spam	3%	25%
Cost of spam-related support per user per year	\$2	\$140
Total cost of spam-related support per year	\$1,980	\$29,400
Total Costs		
Connectivity	\$3,187	\$184
Filtering	\$8,295	\$10,667
Support	\$1,980	\$29,400
Lost Productivity	\$32,593	\$9,567
Total cost of spam per year	\$46,055	\$49,817
Total cost of spam per user per year	\$46	\$237

Table 92

Cost Analysis without Spam Filters (RQ1)

Basics	Org1-NoFilters	Org2-NoFilters
Number of email accounts	1,000	210
Average fully loaded annual salary per employee	\$55,000	\$41,000
Average number of working days per person per year	230	240
Total number of emails received per day	140,647	3,557
Total number of detected spam blocked/tagged per day	127,710	363
Average employee cost per hour	\$32	\$21
Total percentage of email that is detected as spam	90.8%	10.2%

Filtering costs

Hardware cost (per year)	\$0	\$0
Software/Licensing cost (per year)	\$0	\$0
Appliance cost (per year)	\$0	\$0
Total cost of spam filtering per year	\$0	\$0

Lost Productivity costs

Measured spam per user per day (mean)	3.2	6.4
Average time to handle a spam (seconds)	5	5
Calculated spam per user per day	127.7	6.4
Average time to handle spam per user per day (minutes)	10.64	0.53
Average cost to handle spam per user per day	\$5.66	\$0.19
Total cost to handle spam per year	\$1,300,750	\$9,567

Connectivity costs

Cost of office Internet connectivity per month	\$5,850	\$3,000
Cost of remote connectivity per month	\$0	\$0
Bandwidth used by e-mail	5%	5%
Total cost of Internet connectivity per month	\$5,850	\$3,000
Cost of bandwidth used by spam per year	\$3,187	\$184

Support costs

Average cost of user support per user per year	\$66	\$560
Percentage of support time re spam	3%	25%
Cost of spam-related support per user per year	\$2	\$140
Total cost of spam-related support per year	\$1,980	\$29,400

Total Costs

Connectivity	\$3,187	\$184
Filtering	\$0	\$0
Support	\$1,980	\$29,400
Lost Productivity	\$1,300,750	\$9,567

Total cost of spam per year	\$1,305,917	\$39,150
Total cost of spam per user per year	\$1,306	\$186

4.6.3 Organisational Spam Filtering Models (RQ1)

The following model in (Figure 3) was developed to provide a graphical overview of the spam filtering model that was used by each organisation:

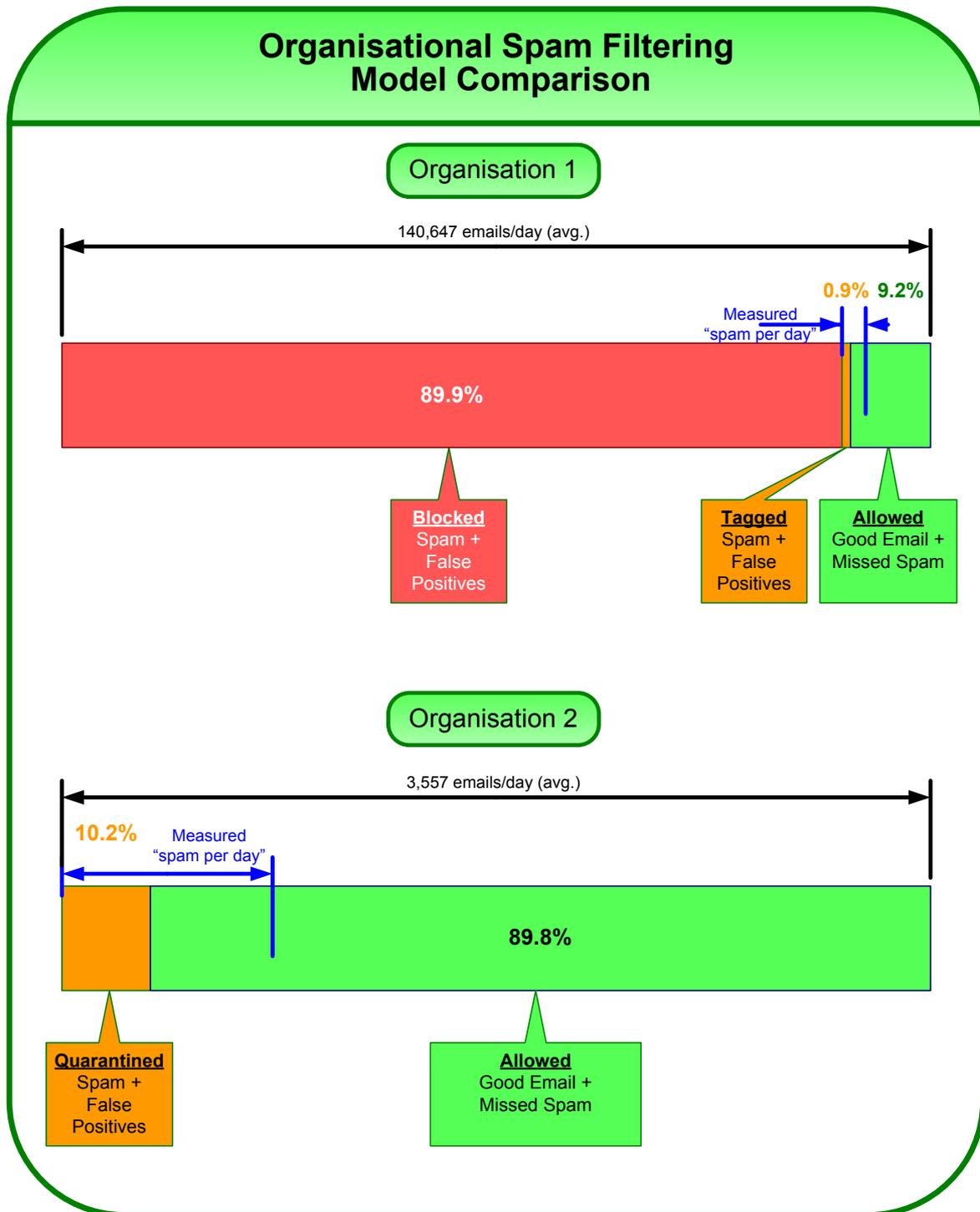


Figure 3. Organisational spam filtering: Model comparison

4.6.4 Spam Filtering Cost Analysis Organisational Differences

Highly positive ROI for organisation 1, negative ROI for organisation 2

Two strikingly different results emerged from the comparison of each organisation's cost analysis with and without spam filtering.

When the archival and measured results were entered into the cost analysis model spreadsheet and the results compared with and without the filters, the total cost of spam per year for Organisation 1 *increased* approximately 28 times without filtering, resulting in a very high ROI compared to not filtering (\$46k vs. \$1.3million).

For Organisation 2 however, the cost actually *decreased* approximately 21% without filtering, indicating a *negative* ROI.

Three key factors appear to have contributed to this:

- Not upgrading anti-spam systems to detect new spam techniques, leading to...
- Spam detected (by filter) < Spam measured (by survey), compounded by...
- Anti-spam technique: Blocked/Tagged vs. Quarantine+Notify

The filter model for each organisation shown previously in figure 3 provides a visual representation of the results obtained from both the archival records and the survey results. Similarly, the following table highlights the differences between the anti-spam techniques employed by each organisation in respect of the spam detected by the filters (UBE_{det}), the spam notified to recipients (UBE_{not}), and the spam measured by the survey (UBE_{meas}):

Table 93

Organisational UBE filtering techniques comparison (RQ1)

UBE Value	Org1	Org2
UBE detected by filters (UBE_{det}) =	Tagged + Blocked	Quarantined
UBE notified to recipients (UBE_{not}) =	Tagged	Quarantined
UBE measured by survey (UBE_{meas}) =	Tagged + UBE_{missed}	Quarantined + UBE_{missed}

Spam Values for Organisation 1

Organisation 1 is receiving considerable quantities of spam (over 90% of all incoming email), which is being detected by their two layers of spam filtering (UBE_{det}).

These two layers of protection seem to be highly effective at identifying/blocking spam, with a low level of possible spam that is tagged and passed on to recipients (UBE_{not}), and a similarly low rate of false negatives, or missed spam (UBE_{missed}), which is also received by the recipient, the combined values of which make up the spam values entered by the survey participants, becoming the measured spam value (UBE_{meas}) calculated by SPSS as 3.2 spam emails per person per day.

Spam Values for Organisation 2

It became clear from the survey results that the detection rate was much lower than for organisation 1, as the archival records showed that only 10.2% of incoming spam was being detected and quarantined (UBE_{det}), which calculates to about 1.7 spam emails per person per day, whereas the measured spam value (UBE_{meas}) calculated by SPSS was much higher at 6.5 spam emails per person per day, indicating a very high level of spam that was being missed by the filters (UBE_{missed}).

During the employee interviews, some participants from Organisation 2 indicated that they did not actually receive the spam email, but that they received a notification email each time an email destined for them had been quarantined. It became clear at this point that organisation 2 was using a different technique from organisation 1 in the way they handled detected spam, and that they were in fact *not* blocking any of it, but were quarantining all of it and then sending a notification email to the recipient for *every* email quarantined.

This means that *the recipient makes the final determination of whether every email is spam or not*, which is functionally equivalent to passing every spam through to them, and results in *practically no benefit* to the organisation through using spam filtering.

4.6.5 The Cost of Spam in New Zealand Organisations

One of the goals of this study was to discover the organisational cost of spam (economic impact) within the New Zealand context.

Organisation 1 are currently receiving large volumes of spam per day, but their combined anti-spam systems appear to provide highly effective detection and blocking, resulting in a current spam/total email detection ratio of about 90%.

Based on the measured average spam levels per user per day, spam was costing organisation 1 about \$46,000 per year, or about \$46/employee/year.

Without the anti-spam filters detecting and blocking the spam, it would instead be costing organisation 1 about \$1.3 million per year, or about \$1,300/employee/year.

These figures seem to be comparable with some figures produced in overseas studies, which presumably were under “no filter” conditions also.

Organisation 2, by comparison, had much higher support overhead costs, and because of the very low detection rate of the out-of-date software being used, only had a 10% spam/total email detection ratio, which actually resulted in employees at organisation 2 receiving about double the amount of spam per day that organisation 1 employees were.

Based on the measured average spam levels per user per day, spam was costing organisation 2 about \$50,000 per year, or about \$237/employee/year.

Without the anti-spam filters detecting and quarantining the spam, this figure actually decreased to about \$39,000 per year, or about \$186/employee/year.

Due to the combination of the key factors found to be contributing to the unusual result for organisation 2, their result should not be regarded as normal for an organisation, although it is possible, and indeed probable, that there are other organisations in New Zealand and elsewhere that will be in the same situation, and would be well-advised to implement the best practices that emerged as a result of this study.

4.6.6 Rule-of-Thumb Economic Cost of Spam for Organisations (RQ1)

Every email received has a cost attached to it, which is composed of a number of components that the previous spreadsheets have attempted to break down, including the cost of Internet bandwidth, the cost of storage (not taken into account in this study), and perhaps most importantly, *the cost of the recipient's time to deal with it.*

Regardless of whether an email is spam or a legitimate email, when it reaches the recipient, there is an immediate cost incurred in having to spend time dealing with the email.

For an organisation, this cost can be simplistically reduced to:

(average cost of an employee per second) x (number of seconds dealing with email),

where (cost of an employee per second) = average employee cost per hour / 3600.

Therefore, if the calculated average cost of an employee-second is 0.9 cents and it takes an employee 5 seconds to deal with that email, that cost value of that email to the organisation is a minimum of *4.5 cents.*

This cost is, of course, a rule-of-thumb minimum when dealing with spam, as it does not take into account the additional cost of support costs etc as does the spreadsheet model, but may be useful to give an indication of how much it is costing an organisation for every spam email, or spam notification email, that is passed on to employees.

4.7 Summary

This chapter has described the two organisations studied to provide a context for the interpretation of results from each for purposes of comparison.

The quantitative and qualitative results from the employee survey and interviews were presented using tables that provided two dimensions of analysis at the organisation and the gender levels, as specified for comparison by the research questions and framework.

Descriptive analysis was used for these results, and included a ratio comparison of gender when analysing the JES results.

Basic thematic analysis was used for the employee interviews, the results of which were also tabulated into frequency counts as there were only eight participants.

The economic analysis provided an unexpected negative ROI result that required developing a simple model of the email filtering process used by each organisation, and also further discussions with the organisations and one of the anti-spam vendors, in order to understand the factors involved that caused this result.

The ROI of anti-spam filtering for organisation 1 shows that although it can be sometimes costly for an organisation to implement an effective system, the alternative, with the high volumes of spam traversing the Internet today, is significantly more costly to an organisation's bottom line in terms of lost productivity.

Finally, a greatly simplified cost calculation model, based on the cost of an employee per second and a measured average spam received figure, can be combined with the time to identify and delete a spam figure of 5 seconds, to produce a rule-of-thumb guideline for any organisation to estimate what the cost is for an employee a single spam email.

Chapter 5 - Discussion and Inferential Analysis

5.1 Introduction

This chapter expands on the descriptive analysis from chapter 4, and makes a number of inferences about the impact of spam in relation to the research questions.

The results of this chapter will form the basis for many of the recommendations for “best practice” in chapter 6, regarding organisational policies and anti-spam measures.

5.2 How UBE is impacting organisations economically (RQ1)

5.2.1 *Anti-spam systems and the economic impact of spam*

Although both organisations had one particular anti-spam system in common, MailMarshal, the results were significantly different in terms of detecting spam.

The two anti-spam filtering layers used by organisation 1 behave in a similar fashion to the similar practice of using two (or more) layers of anti-virus system from different vendors, and the IT manager for organisation 1 indicated during discussions that the spam missed by one system was frequently detected by the other. As spam continues to change and adapt to various anti-spam systems used, this practice may become common in the future.

Keeping anti-spam systems at the latest versions is essential to reducing spam

One of the key factors resulting in significant levels of missed spam by organisation 2’s anti-spam system appears to be the fact that the version used had not been updated for some time. Discussions with the Marshal Software representative confirmed that the version being used by organisation 2 was several years old, and not as effective as newer versions against the recent type of UBE known as “image spam”, and the volume of this type of spam that organisation 2 was receiving resulted in correspondingly high levels of missed spam being delivered to recipients (about twice that of organisation 1’s employees).

Keeping anti-spam software up-to-date with the latest versions therefore seems to be a necessary practice to counter the new techniques being developed by spammers, and significantly reduce the cost of missed spam being delivered to employees.

This conclusion was also reached recently by Garfinkel (2007, June), who reported two statistics from anti-spam vendor MessageLabs, showing that smaller businesses tended to be less effective at blocking spam, with their employees receiving up to five times the amount per person as employees in larger businesses.

He further stated that:

...the conclusion is more or less in line with my own experience. Spam filtering is not something that you can set up and forget: An antispam system that works well today will slowly lose its potency as the spammers learn how to evade the filtering techniques that you've implemented.

(Garfinkel, 2007, June, para 4)

Garfinkel concluded that larger organisations are able to update their antispam systems more frequently as they are better resourced, whereas at smaller organisations the amount of spam received by employees will slowly increase until the system(s) are eventually updated to more current technology, which closely agrees with these research findings.

5.2.2 Content Based Filtering (CBF) and the economic impact of spam

In order to overcome the problems caused by the ineffective filters, organisation 2 began creating custom CBF rules, by analysing the content of missed spam and applying “scores” to particular words that seemed to appear regularly in it.

Unfortunately, as often happens, a number of these words happen to occur frequently in *legitimate email* as well, which resulted in the worsening of a problem all anti-spam systems already inherently have: false positives.

The employee survey results indicate that 76% of respondents receiving spam in organisation 2 believe that the spam filters block good emails. This is also reflected in some of the final comments such as “The one irritating problem is that ordinary emails often get blocked as spam”, and “The only problem I have is that the company block about every e-mail even if it is business related”. One of the interview participants from organisation 2 also commented on this.

This is not a new problem, and is one personally experienced by the researcher as well, during early attempts at blocking spam several years ago.

In describing their own anti-spam systems and techniques, Joe St Sauver from the University of Oregon stated that “On the other hand, one of the biggest issue(s) with CBF is the problem of false positives” (St Sauver, 2004, p. 50).

There is one obvious cost to creating your own custom CBF’s, and one hidden and potentially very expensive cost.

IT support costs

Organisation 2 is already spending a considerable amount of it’s IT Help Desk time dealing with spam issues (25%), and this is not surprising, as they are probably caught in a vicious circle of trying to create custom CBF’s to block the volumes of spam missed by the filters, and then having to deal with the false-positives that result from this practice.

If you wouldn’t write your own signatures to block a new virus, why would you want to write your own custom CBF to block new spam? Organisation 2 could save itself time and money if it simply passed on the missed spam to their vendor, who would be able to much more effectively write new filter rules based on other features they might not have even considered, such as the email headers, which frequently contain much better indicators of emails “spamminess” than the message content does.

The cost of accidentally deleted legitimate email

The hidden cost is one that surfaced during interviews with organisation 2 participants:

deleting legitimate emails accidentally.

Two participants indicated they had previously deleted legitimate emails, at least one of which was a false positive “tagged” as spam. This false positive just happened to be a customer order. The cost of deleted orders was not factored into this study, but is clearly a major cost to be avoided by any organisation.

Use CBF’s to apply organisational policies, not filter spam

If there is indeed a positive correlation between the use of custom CBF’s and the number of false positives, it would be good practice to keep the number of these to a minimum.

During discussions with the Marshal Software representative, it was concluded that because CBF’s are capable of causing such significant issues and both real and potential costs to an organisation, the best practice would be to use CBF’s to *apply organisational policies only*, e.g. filters or rules that modify or route email based on recipient addresses.

5.2.3 Anti-spam techniques and the economic impact of spam

The two organisations studied had each chosen different anti-spam techniques, which also resulted in major differences in the economic cost of spam to their organisations.

Organisation 1 chose a technique of filtering by blocking, and notifying employees of possible spam by “tagging” the subject line.

Organisation 2 chose a technique of filtering by quarantining, and notifying employees of every quarantined email.

Blocking spam can significantly reduce the economic impact

While respondents and participants from both organisations complained about the numbers of spam passing through the filters, most employees at organisation 1 would probably have

no idea of the sheer volume of spam that the anti-spam systems are actually blocking, as they are seeing only the tip of the iceberg, according to the filter statistics.

The difference becomes obvious simply by removing the anti-spam filters from their email system, which would result in a jump in average spam per person per day from 3.2 to 127.7 and a corresponding jump in cost to the organisation from \$46,055 to \$1,305,917.

The ROI for \$8,295 per year in anti-spam filtering is *a cost saving of nearly \$1.26 million*, through blocking positively identified spam.

Notifying does not reduce the economic impact

Organisation 2 could never actually reduce the economic impact of lost productivity, due to the chosen technique of notifying employees about every spam (and false positive) that has been quarantined. There is essentially little difference between notifying the recipient by email that they have a possible spam in quarantine and actually sending it to them, as there is a minimum cost to the business involved in dealing with every email.

Were organisation 1 to use the same technique, it would still cost them \$1.3million/annum.

Blocking and accidentally deleting legitimate email can cost money

Employees accidentally deleting customer orders tagged as spam can potentially have a major economic impact on an organisation, so too can blocking false positives, and what's worse, an organisation may never know it. The solution to this problem lies with the vendors of anti-spam systems, who must design their systems to provide the lowest false positive rate possible. The best practice for any organisation to reduce the economic impact of both lost productivity and lost business is to use (and/or upgrade regularly) an anti-spam system with the highest spam detection rate and the lowest false positive rate.

5.3 How UBE is impacting employees in NZ organisations (RQ2)

Reflecting on the question design in Chapter 3, Research Design, it is appropriate to analyse the employee impact in terms of employee attitude, which is broken down into the following three attitudinal components:

Affective person's general feelings or emotions

Behavioural person's actions or intended/expected actions

Cognitive person's beliefs or knowledge

5.3.1 Affective impacts

Negative emotional responses agree with the results of other studies

The literature review revealed very strong links between spam and strong negative emotional responses, such as the recent study by Siponen and Stucke (2006), where two respondents indicated that "...spam increases frustration and anger among the employees who receive it...".

Frustration and anger among employees as an emotional response to spam is also a very prominent feature in the results of this researcher's study, which provides further confirmation of the results found by Siponen and Stucke (2006), Klotz (2004) and others.

For the majority of employee survey questions about the different types of spam they receive, the Job Emotion Scale (JES) composite anger choices (angry, frustrated, and disgusted) were the response from the majority of respondents, and also from the majority of interview participants.

Similarly, for the Likert scale questions about when they receive spam, “It makes me angry” and “It makes me frustrated” was agreed with by the majority of respondents.

Some positive emotional responses also agree with other studies

A number of respondents and one interview participant indicated that they liked to receive certain types of spam, which is also consistent with the findings of Andrew (2003), and although the interview participant clicked through on links within the spam to read information on the website, did not proceed to the point of purchasing from it.

Spam of a sexual nature incites the most anger and anxiety

While a reasonable percentage of respondents chose “don’t care” for many of the types of spam, a pattern of decreased “don’t care” responses, and increased composite anger responses emerged in relation to the “sexual” spam, i.e. sexual performance drugs, male enhancement/enlargement products, and pornographic websites, with the most extreme values seen from respondents who had received spam relating to child pornography websites.

Levels of composite anxiety (worried and embarrassed) also peaked for these types of spam, indicating that receiving these causes high levels of stress among some employees.

Email, spam, and work-related stress

Research on technology and stress has also found links between receiving large quantities of email (whether legitimate or spam) and work-related stress. Citing a 2001 study by Professor Cathy Cavanaugh, Dye (2007, p. 251) highlights the results of this research as

revealing that it is “not only the amount of e-mail but also the type of message received that leads to stress”, and the participants were “particularly angered” by spam.

Some respondents in both organisations were receiving extremely large quantities of spam daily (up to 86 per day), so it could be inferred from the JES responses that many of the respondents who are receiving spam in both organisations would be experiencing some degree of work-related stress as a result of the spam they are receiving.

5.3.2 Behavioural impacts

Many employees are accidentally deleting legitimate email

More than one in three respondent in both organisations agreed that they had at some time accidentally deleted legitimate email while deleting spam, and with such a high incidence rate, this should be of major concern to organisations.

Although the reason was not explored in the survey, the interviews revealed there are two probable reasons this is happening:

- High levels of spam
- High levels of false positives

One participant indicated they had probably deleted legitimate emails because they were deleting a number of spam emails simultaneously, and had missed the fact that a legitimate email mixed in with the spam had accidentally been selected before deletion.

The other participant indicated they had deleted the legitimate email, which was in fact a customer order, because it was a false positive that had been tagged as spam and so had been deleted *assuming it was spam*.

Unfortunately for organisations, these two reasons usually have a negative correlation, i.e. reducing the levels of spam usually increases the levels of false positives, and, as has occurred with organisation 1, “loosening up” the filters because of too many false positives

has resulted in more spam being passed through to employees again, as a number of respondents from organisation 1 noted and complained about.

Many employees are unable to identify untagged spam and are opening it

Almost half of the respondents from both organisations indicated that the reason they opened untagged spam emails was because they were checking “just in case” it was legitimate, and a number of others were opening them because they believed they looked legitimate.

Since spammers do their best to make spam look as legitimate as possible, it is not surprising that many of them succeed to the point of fooling not only the anti-spam filters, but also the recipients. Despite many employees having had more than five years experience using email, they still seem to lack the ability to identify real spam.

One interview participant, who indicated they were receiving large amounts of spam because they administered a generic email account, suggested that they would benefit from a session on how to spot spam, presumably to reduce the number of times they had to open each email to check it “just in case” it was legitimate.

This idea may have some merit, as it was indicated by Spammer-X (2004), clearly experienced at identifying spam based on just the sender name and the subject line, that he was able to very quickly identify and delete obvious spam.

Some employees will open it because they like it

International surveys have shown that a small percentage of spam recipients like to receive spam and do actually make purchases of products and services offered in them, thus encouraging the spammers to send more of it.

This study has also revealed that small percentages of employees in New Zealand organisations also like to receive and read specific types of spam, but not to the point of purchasing from it, that they will admit to at least.

Curiosity was the reason given by several respondents, so it could be inferred from this and the composite positive emotion (Like it, Happy) responses, that because some employees are interested in the product or service being marketed in the spam, their curiosity was sufficiently aroused that they clicked on the link and went to the website, as was admitted by one of the interview participants. Andrew (2003) found that 1% of respondents liked spam, and Fallows (2005) found that 6% had actually purchased, and behaviours revealed in this study show there are similar percentages among New Zealand employees.

Behaviours on the Internet invite spamming

The following section on cognitive impacts reveals that the organisations and employees know that one of the reasons they are receiving spam is because of their behaviour on the Internet, and so is also mentioned in this section. Specifically, employees are leaving email address “trails” behind when subscribing or registering on some website forums, chat rooms, practices that should be actively discouraged by organisations.

5.3.3 Cognitive impacts

Many employees seem to know about spam, and why they are being spammed

Six out of the eight interview participants had seen something about spam through an external media channel, and five out of eight had been informed about it by their organisation, which indicates many employees have knowledge of spam as a problem. Posting email addresses in clear or machine-readable text on a corporate public website is a well-known way to attract spam (Dantin & Paynter, 2005, p. 33), and is also known to the IT department at organisation 1. Many of the survey respondents also chose this as the reason why they believed they were being spammed, above all other reasons.

Most respondents from both organisations seemed to be aware that the email address “trails” left on either their own corporate public website, or other websites, are a major contributing factor to their being spammed.

These results seem to indicate that both employees and employers know that if an organisational email address is visible in public Internet space for spammers to find and harvest, then it is going to get spammed.

Some employees also seem to know that you should never reply to spam, and consequently also believe that their use of the “auto-reply” function in their email client has resulted in their being spammed, rightly or wrongly.

Most employees know that the spam filters are helping, but their perceptions of effectiveness is based on subjective historical knowledge

Many employees are also keenly aware of the benefits, and shortcomings, of the spam filters at their organisations, and their perceptions of the effectiveness of their respective anti-spam filters is based on subjective historical knowledge of spam levels in the past.

For organisation 1, despite having kept their anti-spam system up to date and even adding a second layer of filtering protection, thereby reducing the levels of observed spam per user per day from a potential 127 down to a manageable 3.2, with an over 90% detection rate, the employees generally perceive that the filters let too many spam emails through. Most employees probably have no knowledge of how many are *not* being let through.

This contrasts with the “spam holiday” briefly enjoyed by the employees at organisation 2, who, prior to the changes in their domain name, were also receiving large volumes of spam in their Inboxes. Despite having an observed spam per user per day level of 6.4, double that of organisation 1 employees, the general perception is that they are receiving less spam, and that the anti-spam filters do *not* let too many spam emails through.

They also do not seem to be aware that they are effectively also receiving every spam email by way of notification, and that in reality the anti-spam filters are detecting probably only about one third of the spam entering their systems, so in this case, the effect of the domain name change is being incorrectly attributed to the anti-spam filters.

Most employees know about the problems of false positives

One fact that employees at both organisations have considerable knowledge of is the problems caused by false positives. A number of respondents mentioned this in their final comments, as did the interview participants. Employees at organisation 1, for example, are aware that the IT department had to “loosen” the detection scores because they were causing too many false positives. Surprisingly, one participant from organisation 1 was willing to trade an increase in false positives for a reduction in the higher levels of spam now being received as a result of the “loosening”. This was also a frequent criticism from employees at organisation 2, who also seem to be very aware of the number of legitimate business emails being “tagged” as spam. These responses indicate that most employees do know about the false positive problems inherent in every anti-spam system.

5.4 How employees are impacted differently because of their gender (RQ3)

There were slightly fewer men than women respondents for organisation 1, and slightly more men than women respondents for organisation 2.

Many of the survey responses were of approximately equal proportions when compared by gender, but for the questions with an emotional response (e.g. angry, frustrated or worried) the responses were usually significantly different depending on gender.

5.4.1 “Sexual” spam affects women significantly more than men

During the analysis of how respondents really feel about the types of spam they receive, the ratios of women to men expressing composite anger (angry, frustrated, disgusted) were

considerably higher for spam of a sexual nature, e.g. sexual performance drugs, male enhancement/enlargement products. Typically the ratios for M:F were from 1:2 up to 1:8 in expressing composite anger towards this type of spam. Men still expressed anger about this type of spam, but generally not to the degree expressed by women.

5.4.2 More men than women like to receive certain types of spam

Some respondents indicated that they liked to receive (“Like it”, “Happy”) the following types of spam:

- Selling cheap software
- Weight loss drugs/programmes
- Mortgage/Loan financing
- Job/Employment offers
- Dating websites
- Stock market “tips”
- Online casino websites
- “Nigerian” fraud

There were responses from women for only two of these: Weight loss drugs/programmes and Job/Employment offers. Similarly, for the survey statement “I enjoy receiving it”, 3 respondents agreed with the statement, and all were men.

5.4.3 Women are usually more frustrated by spam than men

One particularly consistent ratio was the ratio for the “frustrated” response, which in all but one case for organisation 2 showed a higher ratio of women than men.

5.4.4 Men usually don’t care about spam

The other particularly consistent ratio was the ratio for the “don’t care” response, which was in nearly all types of spam a higher ratio for men than for women.

5.4.5 Gender stereotypes and emotional responses to spam

An explanation for the differing emotional responses may be found in research on emotion, phobias and technology, which indicates that “There appears to be strong evidence

supporting gender differences in relation to computerphobia. Females are more likely to possess higher levels of computer anxiety than males and to experience more negative attitudes towards computers.” (Owen, 2003, p. 250).

It is likely however, that earlier and more general research relating to gender stereotypical emotional reactions, which for example indicates that typically men tend to hide their emotions, while women tend to “show and admit to more” when it comes to fear and anger (Campbell, 1989, p. 183), can also provide an explanation for the gender differences relating to technology indicated by Owen.

Whether the emotional responses are technology specific as indicated by Owen or simply general stereotypical responses as indicated by Campbell, gender differences relating to emotional response did emerge during this study, and would seem to be consistent with the research of others.

5.5 Summary

This chapter has discussed the major findings that emerged from the analysis of the results, which will answer the three research questions.

These can be summarised as follows:

The processes and techniques used when implementing and maintaining an anti-spam system can have a significant effect on the economic impact of spam to an organisation.

Both employees and the IT departments are aware of the problems and issues created by spam, but both still engage in practices that attract it.

Spam has significant negative affective impacts on employees, particularly when the spam is of a sexual nature, and women appear to be affected by this much more than men, but there is also a small minority of employees who like to receive specific types of spam.

Employees have trouble identifying spam, and many have deleted good emails accidentally.

Chapter 6 - Conclusions and Recommendations

6.1 Introduction

This chapter provides final major conclusions based on the analyses conducted in the study, and makes recommendations for organisations to minimise the impact of UBE.

6.2 Conclusions

This study has shown that UBE (spam) does seem to be having a significant negative impact on organisations and employees in New Zealand, both economically (RQ1) and socially (RQ2, RQ3), even when using highly effective anti-spam systems, but if a system is not correctly configured or regularly upgraded, the results can be as bad as or worse than not having an anti-spam system at all.

Blocking positively identified spam, or at least not notifying employees about it, seems to be the anti-spam technique with the greatest cost benefits for an organisation (RQ1).

Large volumes of spam and false positives are still causing major issues which are both frustrating and angering employees (RQ2, RQ3), and potentially costing the organisation lost business when customer orders are deleted (RQ1). IT staff “tweaking” the systems in an effort to reduce spam levels frequently make the false positive situation much worse.

More education of both employers and employees seems to be needed in the areas of both spam avoidance and spam prevention (RQ2).

Spam of a sexual nature in particular causes the most anger, frustration, and anxiety among employees (RQ2), and should be considered a source of work-related stress by employers.

Women are significantly more angered by spam of a sexual nature than men, and over all of the types of spam women are generally more frustrated by it, whereas men generally don’t care about it (RQ3).

Of the minority of employees who like receiving certain types of spam, the majority will be men (RQ3).

6.3 Recommendations

6.3.1 Organisational best practice to reduce the impact of UBE

Technical practices

- Use anti-spam software or hardware with the highest hit rate and lowest false positive rate that you can afford, particularly if you have large spam volumes. The ROI is well worth it.
- Regularly upgrade your anti-spam systems. As spam methods change, your anti-spam system will need to be upgraded to adapt to the changes, otherwise spam levels may rise.
- Most anti-spam systems have global rules that can be updated frequently, either daily, hourly or even real-time. Configure it to do so.
- Use a highly reputable Real-time Block List (RBL). Most vendors recommend Spamhaus's sbl-xbl list. Others can be much more aggressive and unforgiving of minor infractions.
- Block or quarantine high-score spam, some experimentation may be necessary to find an optimal threshold that minimises false positives.
- Tag and pass on, or quarantine and notify only "possible" spam. Preferably send notification "digests", rather than for every quarantined item, or allow employees to manage their own individual quarantine area.
- If you quarantine spam with high-scores, don't notify the recipients.
- Avoid creating custom Content Based Filter (CBF) rules as much as possible, ideally only to implement corporate email policies, as they can cause more problems with false positives than they solve.
- Instead of creating CBF's, pass on the missed spam and the "ham" (false positives) to the anti-spam vendor. They will be better equipped to identify relevant features in the emails.
- Consider engaging the services of an engineer from the anti-spam vendor's support team for a day or so, to ensure your system is correctly setup and maintained.
- If an anti-spam system doesn't have a method for users to forward missed spam and "ham" to the vendor directly, provide a "public" folder or email address for them to do this, and forward it yourself. This will improve the filter detection rate over time as the vendor modifies or adds to the global rules.
- If particular types of spam are consistently being missed in large volumes by the anti-spam system, and all the previous practices have not improved this, it may be time to invest in a second layer anti-spam system from a different vendor, much like organisations do now with their anti-virus systems.
- Avoid spam-attracting practices such as placing organisation email addresses in clear text on the public corporate website. Obfuscate or "munged" these in some way instead, otherwise spammers will quickly find and harvest these. Hex or hex/html encoding is preferred, and a number of websites offer free utilities to obfuscate addresses this way.

Business practices

- If the organisation has an Intranet website for employees, consider creating, if not already available, specific pages dealing with email. Contents should cover sections on netiquette, acceptable use policy (AUP) and spam,
- Remind employees of the “bad” behaviours that will get them spammed, e.g. putting their email address in public places on the Internet, such as forums, chat rooms etc., and encourage them to be more aware of the consequences if they do.
- Remind them to practice InternetNZ’s “Four Golden Rules”:
 - Never buy anything from spam
 - Never reply to spam
 - Never use “remove” or “unsubscribe” options
 - Distrust everything from people you don’t know(InternetNZ, 2006a)
- Provide employees with more information about the levels of spam being detected, perhaps by posting weekly or monthly volume reports on the Intranet, and perhaps an “Alert” section that highlights currently received phishing scams etc.
- Support employees receiving spam, and reassure them that if they are receiving spam of a sexual nature in particular, suspicions will not necessarily be raised or questions asked about their surfing habits, since email addresses are usually harvested from many sources, and then spammed indiscriminately.
- Email the Intranet links to the above information about spam and how to deal with both missed spam and false positives to all employees on a regular basis (e.g. at 6-monthly intervals).
- Perhaps create a small pamphlet, based on the Intranet pages, which can also be given out at staff induction or training sessions, so everyone knows the issues, do’s and don’ts right from the start. Staff training about spam is regarded as an often overlooked but important part of any spam reduction effort by InternetNZ (2006b).

6.3.2 Recommendations for further research

It is recommended that additional organisations be studied to further confirm the findings of this exploratory research, particularly with respect to smaller organisations, which make up the majority of New Zealand businesses, and may also be experiencing problems with spam for similar reasons to those revealed in organisation 2.

Alternatively a longitudinal study could be conducted that researches the impacts and effects of the changing nature of UBE on an organisation.

6.4 Limitations of the research

The major limiting factor in this research was the low response rate encountered with the web-based employee survey, which had only a 12.9% and 21.4% response rate respectively.

6.5 Strengths of the research

The major strength of this research was the comparative case study framework, which contrasted the major differences between the organisations' economic impact and the way their antispam systems were configured and maintained, yet highlighted the significant level of agreement in the social impact.

6.6 Summary

This chapter concludes the research by summarising the major findings, and making recommendations for organisational best practice that will reduce the impact of UBE on both organisations and their employees.

Appendix A - Organisational Questionnaires (RQ1, RQ2)

Organisation 1 (OQ1.1)		Date: 20/12/06	
Q1	Is Unsolicited Bulk Email (UBE) considered to be a minor, significant or major problem for your organisation? <i>Moderate problem.</i>		
Q2	If UBE is considered a significant or major problem, which areas of the organisation are aware of this as a problem (e.g. IT, HR, Senior Management) to the best of your knowledge? <i>N/A</i>		
Q3	What specific policies, processes or techniques do you employ to control/prevent UBE?	Please list each of these, and indicate how useful and effective you believe each of these to be, using the scale: Not at all Not very Somewhat Very Extremely	
	Policy/Process/Technique	Useful	Effective
1	<i>MailMarshal</i>	<i>Somewhat</i>	<i>Somewhat</i>
2	<i>Barracuda Spamware</i>	<i>Very</i>	<i>Very</i>
3	<i>Public Folder for forwarding spam</i>	<i>Very</i>	<i>Very</i> <i>Staff know they can forward spam to account, cuts down on Help Desk calls</i>
4	<i>Email reminder occasionally</i>	<i>Somewhat</i>	<i>Don't know</i>
5	<i>Policy on Intranet</i>	<i>Not Very</i>	<i>Don't know</i>
Q4	Does your organisation have an Acceptable Use or Email Policy for employees, which specifically discusses UBE (i.e. "spam", "junk mail" etc) in some way? <i>No. Netiquette for Internal only, not specifically for spam</i>		
Q5	If so, what main points does the policy cover? Some examples might be: Definition of "spam", what the organisation does to control it, and what employees should and should not do if they receive it <i>N/A</i>		
Q6	Is UBE discussed during staff induction or in any staff training (if so, which of these)? <i>No.</i>		
Q7	What do you regard as being the reason(s) that the organisation's email addresses are being sent UBE (e.g. possible activities the organisation may be doing, possible activities the employees may be doing, or some other reason or activity)? <i>1.) Leaving details on websites, e.g. subscribing.</i> <i>2.) Email details on our websites.</i>		
Q8	To the best of your knowledge, have any employees ever logged into a website and provided information after clicking on a link in an unsolicited email they received from a bank or other online financial organisation (e.g. Paypal)? <i>No, but some have replied asking to be removed.</i>		

Cost calculation data for Organisation 1 (OQ1.2)

Employee Costs

How many employees/email accounts does your organisation have?	1,200/1,000
What is the average calculated “cost” of an employee (wages/salary + overheads, i.e. the fully burdened HR cost) per year?	\$55,000
What is the average number of working days per person per year?	230
What are your standard working hours per day?	7.5
(Average employee cost/hr = (cost / (working days * working hours)))	

IT Department Costs

If you use specific server hardware/software or an appliance to block UBE, what are the annual costs attributed to these?

Hardware (cost/x years)	\$12,000 / 5yrs
Software/Licenses	\$ 5,000 / yr
Appliance (if applicable)	\$7,000 / 5yrs
What are your Monthly Internet Connection costs?	\$5,850/mth
Approximate percentage of bandwidth used by incoming SMTP traffic?	5%
Approximate percentage of total SMTP traffic is UBE?	1%
<i>(Actual value, based on Spam Stats below, would be more like 89.7%)</i>	
Cost of user support per year (i.e. Help Desk type support) (e.g. cost of Help Desk support / # of employees)	\$66/yr
Estimated percentage of time dealing with spam-related calls (e.g. spam-related jobs / total jobs)	3%

Spam Statistics

Total avg. number of all email messages received per day	140,647
Either:	
Average number of spams received per day	127,710
Or:	
Average percentage of spams received per day	89.7 % (calc.)

Note 1. Spam received should include both blocked and tagged

Note 2. Total average of all emails excludes email detected with viruses

Organisation 2 (OQ2.1)	Date: 16/05/07
-------------------------------	-----------------------

Q1 Is Unsolicited Bulk Email (UBE) considered to be a minor, significant or major problem for your organisation?

Significant.

Q2 If UBE is considered a significant or major problem, which areas of the organisation are aware of this as a problem (e.g. IT, HR, Senior Management) to the best of your knowledge?

All Management, IT Department, HR

Q3	What specific policies, processes or techniques do you employ to control/prevent UBE?	Please list each of these, and indicate how useful and effective you believe each of these to be, using the scale:	
		Useful	Effective
		 Not at all Not very Somewhat Very Extremely	
	Policy/Process/Technique		
1	MailMarshal gateway with spam filtering and virus scan	Very	Somewhat
2	Trend Micro scanning on Exchange Server	Very	Not Very
3	Client Antivirus	Very	Not Very
4	Outlook Harmful Attachment Protection	Not Very	Somewhat
5	Configuring to deny relaying internal and external	Somewhat	Somewhat

Q4 Does your organisation have an Acceptable Use or Email Policy for employees, which specifically discusses UBE (i.e. “spam”, “junk mail” etc) in some way?

Yes.

Q5 If so, what main points does the policy cover? Some examples might be: Definition of “spam”, what the organisation does to control it, and what employees should and should not do if they receive it

1.) Not to reply to it. 2.) That Company monitors and intercepts.

Q6 Is UBE discussed during staff induction or in any staff training (if so, which of these)?

No.

Q7 What do you regard as being the reason(s) that the organisation’s email addresses are being sent UBE (e.g. possible activities the organisation may be doing, possible activities the employees may be doing, or some other reason or activity)?

1.) Employees giving addresses on online shopping, website logons, discussion groups etc.

2.) Employees giving addresses to “friends”, associates and such like, who have viruses/worms etc on their computers.

Q8 To the best of your knowledge, have any employees ever logged into a website and provided information after clicking on a link in an unsolicited email they received from a bank or other online financial organisation (e.g. Paypal)?

No.

Cost calculation data for Organisation 2 (OQ2.2)

Employee Costs

How many employees/email accounts does your organisation have?	500/210
What is the average calculated “cost” of an employee (wages/salary + overheads, i.e. the fully burdened HR cost) per year?	\$41,000
What is the average number of working days per person per year?	240
What are your standard working hours per day?	8
(Average employee cost/hr = (cost / (working days * working hours)))	

IT Department Costs

If you use specific server hardware/software or an appliance to block UBE, what are the annual costs attributed to these?

Hardware (cost/x years)	\$20,000 / 3 yrs
Software/Licenses	\$12,000 / 3 yrs
Appliance (if applicable)	N/A
What are your Monthly Internet Connection costs?	\$3,200/mth
Approximate percentage of bandwidth used by incoming SMTP traffic?	?? %
Approximate percentage of total SMTP traffic is UBE?	11 %
Cost of user support per year (i.e. Help Desk type support) (e.g. cost of Help Desk support / # of employees)	\$560 / yr
Estimated percentage of time dealing with spam-related calls (e.g. spam-related jobs / total jobs)	25 %

Spam Statistics

Total avg. number of all email messages received per day	3,557
Either:	
Average number of spams received per day	363.3
Or:	
Average percentage of spams received per day	10.2 % (calc.)

Note 1. Spam received should include both blocked and tagged

Note 2. Total average of all emails excludes email detected with viruses

Appendix B – Job Emotion Scale (JES)

Scales used in previous studies:

Job Emotion Scale (JES), a 16-item instrument to measure emotion at work, created by (Fisher, 2000, Mar2000 Special Issue, p. 195):

Liking	Happy	Enthusiastic	Pleased
Proud	Optimistic	Enjoying	Content
Depressed	Frustrated	Angry	Disgusted
Unhappy	Disappointed	Embarrassed	Worried

Modified JES, the Composite Emotion Scale used by (Grandey et al., 2002, p. 41):

Positive emotions	Negative emotions
Composite positive	Composite negative
Liking	Composite anger
Enthusiastic	Angry
Proud	Frustrated
Enjoyment	Disgusted
Happy	Composite Sadness
Pleased	Disappointed
Optimistic	Unhappy
Content	Depressed
	Composite anxiety
	Worried
	Embarrassed

Modified Grandey et al. JES as used in this study:

Positive	Negative (composite anger)	Negative (composite anxiety)	Neutral
Like it	Angry	Worried	Don't Care
Happy	Frustrated	Embarrassed	
	Disgusted		

Appendix C – Online Employee Survey

HTML Page 1:

Measuring the Impact of Unsolicited Bulk Email (spam)

Purpose

The purpose of this Survey is to try to determine the impact of Unsolicited Bulk Email (UBE, or "spam") on organisations like yours, within New Zealand. Your answers will provide valuable information about spam in New Zealand, including how employees like yourself feel about spam emails you may receive at work. This research has been approved from 26 July 2006 until 28 February 2007.

This Survey is Voluntary

Filling out this survey is completely voluntary, you can leave the survey at any time, and your answers will not be saved.

This Survey is Anonymous

Your assistance with this research is entirely anonymous. Your answers to the questions will remain strictly confidential. No information that could personally identify you (e.g. name, email address) will be requested.

Please note that to ensure the security and anonymity of your Survey answers, all interaction with this website uses secure encryption (note the "https://" in your browser URL bar), and you should see a yellow "padlock" on the border of your browser window (usually at the bottom). If you wish, you might also choose to answer the Survey questions from somewhere other than at work (e.g. from home), as long as you answer the Survey only once.

Definition of Spam

The email sent by your Information Technology department included a [definition of spam](#) as used by this survey.

Security Password

(Unauthorised survey entry protection, and informed consent confirmation)

Please enter your organisation's Password (that was sent to you in your IT department's email) into the box below. Entering the Password also confirms you understand the Survey is Voluntary and Anonymous and you agree to continue.

IMPORTANT

This Survey is **only** about spam email you receive **at work** !

Please make sure you have the following information available:

(Note: if you have not received any spam recently, there will only be a few questions before finishing)

- 1.) How many spam emails you have received
- 2.) Over how many days these were received (e.g. 50 spam emails over 12 days)
- 3.) The approximate average time it takes you to identify and delete a spam email (e.g. 5, 10, 15 seconds etc)
- 4.) Approximately how often you delete spam (e.g. 3x per day, 5x per week etc)

Next, click the "Start" button below to begin the Survey

HTML Page 2:

Unsolicited Bulk Email (spam) Survey
Page 2 of 8

Demographics

Please provide some basic information about yourself

Q1 What is your Gender?

- Male Female

Q2 What Ethnic Group do you identify with?

Please select one

- Asian
 NZ European
 NZ Maori
 Pacific Islander
 Prefer not to say
 Other:

Q3 What is your approximate wage/salary range?
(only used for spam cost calculations)

- \$0 - \$9,999
 \$10,000 - \$19,999
 \$20,000 - \$29,999
 \$30,000 - \$39,999
 \$40,000 - \$49,999
 \$50,000 - \$59,999
 \$60,000 - \$69,999
 \$70,000 - \$79,999
 \$80,000 - \$89,999
 \$90,000 - \$99,999
 \$100,000+

Q4 Approximately how long have you been using email?

Years Months

Submit Answers

Clear All

HTML Page 3:

Unsolicited Bulk Email (spam) Survey
Page 3 of 8

Do You Receive Any Unsolicited Bulk Emails (spam)?

In the email you were sent by your Information Technology department, you were asked to save any spam emails you received over a period of about two weeks.

If you have not received **ANY** spam in the past two weeks, or are uncertain, please select "No" and submit your answer to skip to the end of the survey.

Q5 Have you ever received ANY spam emails in your work email account with your current employer?

Yes Uncertain No

Q6 Have you received any spam emails in the past two weeks approximately?

Yes No

HTML Page 4:

Unsolicited Bulk Email (spam) Survey

Page 4 of 8

How Much Unsolicited Bulk Email (spam) Do You Receive?

In the email you were sent by your Information Technology department, you were asked to save any spam emails you received over a period of about two weeks.

For these questions, you will enter four sets of numbers:

- 1.) How many spam emails you have received
- 2.) Over how many days did you receive these (e.g. 12, 13, 14 etc)
- 3.) How long you believe it took, on average, for you to identify and delete a single spam (e.g. 5 seconds)
- 4.) Approximately how often you normally delete unsolicited spam emails.

If you have not already made a note of them before starting the survey, you may need to open your email client (e.g. Microsoft Outlook) to check these numbers before entering them in the spaces below,

Q7 I have received unsolicited bulk emails (spam)

Q8 Over a period of days

Q9 It takes me, on average about seconds to identify and delete one spam email

Q10 How often, on average, do you normally delete unsolicited emails from your work mailbox (e.g. 2 times per day, 4 times per week etc) ?

(a) On average, I delete unsolicited emails about: (b) Times per: Hour Day Week Month

Q11 Do you believe you are receiving less or more spam now than a year ago?

Less Somewhat Less About the Same Somewhat More More

Unsolicited Bulk Email (spam) Survey
Page 5 of 8

Why do you receive spam? Is spam filtering working?
What do you do with some spam?

Q12 Why do you think you are receiving spam?

If you receive spam, then spammers have somehow found your email address, and listed below are some ways people think spammers may have found theirs. Choose any or all that may apply to how you think spammers found **your** email address. If the way you think they found it is not listed here, use "Other" to describe the way(s).

- I posted my email address online in a forum/blog/chat room/Instant Message
- My email address is on someone's website
- I replied to a spam email at least once
- My email address is on our organisational website
- I accidentally visited an inappropriate website
- I registered my email address on a website that may be suspect
- I don't really know

Other:

Strongly Agree Agree Neutral Disagree Strongly Disagree

Q13 Spam Filters in My Organisation:

	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
(a) Generally block spam quite well	<input type="radio"/>				
(b) Let too many spam emails through	<input type="radio"/>				
(c) Block unsolicited emails (spam) I want	<input type="radio"/>				
(d) Block good emails (non-spam) I want	<input type="radio"/>				

Q14 To the best of your knowledge, have you ever received a bounce-back email indicating that spam filters used by other people may have blocked or rejected your email? (The message should have included the words "550 ... Denied")

- Yes Uncertain No

Q15 To the best of your knowledge, have you ever accidentally deleted good emails when you were deleting spam?

- Yes Uncertain No

Q16 Have you ever opened any emails that were not "tagged" as possible spam by your organisation's email systems, but that looked to you like they were probably spam?

- Yes Uncertain No

Q17 If "Yes", what was/were the main reason(s) you opened it/them?

(e.g. in case it was a legitimate email, wanted to see what it was selling etc)

Q18 To the best of your knowledge, have you ever clicked on a graphic or http:// link contained within a spam email?

- Yes Uncertain No

Q19 If "Yes", what was the reason you clicked on it?

(e.g. wanted to see what was on the website)

Q20 To the best of your knowledge, have you ever purchased a product or service that was offered in a spam email you received?

- Yes Uncertain No

Q21 Have you ever received an unsolicited email requesting you to login using your username and password to a financial website (e.g. your Bank, PayPal etc), using a link provided in the email?

- Yes Uncertain No

Q22 If "Yes", have you ever clicked on the link provided in the email, and logged in with your username and password?

- Yes Uncertain No

Unsolicited Bulk Email (spam) Survey

Page 6 of 8

How Do You Really Feel About The Unsolicited Emails You Receive?

Q23 In overseas surveys about spam, many people have expressed their feelings or emotions about the spam they receive, and these emotions have been both positive and negative, depending on the **type** of spam they received.

Some people in these surveys said they were happy or liked to receive certain types of spam, but were also angry, worried or embarrassed about others they received.

For the types of spam email described below that you have **actually received**, choose the words from the list underneath that best describes how you feel when you receive that type of spam.

You may choose more than one word for each, but choosing "Don't Care" means other choices won't count for that type.

(a) **Selling Cheap Software**

- | | | | |
|----------------------------------|-------------------------------------|------------------------------------|--------------------------------------|
| <input type="checkbox"/> Like it | <input type="checkbox"/> Angry | <input type="checkbox"/> Disgusted | <input type="checkbox"/> Embarrassed |
| <input type="checkbox"/> Happy | <input type="checkbox"/> Frustrated | <input type="checkbox"/> Worried | <input type="checkbox"/> Don't Care |

(b) **Sexual Performance Drugs (Viagra, Cialis etc)**

- | | | | |
|----------------------------------|-------------------------------------|------------------------------------|--------------------------------------|
| <input type="checkbox"/> Like it | <input type="checkbox"/> Angry | <input type="checkbox"/> Disgusted | <input type="checkbox"/> Embarrassed |
| <input type="checkbox"/> Happy | <input type="checkbox"/> Frustrated | <input type="checkbox"/> Worried | <input type="checkbox"/> Don't Care |

(c) **Weight Loss Drugs/Programmes**

- | | | | |
|----------------------------------|-------------------------------------|------------------------------------|--------------------------------------|
| <input type="checkbox"/> Like it | <input type="checkbox"/> Angry | <input type="checkbox"/> Disgusted | <input type="checkbox"/> Embarrassed |
| <input type="checkbox"/> Happy | <input type="checkbox"/> Frustrated | <input type="checkbox"/> Worried | <input type="checkbox"/> Don't Care |

(d) **Male Enhancement/Enlargement Products**

- | | | | |
|----------------------------------|-------------------------------------|------------------------------------|--------------------------------------|
| <input type="checkbox"/> Like it | <input type="checkbox"/> Angry | <input type="checkbox"/> Disgusted | <input type="checkbox"/> Embarrassed |
| <input type="checkbox"/> Happy | <input type="checkbox"/> Frustrated | <input type="checkbox"/> Worried | <input type="checkbox"/> Don't Care |

(e) **Mortgage/Loan Financing**

- | | | | |
|----------------------------------|-------------------------------------|------------------------------------|--------------------------------------|
| <input type="checkbox"/> Like it | <input type="checkbox"/> Angry | <input type="checkbox"/> Disgusted | <input type="checkbox"/> Embarrassed |
| <input type="checkbox"/> Happy | <input type="checkbox"/> Frustrated | <input type="checkbox"/> Worried | <input type="checkbox"/> Don't Care |

(f) **Job/Employment Offers**

- | | | | |
|----------------------------------|-------------------------------------|------------------------------------|--------------------------------------|
| <input type="checkbox"/> Like it | <input type="checkbox"/> Angry | <input type="checkbox"/> Disgusted | <input type="checkbox"/> Embarrassed |
| <input type="checkbox"/> Happy | <input type="checkbox"/> Frustrated | <input type="checkbox"/> Worried | <input type="checkbox"/> Don't Care |

(g) **Adult Pornography Websites**

- | | | | |
|----------------------------------|-------------------------------------|------------------------------------|--------------------------------------|
| <input type="checkbox"/> Like it | <input type="checkbox"/> Angry | <input type="checkbox"/> Disgusted | <input type="checkbox"/> Embarrassed |
| <input type="checkbox"/> Happy | <input type="checkbox"/> Frustrated | <input type="checkbox"/> Worried | <input type="checkbox"/> Don't Care |

(h) **Child Pornography Websites**

- | | | | |
|----------------------------------|-------------------------------------|------------------------------------|--------------------------------------|
| <input type="checkbox"/> Like it | <input type="checkbox"/> Angry | <input type="checkbox"/> Disgusted | <input type="checkbox"/> Embarrassed |
| <input type="checkbox"/> Happy | <input type="checkbox"/> Frustrated | <input type="checkbox"/> Worried | <input type="checkbox"/> Don't Care |

(i) **Dating Websites**

- | | | | |
|----------------------------------|-------------------------------------|------------------------------------|--------------------------------------|
| <input type="checkbox"/> Like it | <input type="checkbox"/> Angry | <input type="checkbox"/> Disgusted | <input type="checkbox"/> Embarrassed |
| <input type="checkbox"/> Happy | <input type="checkbox"/> Frustrated | <input type="checkbox"/> Worried | <input type="checkbox"/> Don't Care |

(j) **Stock Market "Tips"**

- | | | | |
|----------------------------------|-------------------------------------|------------------------------------|--------------------------------------|
| <input type="checkbox"/> Like it | <input type="checkbox"/> Angry | <input type="checkbox"/> Disgusted | <input type="checkbox"/> Embarrassed |
| <input type="checkbox"/> Happy | <input type="checkbox"/> Frustrated | <input type="checkbox"/> Worried | <input type="checkbox"/> Don't Care |

(k) **Online Casino Websites**

- | | | | |
|----------------------------------|-------------------------------------|------------------------------------|--------------------------------------|
| <input type="checkbox"/> Like it | <input type="checkbox"/> Angry | <input type="checkbox"/> Disgusted | <input type="checkbox"/> Embarrassed |
| <input type="checkbox"/> Happy | <input type="checkbox"/> Frustrated | <input type="checkbox"/> Worried | <input type="checkbox"/> Don't Care |

(l) **"Nigerian" Fraud (i.e. want to deposit \$xx million in your bank account)**

- | | | | |
|----------------------------------|-------------------------------------|------------------------------------|--------------------------------------|
| <input type="checkbox"/> Like it | <input type="checkbox"/> Angry | <input type="checkbox"/> Disgusted | <input type="checkbox"/> Embarrassed |
| <input type="checkbox"/> Happy | <input type="checkbox"/> Frustrated | <input type="checkbox"/> Worried | <input type="checkbox"/> Don't Care |

(m) **Selling Other General Products/Services**

- | | | | |
|----------------------------------|-------------------------------------|------------------------------------|--------------------------------------|
| <input type="checkbox"/> Like it | <input type="checkbox"/> Angry | <input type="checkbox"/> Disgusted | <input type="checkbox"/> Embarrassed |
| <input type="checkbox"/> Happy | <input type="checkbox"/> Frustrated | <input type="checkbox"/> Worried | <input type="checkbox"/> Don't Care |

Q24 **What Are Your Feelings About Spam in General?**

- | | | | |
|----------------------------------|-------------------------------------|------------------------------------|--------------------------------------|
| <input type="checkbox"/> Like it | <input type="checkbox"/> Angry | <input type="checkbox"/> Disgusted | <input type="checkbox"/> Embarrassed |
| <input type="checkbox"/> Happy | <input type="checkbox"/> Frustrated | <input type="checkbox"/> Worried | <input type="checkbox"/> Don't Care |

Submit Answers

Clear All

HTML Page 7:

Unsolicited Bulk Email (spam) Survey

Page 7 of 8

Q25 - When I receive spam...

	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
(a) It is a waste of my time at work	<input type="radio"/>				
(b) I worry that fellow employees might see it	<input type="radio"/>				
(c) It makes me angry	<input type="radio"/>				
(d) I enjoy receiving it	<input type="radio"/>				
(e) It is an intrusion on my privacy	<input type="radio"/>				
(f) I delete them immediately	<input type="radio"/>				
(g) They are sometimes interesting to read	<input type="radio"/>				
(h) The email was sent by the person it says it is "From:"	<input type="radio"/>				
(i) I sometimes forward it on to colleagues or friends	<input type="radio"/>				
(j) It makes me frustrated	<input type="radio"/>				

	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
(k) I believe they are mostly deceptive or fraudulent	<input type="radio"/>				
(l) I have sometimes replied to it	<input type="radio"/>				
(m) I sometimes report it to my manager or IT Department	<input type="radio"/>				
(n) I sometimes find the content of the email is objectionable	<input type="radio"/>				
(o) I am concerned I might accidentally delete good emails with the spam	<input type="radio"/>				
(p) I wish the IT Department would do more to stop it	<input type="radio"/>				
(q) I am worried I am receiving it because I might have accidentally visited a website with similar content	<input type="radio"/>				
(r) I hate receiving it	<input type="radio"/>				
(s) I worry my colleagues or manager might see me reading it, if it is objectionable content	<input type="radio"/>				

HTML Page 8:

Survey Complete !

Thank you for completing the survey.

Your participation is greatly appreciated, and will assist in understanding the impact that spam has on New Zealand organisations and their employees.

Any Final Comments?

If you have any comments that you would like to add about spam, how you feel about it, or how it is affecting you at work, please enter them here before clicking on the "Finished" button to complete the survey.
Thank you.

Spam Definition (Link on Login Page)

Unsolicited Bulk Email (spam) Survey

Definition Of Spam

For the purposes of this research, Unsolicited Bulk Email (UBE, or spam), is defined as:

"Any substantially identical emails sent to large numbers of email addresses, from a sender unknown to recipients who had not given permission for the email to be sent"

This definition is intended to include:

Unsolicited Commercial Email (UCE) marketing products or services such as Viagra, Job Offers or pornographic web sites, Fraud or identity-theft emails such as Nigerian scams and "phishing" attempts (that ask you to go to a bank or financial website such as PayPal and enter your username and password).

DO NOT count emails you may have received that contained viruses, or emails sent within your organisation to some form of "All Users" distribution list.

Appendix D – UBE Cost Analysis Spreadsheet Model

14	Basics	Organisation (Column F)
15	Number of email accounts	0
16	Average fully loaded annual salary per employee	0
17	Average number of working days per person per year	0
18	Total number of emails received per day	0
19	Total number of detected spam blocked/tagged per day	0
20	Average employee cost per hour	=IF(F17>0,F16/(F17*7.5),"")
21	Total percentage of email that is detected as spam	=IF(F18>0,F19/F18,"")
22		
23	Filtering costs	
24	Hardware cost (per year)	0
25	Software/Licensing cost (per year)	0
26	Appliance cost (per year)	0
27	Total cost of spam filtering per year	=SUM(F24:F26)
28		
29	Lost Productivity costs	
30	Measured spam per user per day (mean)	0
31	Average time to handle a spam (seconds)	0
32	Calculated spam per user per day	=IF(F27>0,F30,MAX(F30,F19/F15))
33	Average time to handle spam per user per day (minutes)	=(F32*F31)/60
34	Average cost to handle spam per user per day	=IF(F33>0,F20*(F33/60),"")
35	Total cost to handle spam per year	=IF(F17>0,F15*F34*F17,0)
36		
37	Connectivity costs	
38	Cost of office Internet connectivity per month	0
39	Cost of remote connectivity per month	0
40	Bandwidth used by e-mail	0
41	Total cost of Internet connectivity per month	=F38+F39
42	Cost of bandwidth used by spam per year	=F41*F40*F21*12
43		
44	Support costs	
45	Average cost of user support per user per year	0
46	Percentage of support time re spam	0
47	Cost of spam-related support per user per year	=F45*F46
48	Total cost of spam-related support per year	=F15*F47
49		
50	Total Costs	
51	Connectivity	=F42
52	Filtering	=F27
53	Support	=F48
54	Lost Productivity	=F35
55		
56	Total cost of spam per year	=SUM(F51:F54)
57	Total cost of spam per user per year	=F56/F15

Modified spreadsheet model used with permission of Mark Gibbs of Network World
(downloadable from: <http://www.networkworld.com/columnists/2003/0707backspin.html>)

Appendix E – Employee Interview Forms

Invitation to Participate Form



Information for Participants

The Socio-Economic Impact of Unsolicited Bulk Email (UBE) on Organisations in New Zealand

I am a Master of Computing student at Unitec New Zealand, Mt Albert, Auckland. Part of my degree programme involves a research paper on a subject of our choice. My research topic looks at the impact of unsolicited bulk email on organisations in New Zealand. I am doing this research at several organisations, and have the approval of your organisation to carry out the research.

What I am doing

What I want to find out for this research, is how unsolicited bulk email (often called “spam” or “junk email”) is affecting organisations in New Zealand, and how it is affecting the employees of these organisations.

What it will mean for you

I wish to interview you and talk about:

- what you know about unsolicited bulk emails
- what sort of unsolicited emails you are receiving
- how you feel about the unsolicited emails you are receiving
- what you do with the unsolicited emails you receive
- what opinions you have about unsolicited emails and how your organisation deals with them

I would like it if you could meet with me for up to 45 minutes during work time to talk about these kinds of things. I will be taping the interview and will be transcribing it (typing the conversation out) later. No information that could identify you will be requested, but the information on the tapes will be kept as an electronic audio file in case this needs to be referenced, for up to 5 years. Nobody but I or my Supervisor will have access to this file during this time.

You are free to withdraw from this project for whatever reason within two weeks of the interview.

What I will do with this information

By taking part in this research you will be helping me to understand how unsolicited email is affecting you and your ability to do your job, and how in turn this affects your organisation.

Consent

If you agree to participate, you will be asked to sign a consent form. This does not stop you from changing your mind if you wish to withdraw from the project. However, because of my schedule, any withdrawals must be done within 2 weeks after I have interviewed you, so that I may try to schedule an interview with other employees if necessary.

Please contact me if you need more information about the project:

Brian Foster, Ph: 815-4321 x8255, Email: xxx@unitec.ac.nz

At any time if you have any concerns about the research project you can contact my supervisor:

Donald Joyce, Ph: 815-4321 x6065, Email xxx@unitec.ac.nz

Confidentiality

Your name and information that may identify you will be kept completely confidential. All information collected from you will be stored in a protected file and the only people allowed access to this information will be yourself, I and my two supervisors.

Thank you!

This study has been approved by the Unitec Research Ethics Committee from 21 February 2007 to 1 July 2007. If you have any complaints or reservations about the ethical conduct of this research, you may contact the Committee through the UREC Secretariat (Ph: 09 815 4321 ext.7254). Any issues you raise will be treated in confidence and investigated fully, and you will be informed of the outcome.

Interview Consent Form



Participation Consent

The Socio-Economic Impact of Unsolicited Bulk Email (UBE) on Organisations in New Zealand

This consent form will help provide information for a research project looking at the socio-economic impact of Unsolicited Bulk Emails (spam, or "junk" mail) in organisations in New Zealand

I have had the research project explained to me and I have read and understand the information sheet given to me.

I understand that I don't have to be part of this if I don't want to and I may withdraw at any time prior to the completion of the research project.

I understand that everything I say is confidential and none of the information I give will identify me and that the only persons who will know what I have said will be the researchers and their supervisor. I also understand that all the information that I give will be stored securely on a computer at Unitec for a period of 5 years.

I understand that my discussion with the researcher will be taped and transcribed.

I understand that I can see the finished research document.

I am aware that I may contact the Research Supervisor/Coordinator, Donald Joyce, at Unitec (09) 815-4321 ext. 6065, if I have any queries about the project.

I have had time to consider everything and I give my consent to be a part of this.

Participant Signature: *Date:*

Project Researcher: *Date:*

This study has been approved by the Unitec Research Ethics Committee from 21 February 2007 to 1 July 2007. If you have any complaints or reservations about the ethical conduct of this research, you may contact the Committee through the UREC Secretariat (Ph: 09 815 4321 ext.7254). Any issues you raise will be treated in confidence and investigated fully, and you will be informed of the outcome.

Appendix F – Individual Employee Interviews

Impact of UBE on New Zealand Organisations Individual Employee Interviews					
Organisation:	1	Gender:	M	Date:	07-12-2006
Participant #:	1			Time:	3:02pm

Q1 What do you know about Unsolicited Bulk Emails?**a.) Have you read, heard or seen much about UBE (spam) in the media (e.g. newspapers, magazines, radio, TV)?**

A: Only relating to potential viruses, and what're they called, spy ware, things like that. That's really about the only thing I've taken notice, apart from when it comes to spam, 'cause I've got a computer at home that runs through Xtra, and you're sort of always aware that they could have? (*words unclear**)

b.) Has your organisation provided you with any information about UBE? (0:55)

A: Yeah, the I.T. department essentially tells you just to "delete them, don't even open them", so, that's essentially the advice you get. Up until recently the (anti-spam product named) has picked up most of them, I think it's just they seem to be sneaking through now I think they've loosened it up, but yeah, there was a time when virtually none of them got through, any that did we just deleted.

Q: Do they advise you of anything that's happening in terms of changes they've made to the system?

A: Yes, yes they do, recently that's why I was aware that more spam was coming through and yet there's actually now something they've done, they've changed something over there 'cause it comes through now with a thing called "spam" on it, whereas we never had that before...

Q: A Tag?

A: Yes, so, and they did say that they'd changed the parameters and loosened something up because it was stopping too many authorised emails so they have done something and they did pre-warn us that that was going to happen so, yes, delete, delete, delete.

c.) If so, what sort of information? (02:00)

Q: The other question was if so, what sort of information, so I guess you've answered that one.

d.) What do you believe might be the reason(s) you receive UBE; how do you think the spammers got your email address? (02:06)

Q: Now I'm assuming that you've been chosen because I asked them to randomly choose people, I assume the reason is because you are receiving some spam?

A: Yes

Q: So if you are receiving spam, what do you believe might be the reason(s) that you're receiving it, and if you're receiving it they've obviously got your email address, so do you have any ideas how they might have got your email address?

A: No, I wouldn't have a..., mind you I'm a (*job title**) so my, because I choose (*items**) for a living, my email address is on all sorts of international (*item**) databases so I'm guessing that's possibly where I'm getting them from ahead of maybe anyone else, so

yeah, I don't know, but yeah, most people's email addresses here would be, are internal, whereas mine may be on some external databases somewhere, so, I would guess that's possibly why.

Q2 What can you tell me about the Unsolicited Bulk Emails you receive? (03:03)

a.) Thinking about the different types of UBE you have received in the past, which of the following types have you received, in your email account with this organisation, to the best of your knowledge? (Participant responses as below)

- Selling Cheap Software
- Sexual Performance Drugs (Viagra, Cialis etc)
- Weight Loss Drugs/Programmes
- Male Enhancement/Enlargement Products
- Mortgage/Loan Financing
- Job/Employment Offers
- Adult Pornography Websites
- Child Pornography Websites
- Dating Websites
- Stock Market "Tips"
- Online Casino Websites
- "Nigerian" Fraud (i.e. want to deposit \$xx million in your bank account)
- Selling Other General Products/Services

b.) To the best of your knowledge, has the amount of unsolicited email you receive increased or decreased in the past 12 months (or less than 12 months if not employed with this organisation for that long)? (04:07)

A: Increased, dramatically

Q: Increased dramatically?

A: Yes. Especially bloody Viagra stuff, whoo daddy, that's just, through the roof.

Q3 How do you feel about Unsolicited Bulk Emails? (04:34)

a.) For each of these different types of UBE you have indicated you have received in q2, what emotions from the following list would best describe how you feel about each type? If you found any of these types of email particularly offensive or objectionable, please indicate this next to the UBE type also. (Participant responses as below)

Selling Cheap Software

- Like it Angry Disgusted Embarrassed Particularly
 Happy Frustrated Worried Don't Care Offensive

Sexual Performance Drugs (Viagra, Cialis etc)

- Like it Angry Disgusted Embarrassed Particularly
 Happy Frustrated Worried Don't Care Offensive

Weight Loss Drugs/Programmes

- Like it Angry Disgusted Embarrassed Particularly
 Happy Frustrated Worried Don't Care Offensive

Male Enhancement/Enlargement Products

- Like it Angry Disgusted Embarrassed Particularly
 Happy Frustrated Worried Don't Care Offensive

Mortgage/Loan Financing

- Like it Angry Disgusted Embarrassed Particularly
 Happy Frustrated Worried Don't Care Offensive

Job/Employment Offers

- Like it Angry Disgusted Embarrassed Particularly
 Happy Frustrated Worried Don't Care Offensive

Adult Pornography Websites

- Like it Angry Disgusted Embarrassed Particularly
 Happy Frustrated Worried Don't Care Offensive

Child Pornography Websites

- Like it Angry Disgusted Embarrassed Particularly
 Happy Frustrated Worried Don't Care Offensive

Dating Websites

- Like it Angry Disgusted Embarrassed Particularly
 Happy Frustrated Worried Don't Care Offensive

Stock Market "Tips"

- Like it Angry Disgusted Embarrassed Particularly
 Happy Frustrated Worried Don't Care Offensive

Online Casino Websites

- Like it Angry Disgusted Embarrassed Particularly
 Happy Frustrated Worried Don't Care Offensive

"Nigerian" Fraud (i.e. want to deposit \$xx million in your bank account)

- Like it Angry Disgusted Embarrassed Particularly
 Happy Frustrated Worried Don't Care Offensive

Selling Other General Products/Services

- Like it Angry Disgusted Embarrassed Particularly
 Happy Frustrated Worried Don't Care Offensive

What Are Your Feelings About Spam in General?

- Like it Angry Disgusted Embarrassed Particularly
 Happy Frustrated Worried Don't Care Offensive

Q3 How do you feel about Unsolicited Bulk Emails (Contd...)

b.) If you found any of the unsolicited emails you received offensive or objectionable, have you ever opened any of these emails when your work colleague(s) or manager(s) were present, or able to see your computer screen? (06:48)

Q: The next question was: If you found any of these emails offensive or objectionable, which I don't think you actually did, did you?

A: No

Q: The question was going to be: have you ever opened any of these when any of your work colleagues or managers were present, or able to see your computer screen?

A: No, anything that comes up as spam, or anything that essentially comes up that I don't know who it's from, or that it doesn't look legit, I just delete straight away without even opening it, so... Too busy to be worrying about stuff like that I'm afraid.

c.) If so, how did you feel in this situation? N/A

d.) If not, how do you think you might feel in that situation? (07:24)

Q: This is a sort of conjectural question: If you did happen to open something like that, when somebody was present and one of these types of offensive emails might happen to come up, how do you think you might feel in that sort of situation?

A: I wouldn't really, I wouldn't care personally, but I might be a little, I might be concerned that people think I'm, you know, surfing offensive sites in company time, which would be my only concern but it doesn't offend me nothing would offend me. And also I'd be worried about, you know, getting red-flagged from the I.T. department more than anything, that'd be about it.

Q4 What do you do with Unsolicited Bulk Emails? (08:12)

a.) If participant has indicated they have received any unsolicited emails requesting personal information including a login/password (e.g. for a bank account, Paypal account etc) in section 2), then ask:

For any of the unsolicited emails you indicated you have received that requested you provide login/password information for a bank or other online financial website, have you ever:

(i) Clicked on the link provided in the email?

(ii) Entered your login ID and password?

Q: I just have to again check your responses to see if you've ever received an email requesting personal information.

A: I may well have but I probably wouldn't have opened them so I wouldn't know.

Q: Have you ever received anything requesting personal information such as login to a banking site or your Paypal account?

A: I've seen a couple of those Nigerian things just in the sort of preview thing as I'm going through and I've just deleted it straight away, but I have received them, yes.

Q: But you haven't received any that have actually asked you to, you know, click here and login and provide your password or anything like that?

A: No, I've had ones that have asked, you know, to submit all your information, but never actually anything quite that carried away, no.

Q: Not to that extent, ok.

(i) No

(ii) N/A

b.) For any other non-financial unsolicited emails, have you ever clicked on any links included in unsolicited emails you have received? (9:09)

A: No

c.) If “Yes”, what was the reason you clicked on it? e.g. it was an “Unsubscribe” or “Stop receiving” link, or you wanted to see what was on the website because it looked interesting, what? N/A

d.) Have you at any time purchased any products or services offered in an unsolicited email?

A: No

e.) What do you normally do with the unsolicited emails you receive? (09:33)

Delete them?

Report them to the IT Department?

Forward them to the IT Department?

Reply to them?

Other?

Q: I think you’ve already partly answered this question, well, mostly answered this question, do you delete them?

A: Yeah, absolutely

Q: Do you at all report them to the IT Department?

A: No

Q: Do you forward them to the IT department at any time, for any reason?

A: Nope, too busy

Q: Have you ever replied to any of them, saying “please delete me”, or “unsubscribe me” or something?

A: No, I got myself unsubscribed from “Old Friends”, which I thought was a great idea at the time, but, actually funny you should say that because through “Old Friends” I’d heard that people were getting signed up for that Nigerian, I heard of someone there who had access to “Old Friends” database so I unsubscribed myself from that just to take myself out of the loop there.

Q: You thought it was a precaution?

A: Yeah, I’d heard that someone had gone through and looked at Old Friends and then found some of the connections and said “Hi, this is so-and-so, remember me from High School. Hey, I need some help with you know, handling some money I need to blah, blah, blah, the old Nigerian scam..

Q: It actually came through the Old Friends...?

A: (??? slightly garbled) or whether it’s an Urban Myth but I thought, well I’m not prepared to take that risk so I unsubscribed just on the off-chance. Pain-in-the-***

Q: Apart from deleting them is there anything else that you do with them normally, that’s basically it?

A: No

Q5 What are your opinions about Unsolicited Bulk Emails? (10:54)

a.) Do you think that unsolicited emails waste your time at work? (11:05)

A: Yes. Well they do, yeah, they would more so if I opened them, but even going through and deleting them is a pain-in-the-***, I've got better things to do. But if the (anti-spam vendor name) would delete them all and still let through, obviously which is the balancing act with (anti-spam vendor name), then I'd be a happy man. I don't need to get Viagra ads every f*** day at work, thank you very much.

b.) Do you think they are a waste of your organisation's time and money? (11:30)

A: Yeah, absolutely they are. Look I'm quite I.T. savvy.

Q: Apart from your own time and money...

A: Yeah, I'd imagine some people aren't quite as I.T. savvy, and certainly, you know, some of the blokes around here would probably be like, ahaha, open them up and, oh God, yeah, huge waste of time.

c.) How well do you think your organisation is doing in controlling the amount of unsolicited email that you receive? Is it doing a good job, a poor job? (11:48)

A: Yeah, I think the I.T. department are fantastic, and yeah, I think they're doing the best they can I'd imagine, with the resources they've got, but it's always gonna be a bit tough (??? Garbled, road noise), I think they're doing the best they can. They certainly seem to be aware of it, and always trying to deal with it. Certainly if there's a new virus threat that comes out they're onto it very, very quickly, so, they're pretty switched-on.

d.) Do you think more could be done by your organisation to control unsolicited email? (12:18)

A: I would imagine anything within budget that can be done, they're doing it. I don't know how much more they can do. I don't know whether it's a budgetary thing or a software thing, but I'm sure within reason that anything that reasonably can be done is being done.

e.) If "Yes", what more do you think they could do to control it? N/A

f.) Do you think your organisation could provide you with more information about unsolicited email? (12:48)

Q: You've said that they have already advised people to delete it; do you think that they could provide you with any more information about it?

A: I don't really think, I'd certainly personally think that I've got enough knowledge just to delete them, although I'm sure some other people may be new, staff members may not have got that message, so, it's possibly something they need to be reminded of, but, as someone who's been with the company for a long time I'm aware of the company policy, and what to do, and, you know, especially when my own home email address is through the work address, even though I have an Xtra, I do use Xtra but I sign straight into the company account so, you know, certainly if I'm at home and I know that my laptop is susceptible to viruses so, you know, certainly at home, just delete them all, 'cause it's not going to get too many viruses on here, but the last thing I want is b***** spyware on my laptop.

g.) If "Yes", what information do you think they should provide? N/A

Impact of UBE on New Zealand Organisations Individual Employee Interviews				
Organisation:	1	Gender: F	Date:	15-12-06
Participant #:	2		Time:	10:32am

Q1 What do you know about Unsolicited Bulk Emails? (0:25)

a.) Have you read, heard or seen much about UBE (spam) in the media (e.g. newspapers, magazines, radio, TV)? (0:31)

A: Yes

Q: Do you remember which media at all, approximately?

A: All the major, you know, all the major newspapers have had stuff on spam, the Listener, Time, Newsweek.

Q: Ok, anything on TV?

A: Not that I can remember, but probably.

b.) Has your organisation provided you with any information about UBE? (1:05)

A: A little bit

Q: What have they told you?

A: They have said they work very hard to stop it reaching us

c.) If so, what sort of information? (1:21)

Q: Have they actually provided you with any formal information about “this is what spam is”?

A: Not that I can recall. I think they assume we all know.

d.) What do you believe might be the reason(s) you receive UBE; how do you think the spammers got your email address? (1:43)

A: I think it's off, clicking onto a particular website somehow, you know, it records your email address or cookies or whatever, and then it gets handed around to these nefarious people.

Q2 What can you tell me about the Unsolicited Bulk Emails you receive? (2:23)

a.) Thinking about the different types of UBE you have received in the past, which of the following types have you received, in your email account with this organisation, to the best of your knowledge? (Participant responses as below)

- Selling Cheap Software
- Sexual Performance Drugs (Viagra, Cialis etc)
- Weight Loss Drugs/Programmes
- Male Enhancement/Enlargement Products
- Mortgage/Loan Financing
- Job/Employment Offers
- Adult Pornography Websites
- Child Pornography Websites
- Dating Websites
- Stock Market "Tips"
- Online Casino Websites
- "Nigerian" Fraud (i.e. want to deposit \$xx million in your bank account)
- Selling Other General Products/Services

b.) To the best of your knowledge, has the amount of unsolicited email you receive increased or decreased in the past 12 months (or less than 12 months if not employed with this organisation for that long)? (3:23)

A: Increased.

Q: Definitely increased?

A: Definitely increased.

Q: Have you noticed whether the amount that it's increased by, has it been tagged in particular, like, you're getting more that's actually coming through as being tagged as spam, or is it coming through as completely untagged?

A: I would say 99% of it is tagged as spam. It's only rarely that I'd get a spam that isn't tagged. Of course sometimes I get some tagged as spam that aren't.

Q: False positives they're called.

A: Are they?

Q: Legitimate emails, but they've actually been tagged.

A: Yeah.

Q3 How do you feel about Unsolicited Bulk Emails? (4:56)

a.) For each of these different types of UBE you have indicated you have received in q2, what emotions from the following list would best describe how you feel about each type? If you found any of these types of email particularly offensive or objectionable, please indicate this next to the UBE type also. (Participant responses as below)

Selling Cheap Software

- Like it Angry Disgusted Embarrassed Particularly
 Happy Frustrated Worried Don't Care Offensive

Sexual Performance Drugs (Viagra, Cialis etc)

- Like it Angry Disgusted Embarrassed Particularly
 Happy Frustrated Worried Don't Care Offensive

Weight Loss Drugs/Programmes

- Like it Angry Disgusted Embarrassed Particularly
 Happy Frustrated Worried Don't Care Offensive

Male Enhancement/Enlargement Products

- Like it Angry Disgusted Embarrassed Particularly
 Happy Frustrated Worried Don't Care Offensive

Mortgage/Loan Financing

- Like it Angry Disgusted Embarrassed Particularly
 Happy Frustrated Worried Don't Care Offensive

Job/Employment Offers

- Like it Angry Disgusted Embarrassed Particularly
 Happy Frustrated Worried Don't Care Offensive

Adult Pornography Websites

- Like it Angry Disgusted Embarrassed Particularly
 Happy Frustrated Worried Don't Care Offensive

Child Pornography Websites

- Like it Angry Disgusted Embarrassed Particularly
 Happy Frustrated Worried Don't Care Offensive

Dating Websites

- Like it Angry Disgusted Embarrassed Particularly
 Happy Frustrated Worried Don't Care Offensive

Stock Market "Tips"

- Like it Angry Disgusted Embarrassed Particularly
 Happy Frustrated Worried Don't Care Offensive

Online Casino Websites

- Like it Angry Disgusted Embarrassed Particularly
 Happy Frustrated Worried Don't Care Offensive

"Nigerian" Fraud (i.e. want to deposit \$xx million in your bank account)

- Like it Angry Disgusted Embarrassed Particularly
 Happy Frustrated Worried Don't Care Offensive

Selling Other General Products/Services

- Like it Angry Disgusted Embarrassed Particularly
 Happy Frustrated Worried Don't Care Offensive

What Are Your Feelings About Spam in General?

- Like it Angry Disgusted Embarrassed Particularly
 Happy Frustrated Worried Don't Care Offensive

Q3 How do you feel about Unsolicited Bulk Emails (Contd...)

b.) If you found any of the unsolicited emails you received offensive or objectionable, have you ever opened any of these emails when your work colleague(s) or manager(s) were present, or able to see your computer screen? (6:42)

A: No. I've had one child pornog... well it appeared... I didn't open it, child pornography site, and I, without even thinking sent it to the boss, to xxx, and to the IT guy, xxx, and said "what are you going to do about it", and they went "oh, it's too hard", so I sent it to the cops, so that at least it's on their database.

Q: You didn't open it?

A: I assumed that it, because it talked about sex with young children that probably it wasn't...

Q: Yeah, that was on the subject of...

A: That was just a hook, and it was (*words unclear**)

c.) If so, how did you feel in this situation? (7:50)

Q: You haven't opened it in front of anybody, but...

A: I was horrified

Q: But you haven't opened it in front of anybody, so...

d.) If not, how do you think you might feel in that situation?

Q: If you happened to open something like that, of that nature, and somebody was there with you?

A: I'd be horrified. Absolutely appalled.

Q4 What do you do with Unsolicited Bulk Emails? (8:25)

a.) If participant has indicated they have received any unsolicited emails requesting personal information including a login/password (e.g. for a bank account, Paypal account etc) in section 2), then ask:

For any of the unsolicited emails you indicated you have received that requested you provide login/password information for a bank or other online financial website, have you ever:

(i) Clicked on the link provided in the email?

(ii) Entered your login ID and password?

Q: You have received some of a type which was like a Nigerian Fraud, have you received anything similar to that, which is what they call "phishing", like of a type, a nature where they pretend to be a bank, and they want you to login?

A: Yes. There was a whole spate of those last year. They seem to have dropped off now.

(i) Never in a million years.

(ii) N/A

b.) For any other non-financial unsolicited emails, have you ever clicked on any links included in unsolicited emails you have received? (9:32)

A: Probably two or three times, I suspect

c.) If “Yes”, what was the reason you clicked on it? e.g. it was an “Unsubscribe” or “Stop receiving” link, or you wanted to see what was on the website because it looked interesting, what?

A: I did that once until somebody said, “please don’t do that”, so I stopped doing it, and the other two or three would have been where I thought it was somebody with a xxx idea, so I thought it was somebody in the industry. Just from the way that the letter was written, and then once you’ve gone through, you realise that, it ain’t.

d.) Have you ever at any time ever purchased any products or services offered in an unsolicited email? (10:56)

A: No.

e.) What do you normally do with the unsolicited emails you receive? (11:04)

Delete them?

Report them to the IT Department?

Forward them to the IT Department?

Reply to them?

Other?

A: Delete them.

Q: I think you did mention that you’ve reported them or forwarded them to the IT department.

A: Once.

Q: You forwarded them that one once, but you normally just delete them?

A: What’re they gonna do?

Q5 What are your opinions about Unsolicited Bulk Emails? (11:46)

a.) Do you think that unsolicited emails waste your time at work?

A: Yeah.

b.) Do you think they are a waste of your organisation's time and money? (11:59)

A: Yeah. Very.

Q: Very much so?

A: Yeah, very much so.

c.) How well do you think your organisation is doing in controlling the amount of unsolicited email being received? Is it doing a good job, a poor job? (12:09)

A: They used to do a, you know, almost 100% job, but, it was found they were stopping too many legitimate emails, that just happened to sort of look like, feel like spam, and...

Q: False positives

A: False positives, and, you know, it caused us some distress at not getting legitimate emails, so they, I don't know what the correct term is, but it is as if they've slightly loosened...

Q: They've loosened it up?

A: ...the barrier, and, so I get probably 20 a day now. Before I would have got 2. But I don't find that (uncertain of actual words, think it was the following) all that obnoxious.

Q: Does that mean you think they're doing a good job, or in your opinion you think maybe they're doing not quite so good a job because they're letting more through, or...?

A: I've no opinion really. All I know is that we can't have emails stopped, legitimate emails stopped, and if they have no way of absolutely determining, that, for example they often stop xxx's, because xxx's have big attachments, and the form of that is, somebody will say "It's coming now, there might be a message that's coming now. Here it is. Hope you like it". Some kind of impersonal, what appears to be a sort of impersonal message, and then there's this f... great attachment, of, you know, it might be 200 pages of xxx, and they stop that. But now we get a message saying "We've stopped one of these things" as well, which is good. They're probably doing as best job as they're able, yeah, I think, in my opinion, with the resources they have available to them.

d.) Do you think more could be done by your organisation to control unsolicited email? (14:52)

A: I mean the only way you can do, really, is to stop it, you know, entering the systems in the first place, back from over there, really, isn't it?

Q: You think there's probably not much more they can be doing, they're doing the best they can?

A: I think so, yeah, I do.

e.) If "Yes", what more do you think they could do to control it? N/A

f.) Do you think your organisation could provide you with more information about unsolicited email? (15:33)

A: No

g.) If "Yes", what information do you think they should provide? N/A

Impact of UBE on New Zealand Organisations Individual Employee Interviews				
Organisation:	1	Gender: M	Date:	20/12/06
Participant #:	3		Time:	1:07pm

Q1 What do you know about Unsolicited Bulk Emails? (00:26)

a.) Have you read, heard or seen much about UBE (spam) in the media (e.g. newspapers, magazines, radio, TV)?

A: I have, I have seen some on TV, I think “Campbell Live” might have done something about spam and things, and the others would be from my local ISP, which have said that, you know, emails have been blocked due to over-spamming.

Q: Right, yes I think I recall that one too

A: Yes, I think Telecom and Ihug got involved in that one.

b.) Has your organisation provided you with any information about UBE? (01:00)

A: Yes, yes, there’s been notices quite regularly about, you know, what to do with it, and that, you know, they try and stop as much as they can with it.

Q: Do they actually provide you with any written information at all, or just email?

A: They email us saying “If this happens, respond to it this way, or don’t respond to it at all and just delete it”, so there’s instructions on what to do when you see it come through, and it’s quite clear what to do.

c.) If so, what sort of information?

As above.

d.) What do you believe might be the reason(s) you receive UBE; how do you think the spammers got your email address? (01:45)

A: It’ll be from other people’s mailboxes, that I communicate with outside work, sorry, within work, like the agencies I deal with and who I regularly email, I know that they are big organisations with big contacts and so it goes on and on, so I guess the flow effect is from them coming back into me.

Q: Ok, so you think that the information is being passed on by other people somehow.

A: Somehow, yeah, using my attachments, using my emails as a group email with their agencies or their clients and things that, it just flows on from there. And it’s probably accidental that they’re using my email to communicate with other people.

Q2 What can you tell me about the Unsolicited Bulk Emails you receive? (03:00)

a.) Thinking about the different types of UBE you have received in the past, which of the following types have you received, in your email account with this organisation, to the best of your knowledge? (Participant responses as below)

- Selling Cheap Software
- Sexual Performance Drugs (Viagra, Cialis etc)
- Weight Loss Drugs/Programmes
- Male Enhancement/Enlargement Products
- Mortgage/Loan Financing
- Job/Employment Offers
- Adult Pornography Websites
- Child Pornography Websites
- Dating Websites
- Stock Market "Tips"
- Online Casino Websites
- "Nigerian" Fraud (i.e. want to deposit \$xx million in your bank account)
- Selling Other General Products/Services

b.) To the best of your knowledge, has the amount of unsolicited email you receive increased or decreased in the past 12 months (or less than 12 months if not employed with this organisation for that long)? (03:55)

A: That's decreased

Q: Decreased?

A: For me it's decreased. I don't see as much as I did this time last year, so it's decreasing. It's still present, but it's not as... I used to get bulk, like, I'd come back from a weekend and there'd be so much of it there, but now I'm having just one or two quirky little things.

Q: As part of that question, if you look at the total quantity of spam you've received, there'll be some that will get through the spam filters that will be not tagged and there'll be some that has been tagged..

A: Yes, that's newer stuff, it's newer

Q: The whole quantity has decreased altogether

A: Yes, yes, absolutely

Q: Have you noticed any change in the amount that's been tagged or the amount that's not tagged?

A: I'm not too sure what's been tagged, what do you mean by "tagged", see I don't know what's been tagged

Q: Oh, tagged, they'll normally have "spam" in graphics or "spam" in the subject line...

A: Oh, yes, actually, then, everything I get has got that tag on it

Q: It's all tagged?

A: Yeah

Q: But it has decreased in total?

A: Absolutely, yeah.

Q3 How do you feel about Unsolicited Bulk Emails? (05:30)

a.) For each of these different types of UBE you have indicated you have received in q2, what emotions from the following list would best describe how you feel about each type? If you found any of these types of email particularly offensive or objectionable, please indicate this next to the UBE type also. (Participant responses as below)

Selling Cheap Software

- Like it Angry Disgusted Embarrassed Particularly
 Happy Frustrated Worried Don't Care Offensive

Sexual Performance Drugs (Viagra, Cialis etc)

- Like it Angry Disgusted Embarrassed Particularly
 Happy Frustrated Worried Don't Care Offensive

Weight Loss Drugs/Programmes

- Like it Angry Disgusted Embarrassed Particularly
 Happy Frustrated Worried Don't Care Offensive

Male Enhancement/Enlargement Products

- Like it Angry Disgusted Embarrassed Particularly
 Happy Frustrated Worried Don't Care Offensive

Mortgage/Loan Financing (* Participant accidentally omitted ticking an entry)

- Like it Angry Disgusted Embarrassed Particularly
 Happy Frustrated Worried Don't Care Offensive

Job/Employment Offers

- Like it Angry Disgusted Embarrassed Particularly
 Happy Frustrated Worried Don't Care Offensive

Adult Pornography Websites

- Like it Angry Disgusted Embarrassed Particularly
 Happy Frustrated Worried Don't Care Offensive

Child Pornography Websites

- Like it Angry Disgusted Embarrassed Particularly
 Happy Frustrated Worried Don't Care Offensive

Dating Websites

- Like it Angry Disgusted Embarrassed Particularly
 Happy Frustrated Worried Don't Care Offensive

Stock Market "Tips"

- Like it Angry Disgusted Embarrassed Particularly
 Happy Frustrated Worried Don't Care Offensive

Online Casino Websites

- Like it Angry Disgusted Embarrassed Particularly
 Happy Frustrated Worried Don't Care Offensive

"Nigerian" Fraud (i.e. want to deposit \$xx million in your bank account)

- Like it Angry Disgusted Embarrassed Particularly
 Happy Frustrated Worried Don't Care Offensive

Selling Other General Products/Services

- Like it Angry Disgusted Embarrassed Particularly
 Happy Frustrated Worried Don't Care Offensive

What Are Your Feelings About Spam in General?

- Like it Angry Disgusted Embarrassed Particularly
 Happy Frustrated Worried Don't Care Offensive

Q3 How do you feel about Unsolicited Bulk Emails (Contd...)

b.) If you found any of the unsolicited emails you received offensive or objectionable, have you ever opened any of these emails when your work colleague(s) or manager(s) were present, or able to see your computer screen? (07:18) N/A

c.) If so, how did you feel in this situation? N/A

d.) If not, how do you think you might feel in that situation? (07:40)

Q: If not, if you haven't actually marked them, if something like that happened, how do you think you might feel in a situation like that if there was a particularly offensive email that came through?

A: Right, so this has become open, and my boss has been behind me and...

Q: A hypothetical question basically...

A: Right, well I would feel pretty peeved. In some ways I'd be awfully embarrassed. A bit, sort of, yeah I'd be embarrassed because I'd be wondering what they'd be thinking I'm actually doing with that, my intentions not being to look at anything like that coming through, so I'd probably look for more understanding from my boss that this is, this happens, and sometimes the curiosity gets to the cat, and sometimes, when you do, I go really quickly through my emails, I do click unintentionally on things, but if I timed the amount of time I actually clicked something and then I close and delete it, it'd be like nanoseconds, so, yeah. No I'd be embarrassed and a little bit peeved.

Q4 What do you do with Unsolicited Bulk Emails? (08:55)

a.) If participant has indicated they have received any unsolicited emails requesting personal information including a login/password (e.g. for a bank account, Paypal account etc) in section 2), then ask:

For any of the unsolicited emails you indicated you have received that requested you provide login/password information for a bank or other online financial website, have you ever:

(i) Clicked on the link provided in the email?

(ii) Entered your login ID and password?

Q: Have you ever received any requesting personal information, for example to login to a bank site or...?

A: Yes, anz.com

Q: Have you ever clicked on any of the links that were, they have links in those emails usually?

(i) No, no, I've usually rung up the IT department, or at least I've rung up ANZ, or any banks, I've rung and told them, informed them I've got this email.

(ii) No

b.) For any other non-financial unsolicited emails, have you ever clicked on any links included in unsolicited emails you have received? (09:55)

A: No, because I just know the consequences would be just devastating. I'd be accepting their offer to keep on sharing my email out with everybody, you know, "hello, yes you do exist", I know they do some sort of random key generating sort of thing, and that's probably how they find me sometimes, I only need to respond and they go "yes, you do exist", you're on our list of thousands. That's my assumption.

c.) If “Yes”, what was the reason you clicked on it? e.g. it was an “Unsubscribe” or “Stop receiving” link, or you wanted to see what was on the website because it looked interesting, what? (10:35) N/A

d.) Have you at any time ever purchased any products or services offered in an unsolicited email? (10:45)

A: No

e.) What do you normally do with the unsolicited emails you receive: (10:55)

Delete them?

Report them to the IT Department?

Forward them to the IT Department?

Reply to them?

Other?

A: I delete.

Q: Normally delete?

A: Normally delete. Or I send it to, they have got, they do have an address to send it to...

Q: Internally?

A: To forward to, yeah, like a spam... can't remember the address, but they do have it to forward it into there so they can actually tag it, and then delete it, and get rid of it that way, but usually I just delete.

Q: Delete them or forward, that's what you'd normally do?

A: Yeah.

Q5 What are your opinions about Unsolicited Bulk Emails? (11:34)

a.) Do you think that unsolicited emails waste your time at work?

A: Yes they do, but I don't get a lot of it so it's not like a big issue for me, not on my radar screen, so it's not on the radar screen. This time maybe last year or the year before, yes, yes it was a waste of time, there was a lot, but things have got much better since then.

b.) Do you think they are a waste of your organisation's time and money? (12:05)

A: Absolutely. Without a doubt.

c.) How well do you think your organisation is doing in controlling the amount of unsolicited email being received? Is it doing a good job, a poor job? (12:15)

A: I think they're doing an exceptional job. I don't have a good understanding of computers, and those sort of things, so, and I know how difficult it is for, it's like the athlete, with the drugs, and, you know, they're always ahead of the tests and things, and I think it's always cat and mouse, they're always trying to chase, and fix the holes before, you know, so I know that always goes on, so...

d.) Do you think more could be done by your organisation to control unsolicited email? (12:50)

A: No, I'm... that's a difficult one, isn't it? Don't really know them that well.

Q: If you were to say "yes", what do you think they could be doing perhaps, is there anything else that you can think of?

A: Not that I can think of, no.

Q: So you're quite happy with what they're doing basically at the moment, to block it?

A: Yeah.

Q: Especially since yours has decreased...

A: Yeah, well since I have seen a decrease, I think they're actually doing more to stop it. It hasn't gone the opposite way yet. (*IT Manager**), it hasn't gone back the other way yet...

e.) If "Yes", what more do you think they could do to control it? N/A

f.) Do you think your organisation could provide you with more information about unsolicited email? (13:45)

A: No. No, they've made it quite clear what to do with the emails and things. They may need to keep it more sort of regular, to maybe once every two months maybe just go through the policy or how to deal with it, not waiting for something to happen to respond to it so maybe just a regular...

Q: More regular reminders sort of thing?

A: Reminders, and how to do things, how to respond, and if they know of anything that we should be watching out for, to help them to, to let us know.

g.) If "Yes", what information do you think they should provide? N/A

Impact of UBE on New Zealand Organisations Individual Employee Interviews				
Organisation:	1	Gender: F	Date:	21/12/06
Participant #:	4		Time:	9:11am

Q1 What do you know about Unsolicited Bulk Emails?

a.) Have you read, heard or seen much about UBE (spam) in the media (e.g. newspapers, magazines, radio, TV)? (00:25)

A: Yeah, you know, lots about it, because it's an issue that affects all of us here in the (*department**), it's actually often considered as (*possible topics**), and as various issues come up, the minute there's any sort of a virus suggestion or any kind of issue about spam it's always something that we actually give quite a lot of consideration to as a (*topic**), and often do (*cover the topic**) because we're experienced and we know it's a big issue, and we also know it affects a lot of people and that's the reason why.

b.) Has your organisation provided you with any information about UBE? (01:20)

A: No, I wouldn't say that we have been given a lot of information about it, certainly what I know about spam is mostly through my own experience and also what I read in the newspapers about it, you know, we'll get the odd spam alert or an advisory from our IT people about anything to watch out for from time to time but if we're talking generally, no I wouldn't say I've been greatly informed about spam by my work colleagues.

c.) If so, what sort of information? N/A

d.) What do you believe might be the reason(s) you receive UBE; how do you think the spammers got your email address? (02:10)

A: I'd be fascinated to know how spammers get whatever email addresses. I suppose the email address that I'm in charge of here in the (*department**) is probably more vulnerable than other people's to spam, because I basically look after the main email inbox for our (*department**). It's the main assignment desk, so therefore it's an email that we publicise through our website as being the contact point for the (*department**), and, you know, every organisation, PR company, government department, anyone wanting to contact us by email about (*the department**) will be using my email address, so it's out there.

Q: Is that your personal internal email address or it's actually...?

A: No, I have my own personal one, and I also operate the main (*xyz**) email which is in a public folder. Anyone can see it but I'm actually sort of in charge of trawling through it day after day.

Q: So you've got two mailboxes to look after basically?

A: Yeah

Q: Do you have much in your personal one, or is it really mainly just...?

A: Spam? Yeah, they both get it but the (*xyz**) one will get probably more of it

Q: A lot more?

A: Yeah, a lot more.

Q: But you don't really know how they might have got hold of your own personal one as well, if you're getting spam in that too?

A: No, I don't know. I guess I harbour suspicions it's, you know, to do with the (xyz*) one because I notice that if I get an email in the (xyz*), and I reply to it, it goes out under my personal one.

Q: It goes from you?

A: Yeah.

Q: So you think it could be related to that?

A: Yeah, I would have thought so, yeah.

Q2 What can you tell me about the Unsolicited Bulk Emails you receive? (04:30)

a.) Thinking about the different types of UBE you have received in the past, which of the following types have you received, in your email account with this organisation, to the best of your knowledge? (Participant responses as below)

- Selling Cheap Software
- Sexual Performance Drugs (Viagra, Cialis etc)
- Weight Loss Drugs/Programmes
- Male Enhancement/Enlargement Products
- Mortgage/Loan Financing
- Job/Employment Offers
- Adult Pornography Websites
- Child Pornography Websites
- Dating Websites
- Stock Market "Tips"
- Online Casino Websites
- "Nigerian" Fraud (i.e. want to deposit \$xx million in your bank account)
- Selling Other General Products/Services

b.) To the best of your knowledge, has the amount of unsolicited email you receive increased or decreased in the past 12 months (or less than 12 months if not employed with this organisation for that long)? (06:05)

A: It's definitely increased, and in very large amounts.

Q3 How do you feel about Unsolicited Bulk Emails? (07:00)

a.) For each of these different types of UBE you have indicated you have received in q2, what emotions from the following list would best describe how you feel about each type? If you found any of these types of email particularly offensive or objectionable, please indicate this next to the UBE type also. (Participant responses as below)

 Selling Cheap Software

- | | | | | |
|----------------------------------|--|------------------------------------|--|---------------------------------------|
| <input type="checkbox"/> Like it | <input type="checkbox"/> Angry | <input type="checkbox"/> Disgusted | <input type="checkbox"/> Embarrassed | <input type="checkbox"/> Particularly |
| <input type="checkbox"/> Happy | <input checked="" type="checkbox"/> Frustrated | <input type="checkbox"/> Worried | <input checked="" type="checkbox"/> Don't Care | Offensive |

 Sexual Performance Drugs (Viagra, Cialis etc)

- | | | | | |
|----------------------------------|-------------------------------------|---|--------------------------------------|--|
| <input type="checkbox"/> Like it | <input type="checkbox"/> Angry | <input checked="" type="checkbox"/> Disgusted | <input type="checkbox"/> Embarrassed | <input checked="" type="checkbox"/> Particularly |
| <input type="checkbox"/> Happy | <input type="checkbox"/> Frustrated | <input type="checkbox"/> Worried | <input type="checkbox"/> Don't Care | Offensive |

 Weight Loss Drugs/Programmes

- | | | | | |
|----------------------------------|--|------------------------------------|--|---------------------------------------|
| <input type="checkbox"/> Like it | <input type="checkbox"/> Angry | <input type="checkbox"/> Disgusted | <input type="checkbox"/> Embarrassed | <input type="checkbox"/> Particularly |
| <input type="checkbox"/> Happy | <input checked="" type="checkbox"/> Frustrated | <input type="checkbox"/> Worried | <input checked="" type="checkbox"/> Don't Care | Offensive |

 Male Enhancement/Enlargement Products

- | | | | | |
|----------------------------------|-------------------------------------|---|--------------------------------------|--|
| <input type="checkbox"/> Like it | <input type="checkbox"/> Angry | <input checked="" type="checkbox"/> Disgusted | <input type="checkbox"/> Embarrassed | <input checked="" type="checkbox"/> Particularly |
| <input type="checkbox"/> Happy | <input type="checkbox"/> Frustrated | <input type="checkbox"/> Worried | <input type="checkbox"/> Don't Care | Offensive |

 Mortgage/Loan Financing

- | | | | | |
|----------------------------------|--|------------------------------------|--|---------------------------------------|
| <input type="checkbox"/> Like it | <input type="checkbox"/> Angry | <input type="checkbox"/> Disgusted | <input type="checkbox"/> Embarrassed | <input type="checkbox"/> Particularly |
| <input type="checkbox"/> Happy | <input checked="" type="checkbox"/> Frustrated | <input type="checkbox"/> Worried | <input checked="" type="checkbox"/> Don't Care | Offensive |

 Job/Employment Offers

- | | | | | |
|----------------------------------|-------------------------------------|------------------------------------|--|---------------------------------------|
| <input type="checkbox"/> Like it | <input type="checkbox"/> Angry | <input type="checkbox"/> Disgusted | <input type="checkbox"/> Embarrassed | <input type="checkbox"/> Particularly |
| <input type="checkbox"/> Happy | <input type="checkbox"/> Frustrated | <input type="checkbox"/> Worried | <input checked="" type="checkbox"/> Don't Care | Offensive |

 Adult Pornography Websites

- | | | | | |
|----------------------------------|-------------------------------------|------------------------------------|--------------------------------------|---------------------------------------|
| <input type="checkbox"/> Like it | <input type="checkbox"/> Angry | <input type="checkbox"/> Disgusted | <input type="checkbox"/> Embarrassed | <input type="checkbox"/> Particularly |
| <input type="checkbox"/> Happy | <input type="checkbox"/> Frustrated | <input type="checkbox"/> Worried | <input type="checkbox"/> Don't Care | Offensive |

 Child Pornography Websites

- | | | | | |
|----------------------------------|-------------------------------------|------------------------------------|--------------------------------------|---------------------------------------|
| <input type="checkbox"/> Like it | <input type="checkbox"/> Angry | <input type="checkbox"/> Disgusted | <input type="checkbox"/> Embarrassed | <input type="checkbox"/> Particularly |
| <input type="checkbox"/> Happy | <input type="checkbox"/> Frustrated | <input type="checkbox"/> Worried | <input type="checkbox"/> Don't Care | Offensive |

 Dating Websites

- | | | | | |
|----------------------------------|-------------------------------------|------------------------------------|--------------------------------------|---------------------------------------|
| <input type="checkbox"/> Like it | <input type="checkbox"/> Angry | <input type="checkbox"/> Disgusted | <input type="checkbox"/> Embarrassed | <input type="checkbox"/> Particularly |
| <input type="checkbox"/> Happy | <input type="checkbox"/> Frustrated | <input type="checkbox"/> Worried | <input type="checkbox"/> Don't Care | Offensive |

 Stock Market "Tips"

- | | | | | |
|----------------------------------|--|------------------------------------|--|---------------------------------------|
| <input type="checkbox"/> Like it | <input type="checkbox"/> Angry | <input type="checkbox"/> Disgusted | <input type="checkbox"/> Embarrassed | <input type="checkbox"/> Particularly |
| <input type="checkbox"/> Happy | <input checked="" type="checkbox"/> Frustrated | <input type="checkbox"/> Worried | <input checked="" type="checkbox"/> Don't Care | Offensive |

 Online Casino Websites

- | | | | | |
|----------------------------------|--|------------------------------------|--|---------------------------------------|
| <input type="checkbox"/> Like it | <input type="checkbox"/> Angry | <input type="checkbox"/> Disgusted | <input type="checkbox"/> Embarrassed | <input type="checkbox"/> Particularly |
| <input type="checkbox"/> Happy | <input checked="" type="checkbox"/> Frustrated | <input type="checkbox"/> Worried | <input checked="" type="checkbox"/> Don't Care | Offensive |

 "Nigerian" Fraud (i.e. want to deposit \$xx million in your bank account)

- | | | | | |
|----------------------------------|--|------------------------------------|--|---------------------------------------|
| <input type="checkbox"/> Like it | <input type="checkbox"/> Angry | <input type="checkbox"/> Disgusted | <input type="checkbox"/> Embarrassed | <input type="checkbox"/> Particularly |
| <input type="checkbox"/> Happy | <input checked="" type="checkbox"/> Frustrated | <input type="checkbox"/> Worried | <input checked="" type="checkbox"/> Don't Care | Offensive |

 Selling Other General Products/Services

- | | | | | |
|----------------------------------|-------------------------------------|------------------------------------|--|---------------------------------------|
| <input type="checkbox"/> Like it | <input type="checkbox"/> Angry | <input type="checkbox"/> Disgusted | <input type="checkbox"/> Embarrassed | <input type="checkbox"/> Particularly |
| <input type="checkbox"/> Happy | <input type="checkbox"/> Frustrated | <input type="checkbox"/> Worried | <input checked="" type="checkbox"/> Don't Care | Offensive |

What Are Your Feelings About Spam in General?

- | | | | | |
|----------------------------------|---|------------------------------------|--------------------------------------|--|
| <input type="checkbox"/> Like it | <input checked="" type="checkbox"/> Angry | <input type="checkbox"/> Disgusted | <input type="checkbox"/> Embarrassed | <input checked="" type="checkbox"/> Particularly |
| <input type="checkbox"/> Happy | <input type="checkbox"/> Frustrated | <input type="checkbox"/> Worried | <input type="checkbox"/> Don't Care | Offensive |

(NB: Participant ticked Adult Porn, Child Porn and Dating by mistake)

Q3 How do you feel about Unsolicited Bulk Emails (Contd...)

Q3.a) Conversation while selecting responses (07:43)

Q: You can tick more than one entry. If you really don't care about it just tick the one, but you can actually tick more than one of the other ones for each

A: Yeah. You know mostly I'd sort of, kind of just feel a little bit annoyed or just, you know, deleted it straight away and don't even think about it, because I can recognise it quickly, so it's probably a little bit frustrating. It's probably a combo of "frustrated" and "don't care". They might sound like they're contradictory, but that's actually kind of, actually it's just interrupting my time and slightly annoying.

b.) If you found any of the unsolicited emails you received offensive or objectionable, have you ever opened any of these emails when your work colleague(s) or manager(s) were present, or able to see your computer screen? (11:10)

A: No, I don't think so. I mean, there was actually a time recently when a number of us got a really offensive spam email at the same time and we discussed it, because we all got it at the same time we all discussed it, you know, we had our Wellington (*department head**) on speaker-phone and he'd got it as well, so, you know, we all had a kind of, well, they had a chuckle over it, but that would be the only kind of time I think when I recall actually discussing contents of an offensive email with somebody.

c.) If so, how did you feel in this situation? N/A

d.) If not, how do you think you might feel in that situation? (12:25)

A: I'd be embarrassed and, you know, and disgusted probably.

Q4 What do you do with Unsolicited Bulk Emails? (12:55)

a.) If participant has indicated they have received any unsolicited emails requesting personal information including a login/password (e.g. for a bank account, Paypal account etc) in section 2), then ask:

For any of the unsolicited emails you indicated you have received that requested you provide login/password information for a bank or other online financial website, have you ever:

- (i) Clicked on the link provided in the email?**
- (ii) Entered your login ID and password?**

Q: Have you ever received any spam requesting personal information, such as a login and password, for example it might be to a bank website or Paypal or something like that, have you ever received any email of that nature?

A: Yeah.

Q: Have you ever clicked on any of the links that they provide in that, that takes you to the website?

A: No

- (i) No**
- (ii) N/A**

b.) For any other non-financial unsolicited emails, have you ever clicked on any links included in unsolicited emails you have received? (13:30)

A: I don't think so, no.

c.) If “Yes”, what was the reason you clicked on it? e.g. it was an “Unsubscribe” or “Stop receiving” link, or you wanted to see what was on the website because it looked interesting, what? N/A

d.) Have you at any time ever purchased any products or services offered in an unsolicited email? (13:55)

A: No

e.) What do you normally do with the unsolicited emails you receive: (14:10)

Delete them?

Report them to the IT Department?

Forward them to the IT Department?

Reply to them?

Other?

A: Delete them mostly, and a couple of times in the last few months we’ve been asked to forward spam emails to IT, and so I’ve done that as well, but most of all I’d be deleting them.

Q: So you have forwarded them to the IT department?

A: To IT, yeah

Q: Who have you forwarded them to?

A: I think they’ve setup a special email address, spam@xyz or something.

Q5 What are your opinions about Unsolicited Bulk Emails? (15:05)

a.) Do you think that unsolicited emails waste your time at work?

A: Yeah

b.) Do you think they are a waste of your organisation’s time and money? (15:15)

A: Yes

c.) How well do you think your organisation is doing in controlling the amount of unsolicited email being received? Is it doing a good job, a poor job? (15:22)

A: Well, you know I understand the arguments for lowering that threshold, and I certainly was having important emails blocked before we did it, for reasons that, you know, I’m not sure about, but, it’s certainly, you know, the Inboxes are just, you know, it feels to me like it’s sort of exploded in the last two or three months to a stage where it’s almost unmanageable for me, so, you know, I don’t think how we’ve got it going at the moment is very good at all, so, you know, I suppose what I’m saying is I think, you know, it’s poor at the moment.

d.) Do you think more could be done by your organisation to control unsolicited email? (16:20)

A: Yes, I would hope so, but I wouldn’t know where, how you start.

e.) If “Yes”, what more do you think they could do to control it? (16:36)

Q: If you did say “yes”, which you did, I was going to ask “what more do you think they could do to control it?”, but you’ve just responded you don’t really know what they could be doing to control it.

A: No, I mean, because there’s so much of it through now, I would probably, you know, suggest that they increase that threshold back up to a more manageable amount, if you see what I mean.

Q: You said you were getting good emails blocked though?

A: Yeah, but not that many

Q: Not too many?

A: Not too many, and, you know, if the trade-off is, you know, having an extra 50 spam emails coming in in a twenty four hour period then I think I’d, you know, put up with the odd important email being blocked, because, not getting off track, but I, you know, I get a lot of emails in the (xyz*) Inbox, and I used to be able to get through them all, when I get in in the morning in the space of half an hour and sort out what was important and delete what was not, but, it’d be fair to say in the last two months that I just can’t get through them all, you know, in a normal session, and now I just...

Q: There’s just so much coming in...

A: Yeah. I just don’t have time to trawl through the Inbox every morning in the same way that I used to be able to, so now I just simply have to try and spot the important ones simply by their subject line or who they’re from.

f.) Do you think your organisation could provide you with more information about unsolicited email? (18:15)

Q: Do you think your organisation could provide you with more information about unsolicited email, for example what it is, how to recognise it, how to deal with it?

A: Yes

g.) If “Yes”, what information do you think they should provide? (18:33)

Q: Ok, well, I’ve given you some examples there, is there any other type of information that you think they could provide you with, what would you like to see, for example, what would you like to see them providing you with?

A: I would probably benefit from a session with somebody in IT, you know, about the ability to spot them, and, I mean I already think I’m probably reasonably adept at that, but I’m sure that they, you know, would know a few extra tips on spotting things quickly and getting rid of them, I’m sure I’d benefit from a session like that too.

Impact of UBE on New Zealand Organisations Individual Employee Interviews				
Organisation:	2	Gender:	F	Date: 12/03/07
Participant #:	1		Time:	11:01am

Q1 What do you know about Unsolicited Bulk Emails? (00:20)

a.) Have you read, heard or seen much about UBE (spam) in the media (e.g. newspapers, magazines, radio, TV)?

A: Not an awful lot really in the media, I mean we're aware of it with the company here, so, yes, that's probably the easiest way.

Q: So internally, but not much outside

A: Internally, but not too much media-wise.

b.) Has your organisation provided you with any information about UBE? (00:45)

A: Yes. Yes, we have been provided with information.

c.) If so, what sort of information? (00:53)

A: On the Intranet, we get updates with regard to spam, also, you know, being warned not to open certain files if you're not aware of the sender, that sort of thing.

Q: Do they send emails out about it, or it's just on the Intranet?

A: Emails periodically as well as on the Intranet.

d.) What do you believe might be the reason(s) you receive UBE; how do you think the spammers got your email address? (01:22)

A: Personally with mine, it's because I also have the sub-address info@xyz, which I think they tend to go for those sort of addresses, as opposed to actually going to a website where it's being found, if that makes sense.

Q: You think it's just a common email type of address that they'd be...

A: I think because it's an "info" that they'd be honing in on basically. As opposed to, because it's all the "info", it's never, any spam received, it's always the info@xyz address as opposed to like, my personal address.

Q: You don't really receive any in your own personal messages?

A: No, I just went through to check that just before the interview actually, and it's all pretty much that way.

Q2 What can you tell me about the Unsolicited Bulk Emails you receive? (02:30)

a.) Thinking about the different types of UBE you have received in the past, which of the following types have you received, in your email account with this organisation, to the best of your knowledge? (Participant responses as below)

- Selling Cheap Software
- Sexual Performance Drugs (Viagra, Cialis etc)
- Weight Loss Drugs/Programmes
- Male Enhancement/Enlargement Products
- Mortgage/Loan Financing
- Job/Employment Offers
- Adult Pornography Websites
- Child Pornography Websites
- Dating Websites
- Stock Market "Tips"
- Online Casino Websites
- "Nigerian" Fraud (i.e. want to deposit \$xx million in your bank account)
- Selling Other General Products/Services

b.) To the best of your knowledge, has the amount of unsolicited email you receive increased or decreased in the past 12 months (or less than 12 months if not employed with this organisation for that long)? (03:10)

A: It's increased, yes it has increased.

Q3 How do you feel about Unsolicited Bulk Emails? (03:45)

a.) For each of these different types of UBE you have indicated you have received in q2, what emotions from the following list would best describe how you feel about each type? If you found any of these types of email particularly offensive or objectionable, please indicate this next to the UBE type also. (Participant responses as below)

Selling Cheap Software

- Like it Angry Disgusted Embarrassed Particularly
 Happy Frustrated Worried Don't Care Offensive

Sexual Performance Drugs (Viagra, Cialis etc)

- Like it Angry Disgusted Embarrassed Particularly
 Happy Frustrated Worried Don't Care Offensive

Weight Loss Drugs/Programmes

- Like it Angry Disgusted Embarrassed Particularly
 Happy Frustrated Worried Don't Care Offensive

Male Enhancement/Enlargement Products

- Like it Angry Disgusted Embarrassed Particularly
 Happy Frustrated Worried Don't Care Offensive

Mortgage/Loan Financing

- Like it Angry Disgusted Embarrassed Particularly
 Happy Frustrated Worried Don't Care Offensive

Job/Employment Offers

- Like it Angry Disgusted Embarrassed Particularly
 Happy Frustrated Worried Don't Care Offensive

Adult Pornography Websites

- Like it Angry Disgusted Embarrassed Particularly
 Happy Frustrated Worried Don't Care Offensive

Child Pornography Websites

- Like it Angry Disgusted Embarrassed Particularly
 Happy Frustrated Worried Don't Care Offensive

Dating Websites

- Like it Angry Disgusted Embarrassed Particularly
 Happy Frustrated Worried Don't Care Offensive

Stock Market "Tips"

- Like it Angry Disgusted Embarrassed Particularly
 Happy Frustrated Worried Don't Care Offensive

Online Casino Websites

- Like it Angry Disgusted Embarrassed Particularly
 Happy Frustrated Worried Don't Care Offensive

"Nigerian" Fraud (i.e. want to deposit \$xx million in your bank account)

- Like it Angry Disgusted Embarrassed Particularly
 Happy Frustrated Worried Don't Care Offensive

Selling Other General Products/Services

- Like it Angry Disgusted Embarrassed Particularly
 Happy Frustrated Worried Don't Care Offensive

What Are Your Feelings About Spam in General?

- Like it Angry Disgusted Embarrassed Particularly
 Happy Frustrated Worried Don't Care Offensive

Q3 How do you feel about Unsolicited Bulk Emails (Contd...)

b.) If you found any of the unsolicited emails you received offensive or objectionable, have you ever opened any of these emails when your work colleague(s) or manager(s) were present, or able to see your computer screen? (05:10)

Q: Now you didn't find any particularly offensive.

A: But then I haven't really received so much of the offensive ones, as in the adult website links, so I mean possibly if I'd been receiving those ones it could be, but because I haven't really experienced those ones...

N/A

c.) If so, how did you feel in this situation? N/A

d.) If not, how do you think you might feel in that situation? (05:45)

A: Probably angry and embarrassed would be the main ones on those ones, yeah. And if it was something that could quite easily be particularly offensive, if it was something like child pornography or something like that. I'd say.

Q4 What do you do with Unsolicited Bulk Emails? (06:45)

a.) If participant has indicated they have received any unsolicited emails requesting personal information including a login/password (e.g. for a bank account, Paypal account etc) in section 2), then ask:

For any of the unsolicited emails you indicated you have received that requested you provide login/password information for a bank or other online financial website, have you ever:

(i) Clicked on the link provided in the email?

(ii) Entered your login ID and password?

Q: Ok, you have received some "Nigerian fraud"-type emails that want to deposit money in your bank account. Have you received any emails asking you to login to a particular website, saying, you know, "we're from your bank, please login"?

A: Yes, yes.

Q: Have you ever clicked on the link provided in the emails?

A: No. No. That's something that the company have, IT has actually been really good about, like putting, with the Intranet and that kind of thing, just reiterating every now and then, you know, never, ever, ever do these things at all.

Q: They give you plenty of warnings about that sort of thing

A: Yes, yes.

(i) No

(ii) N/A

b.) For any other non-financial unsolicited emails, have you ever clicked on any links included in unsolicited emails you have received? (07:40)

A: No. Not myself personally, no.

c.) If "Yes", what was the reason you clicked on it? e.g. it was an "Unsubscribe" or "Stop receiving" link, or you wanted to see what was on the website because it looked interesting, what? N/A

d.) Have you at any time ever purchased any products or services offered in an unsolicited email? (08:00)

A: No.

e.) What do you normally do with the unsolicited emails you receive: (08:12)

Delete them?

Report them to the IT Department?

Forward them to the IT Department?

Reply to them?

Other?

A: Usually what I do is forward to the IT department, and then delete them after I've forwarded them, to, there's a... yeah, to the IT department, so I forward them, basically it's the same as reporting, it's sort of the same thing.

Q: Do they have an address for you to forward them to, or you just send it to a...?

A: We do have, like, not a non-specific one; it's just an IT department address that goes to all members of the IT department. I thought they'd probably do more about it if they're receiving as many emails as I am, so...

Q: I wouldn't hurt to try...

Q5 What are your opinions about Unsolicited Bulk Emails? (09:10)

a.) Do you think that unsolicited emails waste your time at work?

A: Yes, yes they do.

b.) Do you think they are a waste of your organisation's time and money? (09:25)

A: Yes.

c.) How well do you think your organisation is doing in controlling the amount of unsolicited email being received? Is it doing a good job, a poor job? (09:30)

A: They're doing a good job, they've definitely improved in the last six months or so, it has improved a lot.

Q: But you are receiving more spam...?

A: I am receiving more in a way, because they're still letting it through so that you can verify if it's actual spam or not.

Q: They're tagging it?

A: So they are tagging it, yeah. They are identifying it, so they are doing a relatively good job, but it's still probably more than I'd like to see, if that makes sense.

Q: So, even though you're getting more email through, their system seems to be identifying more of it, so that you can more quickly recognise it?

A: Highlighting it as spam, yeah. Yeah, well personally what I do, is I have a rule that if they've identified it as spam it goes into a separate folder, and then at some point in the day I go through it and check that. I don't know how many other people are doing that, but that's sort of how I work it, which makes it easier in a lot of ways because there's pretty much that one folder that you're needing to look at, so, they are identifying it.

d.) Do you think more could be done by your organisation to control unsolicited email? (10:42)

A: Possibly. I mean think they have really improved within the last six months, but I mean there's probably always things that can be done, so yeah, maybe a little bit possibly.

e.) If "Yes", what more do you think they could do to control it? (11:08)

A: I mean anything that's an obvious, that's been obviously tagged as spam, I mean delete it so it's not coming through, or even stop those coming in from the server, which I know they can do, so, something along those lines, if there's certain sort of emails that you'll notice coming through periodically, if they can do something to stop those, right at the server level, just not even receiving them.

Q: So they could do just a bit more fine-tuning, like the tagged ones that are definitely spam.

A: Yeah, I think probably fine-tuning on the... definitely, yeah, well if they're tagging it, well I don't know, if there's two things they're using to identify it as spam, you know, just don't even let it get any further than the initial email server into the company, so...

f.) Do you think your organisation could provide you with more information about unsolicited email? (12:05)

A: I actually think they've been really good with providing information for it, so no, because they periodically remind us and send information through, so...

g.) If "Yes", what information do you think they should provide? N/A

Impact of UBE on New Zealand Organisations Individual Employee Interviews				
Organisation:	2	Gender: F	Date:	12/03/07
Participant #:	2		Time:	11:20am

Q1 What do you know about Unsolicited Bulk Emails? (00:30)

a.) Have you read, heard or seen much about UBE (spam) in the media (e.g. newspapers, magazines, radio, TV)?

A: Newspapers, and, would I say, magazines, and would I say like my emails?

Q: Internal emails?

A: Yeah

Q: Or just from outside?

A: No. Oh through the faxes as well. Sometimes we get people fax, just fax it through to us and tell us to watch out for...

Q: Watch out for such and such?

A: Yeah, yeah.

b.) Has your organisation provided you with any information about UBE? (01:30)

A: Yes, yes they have.

c.) If so, what sort of information? (01:38)

A: They just, the information is just "let us know that don't", would it be like "they don't open", don't, IT just send emails to us and say "look, just beware of this particular email, ok, that goes through, or could come through your system, do not open but we are aware of it in the meantime, but just say, look, in case it slips through us and gets to you", yeah.

Q: Do they provide you with any general information about how to deal with spam, apart from, like these are presumably specific instances, is there anything in general?

A: Well, I can't think of it, no.

Q: Do they just send general emails out, or do you have a website?

A: Yeah, they send us all emails, yeah. I've not known them to give me a website, just say "look, this particular email will just... do not open".

Q: You have an internal Intranet?

A: Yes, yes, yeah.

Q: But you haven't been onto that to have a look for any information?

A: No, no.

Q: So just specific emails?

A: Yeah.

d.) What do you believe might be the reason(s) you receive UBE; how do you think the spammers got your email address? (02:55)

A: That's interesting too, 'cause I'd like to know how, I don't remember ever replying back to any of them. The unknown ones where I don't know who they are, and that's ok, like really known ones is the Viagra ones and that just comes all the time, it's a pain in the butt, I mean, how did they get my emails, I mean, because if it's been blocked by IT, well I normally can see the email address, and I think "ok, yeah I know that" and I'll just let them go, IT knows, just release it anyway, but as for the ones that don't have an email address to reply I think "well how did they get my email address in the first place", how do they get everyone's address, I have no idea.

Q: You really don't know.

A: I don't know.

Q2 What can you tell me about the Unsolicited Bulk Emails you receive? (04:00)

a.) Thinking about the different types of UBE you have received in the past, which of the following types have you received, in your email account with this organisation, to the best of your knowledge? (Participant responses as below)

- Selling Cheap Software
- Sexual Performance Drugs (Viagra, Cialis etc)
- Weight Loss Drugs/Programmes
- Male Enhancement/Enlargement Products
- Mortgage/Loan Financing
- Job/Employment Offers
- Adult Pornography Websites
- Child Pornography Websites
- Dating Websites
- Stock Market "Tips"
- Online Casino Websites
- "Nigerian" Fraud (i.e. want to deposit \$xx million in your bank account)
- Selling Other General Products/Services

b.) To the best of your knowledge, has the amount of unsolicited email you receive increased or decreased in the past 12 months (or less than 12 months if not employed with this organisation for that long)? (04:50)

A: I think it's increased.

Q3 How do you feel about Unsolicited Bulk Emails? (05:15)

a.) For each of these different types of UBE you have indicated you have received in q2, what emotions from the following list would best describe how you feel about each type? If you found any of these types of email particularly offensive or objectionable, please indicate this next to the UBE type also. (Participant responses as below)

 Selling Cheap Software

- | | | | | |
|----------------------------------|-------------------------------------|---|--------------------------------------|---------------------------------------|
| <input type="checkbox"/> Like it | <input type="checkbox"/> Angry | <input type="checkbox"/> Disgusted | <input type="checkbox"/> Embarrassed | <input type="checkbox"/> Particularly |
| <input type="checkbox"/> Happy | <input type="checkbox"/> Frustrated | <input checked="" type="checkbox"/> Worried | <input type="checkbox"/> Don't Care | Offensive |

 Sexual Performance Drugs (Viagra, Cialis etc)

- | | | | | |
|----------------------------------|-------------------------------------|---|--------------------------------------|---------------------------------------|
| <input type="checkbox"/> Like it | <input type="checkbox"/> Angry | <input checked="" type="checkbox"/> Disgusted | <input type="checkbox"/> Embarrassed | <input type="checkbox"/> Particularly |
| <input type="checkbox"/> Happy | <input type="checkbox"/> Frustrated | <input type="checkbox"/> Worried | <input type="checkbox"/> Don't Care | Offensive |

 Weight Loss Drugs/Programmes

- | | | | | |
|----------------------------------|-------------------------------------|------------------------------------|--|---------------------------------------|
| <input type="checkbox"/> Like it | <input type="checkbox"/> Angry | <input type="checkbox"/> Disgusted | <input type="checkbox"/> Embarrassed | <input type="checkbox"/> Particularly |
| <input type="checkbox"/> Happy | <input type="checkbox"/> Frustrated | <input type="checkbox"/> Worried | <input checked="" type="checkbox"/> Don't Care | Offensive |

 Male Enhancement/Enlargement Products

- | | | | | |
|----------------------------------|-------------------------------------|------------------------------------|--------------------------------------|---------------------------------------|
| <input type="checkbox"/> Like it | <input type="checkbox"/> Angry | <input type="checkbox"/> Disgusted | <input type="checkbox"/> Embarrassed | <input type="checkbox"/> Particularly |
| <input type="checkbox"/> Happy | <input type="checkbox"/> Frustrated | <input type="checkbox"/> Worried | <input type="checkbox"/> Don't Care | Offensive |

 Mortgage/Loan Financing

- | | | | | |
|----------------------------------|-------------------------------------|---|--------------------------------------|---------------------------------------|
| <input type="checkbox"/> Like it | <input type="checkbox"/> Angry | <input type="checkbox"/> Disgusted | <input type="checkbox"/> Embarrassed | <input type="checkbox"/> Particularly |
| <input type="checkbox"/> Happy | <input type="checkbox"/> Frustrated | <input checked="" type="checkbox"/> Worried | <input type="checkbox"/> Don't Care | Offensive |

 Job/Employment Offers

- | | | | | |
|----------------------------------|-------------------------------------|------------------------------------|--------------------------------------|---------------------------------------|
| <input type="checkbox"/> Like it | <input type="checkbox"/> Angry | <input type="checkbox"/> Disgusted | <input type="checkbox"/> Embarrassed | <input type="checkbox"/> Particularly |
| <input type="checkbox"/> Happy | <input type="checkbox"/> Frustrated | <input type="checkbox"/> Worried | <input type="checkbox"/> Don't Care | Offensive |

 Adult Pornography Websites

- | | | | | |
|----------------------------------|-------------------------------------|------------------------------------|--------------------------------------|---------------------------------------|
| <input type="checkbox"/> Like it | <input type="checkbox"/> Angry | <input type="checkbox"/> Disgusted | <input type="checkbox"/> Embarrassed | <input type="checkbox"/> Particularly |
| <input type="checkbox"/> Happy | <input type="checkbox"/> Frustrated | <input type="checkbox"/> Worried | <input type="checkbox"/> Don't Care | Offensive |

 Child Pornography Websites

- | | | | | |
|----------------------------------|-------------------------------------|------------------------------------|--------------------------------------|---------------------------------------|
| <input type="checkbox"/> Like it | <input type="checkbox"/> Angry | <input type="checkbox"/> Disgusted | <input type="checkbox"/> Embarrassed | <input type="checkbox"/> Particularly |
| <input type="checkbox"/> Happy | <input type="checkbox"/> Frustrated | <input type="checkbox"/> Worried | <input type="checkbox"/> Don't Care | Offensive |

 Dating Websites

- | | | | | |
|----------------------------------|-------------------------------------|------------------------------------|--------------------------------------|---------------------------------------|
| <input type="checkbox"/> Like it | <input type="checkbox"/> Angry | <input type="checkbox"/> Disgusted | <input type="checkbox"/> Embarrassed | <input type="checkbox"/> Particularly |
| <input type="checkbox"/> Happy | <input type="checkbox"/> Frustrated | <input type="checkbox"/> Worried | <input type="checkbox"/> Don't Care | Offensive |

 Stock Market "Tips"

- | | | | | |
|----------------------------------|-------------------------------------|------------------------------------|--------------------------------------|---------------------------------------|
| <input type="checkbox"/> Like it | <input type="checkbox"/> Angry | <input type="checkbox"/> Disgusted | <input type="checkbox"/> Embarrassed | <input type="checkbox"/> Particularly |
| <input type="checkbox"/> Happy | <input type="checkbox"/> Frustrated | <input type="checkbox"/> Worried | <input type="checkbox"/> Don't Care | Offensive |

 Online Casino Websites

- | | | | | |
|----------------------------------|-------------------------------------|---|--------------------------------------|---------------------------------------|
| <input type="checkbox"/> Like it | <input type="checkbox"/> Angry | <input type="checkbox"/> Disgusted | <input type="checkbox"/> Embarrassed | <input type="checkbox"/> Particularly |
| <input type="checkbox"/> Happy | <input type="checkbox"/> Frustrated | <input checked="" type="checkbox"/> Worried | <input type="checkbox"/> Don't Care | Offensive |

 "Nigerian" Fraud (i.e. want to deposit \$xx million in your bank account)

- | | | | | |
|----------------------------------|-------------------------------------|---|--------------------------------------|---------------------------------------|
| <input type="checkbox"/> Like it | <input type="checkbox"/> Angry | <input type="checkbox"/> Disgusted | <input type="checkbox"/> Embarrassed | <input type="checkbox"/> Particularly |
| <input type="checkbox"/> Happy | <input type="checkbox"/> Frustrated | <input checked="" type="checkbox"/> Worried | <input type="checkbox"/> Don't Care | Offensive |

 Selling Other General Products/Services

- | | | | | |
|----------------------------------|-------------------------------------|---|--------------------------------------|---------------------------------------|
| <input type="checkbox"/> Like it | <input type="checkbox"/> Angry | <input type="checkbox"/> Disgusted | <input type="checkbox"/> Embarrassed | <input type="checkbox"/> Particularly |
| <input type="checkbox"/> Happy | <input type="checkbox"/> Frustrated | <input checked="" type="checkbox"/> Worried | <input type="checkbox"/> Don't Care | Offensive |

What Are Your Feelings About Spam in General?

- | | | | | |
|----------------------------------|--|---|--------------------------------------|---------------------------------------|
| <input type="checkbox"/> Like it | <input checked="" type="checkbox"/> Angry | <input checked="" type="checkbox"/> Disgusted | <input type="checkbox"/> Embarrassed | <input type="checkbox"/> Particularly |
| <input type="checkbox"/> Happy | <input checked="" type="checkbox"/> Frustrated | <input type="checkbox"/> Worried | <input type="checkbox"/> Don't Care | Offensive |

Q3 How do you feel about Unsolicited Bulk Emails (Contd...)

b.) If you found any of the unsolicited emails you received offensive or objectionable, have you ever opened any of these emails when your work colleague(s) or manager(s) were present, or able to see your computer screen? (07:25) N/A

c.) If so, how did you feel in this situation? N/A

d.) If not, how do you think you might feel in that situation? (07:50)

A: Oh, look I'd just say to them, if it had I'd just say to them "Oh, look, I've opened it just to be nosey, but I didn't know that it was going to be this offensive and that, ok, and it doesn't come from anybody I know, so they must've sent it out to the general public. So I wouldn't really feel, I mean..."

Q: So would one of these describe how you'd feel perhaps? (pointed at job emotion scale words)

A: Probably embarrassed, I would be embarrassed, but I'd be ok with it because I'll just tell them the truth, I said "Well it's from somebody I don't even know", so, it's like I said it's been just out to the general public and that, yeah.

Q4 What do you do with Unsolicited Bulk Emails? (09:30)

a.) If participant has indicated they have received any unsolicited emails requesting personal information including a login/password (e.g. for a bank account, Paypal account etc) in section 2), then ask:

For any of the unsolicited emails you indicated you have received that requested you provide login/password information for a bank or other online financial website, have you ever:

(i) Clicked on the link provided in the email?

(ii) Entered your login ID and password?

Q: Now you have received some "Nigerian fraud" type of emails in the past, and, have you actually received any though that requested that you provide a login and password, say like from a bank type email saying that "We request you update your banking details, please click on the link and provide them", have you received any like that?

A: Yeah, yeah I have, but I haven't given...

Q: Have you ever clicked on the link?

(i) No, no, no way.

(ii) N/A

b.) For any other non-financial unsolicited emails, have you ever clicked on any links included in unsolicited emails you have received? (10:22)

A: Oh, probably like, for weight loss, I've been nosey to see if, you know, some of the ideas how to lose weight, because I didn't find that'd be, I mean that'd be ok, because it's not going to ask you to provide any information, mind you it has asked me for an email, not email, but it has asked me if I wanted to go further and that, and they'd probably want a bit more detail but I put "No", there's no way I'm putting any information of my personal information on any of (*words unclear*).

Q: So it was really just to see what information they had on that link?

A: Mmmm (agreement).

c.) If “Yes”, what was the reason you clicked on it? e.g. it was an “Unsubscribe” or “Stop receiving” link, or you wanted to see what was on the website because it looked interesting, what?

Answer is in b.) above.

d.) Have you at any time ever purchased any products or services offered in an unsolicited email? (11:32)

A: No, no.

e.) What do you normally do with the unsolicited emails you receive: (11:45)

Delete them?

Report them to the IT Department?

Forward them to the IT Department?

Reply to them?

Other?

A: Delete. I’ve deleted them and also report them to the IT department, yeah.

Q: You haven’t actually forwarded any to them you just let them know?

A: No, I just ring them and let them know sometimes “why am I getting these all the time”?

Q5 What are your opinions about Unsolicited Bulk Emails? (12:15)

a.) Do you think that unsolicited emails waste your time at work? (12:22)

A: Yes, it sure does.

b.) Do you think they are a waste of your organisation’s time and money? (12:32)

A: Yes it is. Especially our organisation, we’re an organisation where we get emails all the time for our orders for our customers, and so I get hundreds of them all day and that, ok, and when you get like twenty of them in up to a day of those stupid spams and that ok, you know, and you can’t, your email box comes up and says “oh look, it’s these people”, otherwise I’ll go “No”, but when you know, oh it could be a customer, you gotta go “Yes” and answer them straight away and then “bang” that comes up and go “Oh, tsk”, and then I’ve gotta delete it.

Q: It’s not a specific question here, but I might ask it at this point, because you’ve said you get, like, maybe a couple of hundred emails and you get maybe twenty a day that are spam, and you’ve mentioned that they were orders that you receive as well.

A: Yeah

Q: Do you think, to the best of your knowledge, do you think you might have ever accidentally deleted an order.

A: Yes, yes I have, but luckily enough because I can go back into the “Delete” menu and then get it out.

Q: And you’ve accidentally deleted it because...

A: Yes, I’ve deleted the order and that ok, and then I’ve said, and I haven’t done that order, and then I’ve said to the customer “Well no, I didn’t receive it”, if I hadn’t checked in the “Delete” column...

Q: And you think you accidentally deleted that because you thought it was perhaps a spam or something?

A: Yeah, yeah, and it was, because I haven't been allowed to open it, and thinking that it was a spam because IT's gone and blocked it, because it must've been well, you know, I don't know, a virus in it eh? (*words unclear**) and the customer goes "No, I did send it", I said "Oh, hang on, I'll just double-check. It is yours".

c.) How well do you think your organisation is doing in controlling the amount of unsolicited email being received? Is it doing a good job, a poor job? (14:18)

A: Well, if they're controlling it, why are we still getting them? How do they get through? So, no.

d.) Do you think more could be done by your organisation to control unsolicited email? (14:45)

A: Yes.

e.) If "Yes", what more do you think they could do to control it? (14:52)

A: Well that's it, just stop all the spam coming through, stop the unknown, the unknown... ok, I don't expect them to stop the email addresses on them because it's probably someone that we do know, ok, but they seem to be very good at putting a block on them, but these other ones that I've gone, these ones here that I've gone and ticked off,

Q: Some in particular?

A: You know, yeah, the "sexual performance", stuff like that, and stupid...

Q: Viagra and stuff?

A: Yeah, "Casino websites", stuff like that I mean, why are they allowed to still come through, they're not blocked.

Q: Ok, I'm not sure how to answer that one, but you're not really sure how they could control it better, you just know that they really should be doing it a bit better?

A: Yeah, that's all, I mean I'm not IT, so I don't know, I don't know anything about it.

f.) Do you think your organisation could provide you with more information about unsolicited email? (16:02)

Q: Do you think your organisation could provide you with more information about spam perhaps, and how to deal with it?

A: What sort of information?

Q: Just generally, what it is, how to identify it, perhaps, what to do with it if you've received it?

A: Well, what to do with it, I just delete it... that's what you do with it. No, I mean no, no, they don't need to. I see it I just delete it, that's it, you know, end of story. I mean, I don't need counselling over it.

g.) If "Yes", what information do you think they should provide? N/A

Impact of UBE on New Zealand Organisations Individual Employee Interviews				
Organisation:	2	Gender: M	Date:	30/03/07
Participant #:	3		Time:	11:06am

Q1 What do you know about Unsolicited Bulk Emails? (00:18)

a.) Have you read, heard or seen much about UBE (spam) in the media (e.g. newspapers, magazines, radio, TV)? (00:30)

A: No, no.

b.) Has your organisation provided you with any information about UBE? (00:40)

A: No, no.

Q: They don't email you much about it or...

A: No.

c.) If so, what sort of information? (00:55) N/A

d.) What do you believe might be the reason(s) you receive UBE; how do you think the spammers got your email address? (01:02)

Q: What do you believe might be the reason(s) you receive UBE; how do you think the spammers got your email address? Prior to the interview, you referred to something, an incident that happened.

A: As I said earlier, by using the credit card, and emailing to overseas destinations, the spam have picked up on that. We haven't had any unsolicited emails to do with using the card, but it's the email address that seems to be what, that seems to be open...

Q: So shortly after that event, after you'd been using the card...

A: There was definite activity...

Q: There was a lot of activity coming in, in terms of spam?

A: Yep, yep.

Q: And that was because you emailed a particular company you think, or...

A: Yeah well we're a multi-national company and we send emails back and forward to Canada, and, yeah, and then we were making bookings, and, San Francisco and again in Vegas, yeah, from here.

Q2 What can you tell me about the Unsolicited Bulk Emails you receive? (02:40)

a.) Thinking about the different types of UBE you have received in the past, which of the following types have you received, in your email account with this organisation, to the best of your knowledge? (Participant responses as below)

- Selling Cheap Software
- Sexual Performance Drugs (Viagra, Cialis etc)
- Weight Loss Drugs/Programmes
- Male Enhancement/Enlargement Products
- Mortgage/Loan Financing
- Job/Employment Offers
- Adult Pornography Websites
- Child Pornography Websites
- Dating Websites
- Stock Market "Tips"
- Online Casino Websites
- "Nigerian" Fraud (i.e. want to deposit \$xx million in your bank account)
- Selling Other General Products/Services

b.) To the best of your knowledge, has the amount of unsolicited email you receive increased or decreased in the past 12 months (or less than 12 months if not employed with this organisation for that long)? (03:35)

A: It's certainly decreased.

Q: Decreased?

A: As I said to you, due to (*organisation 2**) putting in an upgraded firewall (*for**) spam, to clear a lot of it, yeah. And we're continuously sending, if we get one that's unsolicited, we forward it back to them so that they can load that spammer into the system, so if there's another one comes it hopefully picks them up. There's a couple of smart ones at the moment, they're leaving all the key words out, the Viagra and things like that, they're leaving those words out, and so they just look like legit emails, but they're not, obviously.

Q: Just, sort of going into a little bit more detail, you say it's decreased, now overall it's decreased, or just in a little bit more detail, do you get emails coming through that have been tagged as being spam, so that you recognise that they are spam, have they decreased or increased or...?

A: I would probably get on average three overnight, but when they come to me, this emails been blocked as spam, yeah, our spam blocker's blocking it, so... I may get one or two a day, or overnight, on average.

Q: The actual spam email comes through to you, or has it actually been blocked and you just get...

A: It's been blocked

Q: ...and you get an email saying that "we have blocked this email"

A: Yeah, yeah.

Q: I see, so you don't actually receive the spam email itself.

A: No, no.

Q3 How do you feel about Unsolicited Bulk Emails? (05:40)

a.) For each of these different types of UBE you have indicated you have received in q2, what emotions from the following list would best describe how you feel about each type? If you found any of these types of email particularly offensive or objectionable, please indicate this next to the UBE type also. (Participant responses as below)

Selling Cheap Software

- Like it Angry Disgusted Embarrassed Particularly
 Happy Frustrated Worried Don't Care Offensive

Sexual Performance Drugs (Viagra, Cialis etc)

- Like it Angry Disgusted Embarrassed Particularly
 Happy Frustrated Worried Don't Care Offensive

Weight Loss Drugs/Programmes

- Like it Angry Disgusted Embarrassed Particularly
 Happy Frustrated Worried Don't Care Offensive

Male Enhancement/Enlargement Products

- Like it Angry Disgusted Embarrassed Particularly
 Happy Frustrated Worried Don't Care Offensive

Mortgage/Loan Financing

- Like it Angry Disgusted Embarrassed Particularly
 Happy Frustrated Worried Don't Care Offensive

Job/Employment Offers

- Like it Angry Disgusted Embarrassed Particularly
 Happy Frustrated Worried Don't Care Offensive

Adult Pornography Websites

- Like it Angry Disgusted Embarrassed Particularly
 Happy Frustrated Worried Don't Care Offensive

Child Pornography Websites

- Like it Angry Disgusted Embarrassed Particularly
 Happy Frustrated Worried Don't Care Offensive

Dating Websites

- Like it Angry Disgusted Embarrassed Particularly
 Happy Frustrated Worried Don't Care Offensive

Stock Market "Tips"

- Like it Angry Disgusted Embarrassed Particularly
 Happy Frustrated Worried Don't Care Offensive

Online Casino Websites

- Like it Angry Disgusted Embarrassed Particularly
 Happy Frustrated Worried Don't Care Offensive

"Nigerian" Fraud (i.e. want to deposit \$xx million in your bank account)

- Like it Angry Disgusted Embarrassed Particularly
 Happy Frustrated Worried Don't Care Offensive

Selling Other General Products/Services

- Like it Angry Disgusted Embarrassed Particularly
 Happy Frustrated Worried Don't Care Offensive

What Are Your Feelings About Spam in General?

- Like it Angry Disgusted Embarrassed Particularly
 Happy Frustrated Worried Don't Care Offensive

Q3 How do you feel about Unsolicited Bulk Emails (Contd...)

Conversation occurring while indicating emotional responses:

A: Well in a lot of cases, because they're coming to me already as a block, certainly not angry. I don't really care; it's just time-wasting, isn't it...

The only concern I have is if you respond to one of these, because we've got a very strong ethics, to use email, and to use the website, so, I just don't get into it, I don't open them or anything, but again, I don't care that somebody else is getting them before I ever do.

These ones worry you, the "Nigerian frauds", how do they get hold of your particulars?

b.) If you found any of the unsolicited emails you received offensive or objectionable, have you ever opened any of these emails when your work colleague(s) or manager(s) were present, or able to see your computer screen? (08:40)

Q: Well the answer to that is, I guess "no", because...

A: That's right

Q: ... you didn't find any particularly offensive, so it's Not Applicable

A: No, because I can't open them because they haven't come to me direct, they've come as "spam"

Q: Yes. They just come as saying that you have received them...

A: Yeah

Q: ...but you haven't actually opened them

A: Yeah, but if one ever came through, I wouldn't open it, because that would be, it would be in breach of company rules, which is the answer to the second question, is it?

Two: It breaches the company set of rules, and

Three: There's Big Brother's watching, and I just wouldn't get into that position, I'm a grandfather and there's enough (*word unclear**) going on out there now without me either being involved.

N/A

c.) If so, how did you feel in this situation? N/A

d.) If not, how do you think you might feel in that situation? (09:43)

Q: If that situation did occur, and you did receive an email that was an offensive type of email and you did happen to open it, not realising it or just clicked it accidentally perhaps, and somebody actually saw it on your screen, because they happened to be passing by, or they happened to be with you when you were going through your email, how do you think you might feel in such a situation?

A: Oh I 'd be embarrassed.

Q: Yeah

A: Yeah, because it's just not me, I just don't get into that, yeah. I would be offended and embarrassed.

Q4 What do you do with Unsolicited Bulk Emails? (10:30)

a.) If participant has indicated they have received any unsolicited emails requesting personal information including a login/password (e.g. for a bank account, Paypal account etc) in section 2), then ask:

For any of the unsolicited emails you indicated you have received that requested you provide login/password information for a bank or other online financial website, have you ever:

(i) Clicked on the link provided in the email?

(ii) Entered your login ID and password?

Q: Have you ever received any emails that have requested, that might have got through the filters perhaps, that have requested any personal information, for example a login and a password, so it might have been say from a bank, or a system called Paypal, or something saying “We’re requesting you to login, we need to update your details, please login to this website, click on the link below”, something like that?

A: No

Q: Have you ever had anything like that?

A: No, the nearest would be those Nigerian, you know, letters saying that they want to... I suppose they ask for your details don’t they as well, a lot of those?

Q: They do, yes

A: Yeah, so, the answer’s “yes”, isn’t it?

Q: Well, you’ve never actually clicked on a link?

A: No

Q: A lot of these ones they say, you know, “click on the link here”, it might come from, say, xyz.co.nz, please click on the link below to update your details, you’ve never had anything like that?

A: No

(i) No

(ii) N/A

b.) For any other non-financial unsolicited emails, have you ever clicked on any links included in unsolicited emails you have received? (11:42)

A: No, no. I’ve forwarded them...

c.) If “Yes”, what was the reason you clicked on it? e.g. it was an “Unsubscribe” or “Stop receiving” link, or you wanted to see what was on the website because it looked interesting, what? (12:05) N/A

d.) Have you at any time ever purchased any products or services offered in an unsolicited email? (12:20)

A: No

e.) What do you normally do with the unsolicited emails you receive: (12:28)

Delete them?

Report them to the IT Department?

Forward them to the IT Department?

Reply to them?

Other?

A: Forward them.

Q5 What are your opinions about Unsolicited Bulk Emails? (13:00)

a.) Do you think that unsolicited emails waste your time at work? (13:05)

A: Yes.

b.) Do you think they are a waste of your organisation's time and money? (13:14)

A: Yes.

Q: Just as an aside, it's an additional question, which happened to crop up with another interview, but I haven't actually put it here in the official questions, but it's related to waste of time and money for the organisation. Have you ever had a situation where you have received an email that might be perhaps for an order or a reply from say a potential customer or something, and you might have accidentally deleted it, thinking it was spam, or perhaps that it was, you know, you were deleting a bunch of spam emails and it accidentally got deleted as part of it, to the best of your knowledge, have you ever had a situation occur like that?

A: So what you're asking me is, I'm deleting spam, and I have a customer request come through...

Q: Yep, an inquiry, or perhaps even an order or something.

A: Well they go into a deleted file, and obviously, I guess the answer would be "yes", I have accidentally done that, but I've recovered it back out of the...

Q: You have had a situation occur to you that you know of?

A: Where a potential customer has, I've inadvertently deleted it, and "Oh, where is it?", and gone back and I've found it in the Deleted file, and...

Q: And you think that occurred as a result of deleting spam, or something like that?

A: Yes, yeah, you get distracted and there could be spam either side or whatever. Yeah, yes, the answer's yes.

c.) How well do you think your organisation is doing in controlling the amount of unsolicited email being received? Is it doing a good job, a poor job? (14:50)

A: No, I think (*IT Manager**) and the IT team overall they're doing a pretty good job, it's a constant fight.

d.) Do you think more could be done by your organisation to control unsolicited email? (15:14)

A: I don't know, because I'm not an electronic... yeah, don't know.

e.) If "Yes", what more do you think they could do to control it? N/A

f.) Do you think your organisation could provide you with more information about unsolicited email? (15:40)

Q: Do you think your organisation could provide you with more information about unsolicited emails? You indicated earlier that they hadn't really provided you with any information, do you think they could provide you with more?

A: The only time they send out warnings, is when there's a major virus or something, they'll send out a warning about that, "Don't open it".

Q: But not particularly about spam?

A: No, because...

Q: So they don't point you at any, at the Corporate Intranet site about...

A: No

Q: ...what to do with spam, or anything like that?

A: No. We all know what's to be done. If we get unsolicited mail, which you're referring to, we're a pretty tight organisation from the (*work colleague**) down below, and I think you've spoken to (*this person**) plus myself...

Q: Yes. So you all know just basically if you receive some you just forward it to the IT department?

A: Yep, IT department. Hey look, this is a new one, yeah. And we get some lilies sometimes, some real beauties.

Q: Alright, so you're quite happy with the information they provide you.

A: Yeah.

g.) If "Yes", what information do you think they should provide? N/A

Impact of UBE on New Zealand Organisations Individual Employee Interviews					
Organisation:	2	Gender:	F	Date:	30/03/07
Participant #:	4			Time:	12:12pm

Pre-question discussion

Q: Now there'll be a series of five sections, and a few questions in each, two of the sections I just want you to tick the spam emails that you might have received...

A: Ok

Q: ...and the following section, for those same emails, if you can tick how you feel about them, so there are just a number of answers there that you can...

A: We don't actually get them.

Q: Yep, that's fine.

A: Because they're stopped so we don't even, we just...

Q: You don't get any getting through at all?

A: No

Q: Never?

A: Oh through... we might get one or two that... no they're actually come through via (*parent organisation**) which is across the road, they send it to us saying "you received this and it's classed as spam", and we have the choice as to whether or not we want to open it, or we have to email them and ask them to release it, because some spam that comes through is work-related.

Q: Oh, not counting sort of internal email that you might...

A: Oh, internal spam doesn't go... from each other?

Q: Yeah

A: From each other, here in the office?

Q: Yes. Like, from other sections of the organisation, do people send out email to all the users internally?

A: Yes.

Q: You'd class that as spam as well?

A: No.

Q: No. Oh that's fine. Yeah, this is only from outside.

A: Yes.

Q: The spam we're researching is really only from people outside, it's what they call "unsolicited bulk emails"...

A: Yeah, we don't actually, yeah...

Q: ...email that's, it's usually from a person that you don't know, and it's sent out in bulk to lots and lots of people.

A: Yes, (*our department**), we've only just started getting it recently, because someone has got hold of (*our departmental**) email address, and it comes through to myself and (*my colleague**) under (*our department**).

Q: Yes.

A: But it's actually always blocked. We actually get it sent to us via (*parent organisation**), which is (*a person**) across the road. They'll send it to us and it's not from a particular person, it's actually from (*parent organisation**), and it says "you've received this particular thing and it's classed as spam", and we've got a choice, because sometimes we get, like (*external company**) reports that come through as spam, but they are proper reports that we need.

Q: Right.

A: So they're stopped first, and we have to actually ask for them to be released.

Q: Sure, yeah, all right. We'll refer to this part, prior to the interview in some of the other questions later on, so that's fine, yeah, that's given us a bit of background.

Q1 What do you know about Unsolicited Bulk Emails? (03:05)

a.) Have you read, heard or seen much about UBE (spam) in the media (e.g. newspapers, magazines, radio, TV)? (03:10)

A: No

b.) Has your organisation provided you with any information about UBE? (03:22)

Q: ...that you know of?

A: No, not that I know of.

Q: Have they sent you an email telling you what to do with it, or pointed you at a website or something...

A: No. Yeah, well we can't open it.

c.) If so, what sort of information? (03:45) N/A

d.) What do you believe might be the reason(s) you receive UBE; how do you think the spammers got your email address? (03:52)

A: I have no idea, it's just (*our department**), because it's nation-wide, they'll very shortly probably have (*a related department**), so...

Q: You think they've just guessed the email address perhaps?

A: No, I presume that people get paid to send off all these things, so they just get as many email addresses as they possibly can, and where they've just collected ours.

Q: Yeah, but you really don't know how they've collected you email address?

A: I don't know, and I don't care.

Q2 What can you tell me about the Unsolicited Bulk Emails you receive? (04:35)

a.) Thinking about the different types of UBE you have received in the past, which of the following types have you received, in your email account with this organisation, to the best of your knowledge? (Participant responses as below)

Q: Probably in your case it might be if there are spam emails that have come through that haven't been picked up by your systems...

A: No, they all get picked up.

Q: They pretty much all get picked up?

A: Yep.

Q: Ok. Do they identify at all which types of spam they are or do they tell you what the Subject line looks like, or...

A: No, just in brackets it's got "spam".

Q: Ok, in that case you might not have much to tick, but if you have a look at the types of spam there (handed interview form to participant), if you have received any in the past...

A: Oh, that one there.

Q: ...any that you know about, if you can just tick those particular types for me.

A: (After ticking box) That's it, just the top one. It seems to be a big one that one.

Q: There's a lot of those, yes.

- Selling Cheap Software
- Sexual Performance Drugs (Viagra, Cialis etc)
- Weight Loss Drugs/Programmes
- Male Enhancement/Enlargement Products
- Mortgage/Loan Financing
- Job/Employment Offers
- Adult Pornography Websites
- Child Pornography Websites
- Dating Websites
- Stock Market "Tips"
- Online Casino Websites
- "Nigerian" Fraud (i.e. want to deposit \$xx million in your bank account)
- Selling Other General Products/Services

b.) To the best of your knowledge, has the amount of unsolicited email you receive increased or decreased in the past 12 months (or less than 12 months if not employed with this organisation for that long)? (05:34)

A: Increased.

Q: It's increased. Ok, but it's increased in terms of the ones that they are notifying that they've picked up?

A: It's increased because we never used to get it.

Q: You never used to get it.

A: It used to always be stopped.

Q: Ok.

A: No actually, sorry, no we never used to get it before because they obviously didn't have our address, but now they've got the (*department**) it comes through.

Q: So someone out there has got hold of that address now...

A: Yes, yes.

Q: ...so it's coming through now

A: Yep

Q: That's the reason it's increased?

A: Yes.

Q3 How do you feel about Unsolicited Bulk Emails? (6:30)

a.) For each of these different types of UBE you have indicated you have received in q2, what emotions from the following list would best describe how you feel about each type? If you found any of these types of email particularly offensive or objectionable, please indicate this next to the UBE type also. (Participant responses as below)

 Selling Cheap Software

- | | | | | |
|----------------------------------|-------------------------------------|------------------------------------|--------------------------------------|---------------------------------------|
| <input type="checkbox"/> Like it | <input type="checkbox"/> Angry | <input type="checkbox"/> Disgusted | <input type="checkbox"/> Embarrassed | <input type="checkbox"/> Particularly |
| <input type="checkbox"/> Happy | <input type="checkbox"/> Frustrated | <input type="checkbox"/> Worried | <input type="checkbox"/> Don't Care | Offensive |

 Sexual Performance Drugs (Viagra, Cialis etc)

- | | | | | |
|----------------------------------|-------------------------------------|------------------------------------|--|---------------------------------------|
| <input type="checkbox"/> Like it | <input type="checkbox"/> Angry | <input type="checkbox"/> Disgusted | <input type="checkbox"/> Embarrassed | <input type="checkbox"/> Particularly |
| <input type="checkbox"/> Happy | <input type="checkbox"/> Frustrated | <input type="checkbox"/> Worried | <input checked="" type="checkbox"/> Don't Care | Offensive |

 Weight Loss Drugs/Programmes

- | | | | | |
|----------------------------------|-------------------------------------|------------------------------------|--------------------------------------|---------------------------------------|
| <input type="checkbox"/> Like it | <input type="checkbox"/> Angry | <input type="checkbox"/> Disgusted | <input type="checkbox"/> Embarrassed | <input type="checkbox"/> Particularly |
| <input type="checkbox"/> Happy | <input type="checkbox"/> Frustrated | <input type="checkbox"/> Worried | <input type="checkbox"/> Don't Care | Offensive |

 Male Enhancement/Enlargement Products

- | | | | | |
|----------------------------------|-------------------------------------|------------------------------------|--------------------------------------|---------------------------------------|
| <input type="checkbox"/> Like it | <input type="checkbox"/> Angry | <input type="checkbox"/> Disgusted | <input type="checkbox"/> Embarrassed | <input type="checkbox"/> Particularly |
| <input type="checkbox"/> Happy | <input type="checkbox"/> Frustrated | <input type="checkbox"/> Worried | <input type="checkbox"/> Don't Care | Offensive |

 Mortgage/Loan Financing

- | | | | | |
|----------------------------------|-------------------------------------|------------------------------------|--------------------------------------|---------------------------------------|
| <input type="checkbox"/> Like it | <input type="checkbox"/> Angry | <input type="checkbox"/> Disgusted | <input type="checkbox"/> Embarrassed | <input type="checkbox"/> Particularly |
| <input type="checkbox"/> Happy | <input type="checkbox"/> Frustrated | <input type="checkbox"/> Worried | <input type="checkbox"/> Don't Care | Offensive |

 Job/Employment Offers

- | | | | | |
|----------------------------------|-------------------------------------|------------------------------------|--------------------------------------|---------------------------------------|
| <input type="checkbox"/> Like it | <input type="checkbox"/> Angry | <input type="checkbox"/> Disgusted | <input type="checkbox"/> Embarrassed | <input type="checkbox"/> Particularly |
| <input type="checkbox"/> Happy | <input type="checkbox"/> Frustrated | <input type="checkbox"/> Worried | <input type="checkbox"/> Don't Care | Offensive |

 Adult Pornography Websites

- | | | | | |
|----------------------------------|-------------------------------------|------------------------------------|--------------------------------------|---------------------------------------|
| <input type="checkbox"/> Like it | <input type="checkbox"/> Angry | <input type="checkbox"/> Disgusted | <input type="checkbox"/> Embarrassed | <input type="checkbox"/> Particularly |
| <input type="checkbox"/> Happy | <input type="checkbox"/> Frustrated | <input type="checkbox"/> Worried | <input type="checkbox"/> Don't Care | Offensive |

 Child Pornography Websites

- | | | | | |
|----------------------------------|-------------------------------------|------------------------------------|--------------------------------------|---------------------------------------|
| <input type="checkbox"/> Like it | <input type="checkbox"/> Angry | <input type="checkbox"/> Disgusted | <input type="checkbox"/> Embarrassed | <input type="checkbox"/> Particularly |
| <input type="checkbox"/> Happy | <input type="checkbox"/> Frustrated | <input type="checkbox"/> Worried | <input type="checkbox"/> Don't Care | Offensive |

 Dating Websites

- | | | | | |
|----------------------------------|-------------------------------------|------------------------------------|--------------------------------------|---------------------------------------|
| <input type="checkbox"/> Like it | <input type="checkbox"/> Angry | <input type="checkbox"/> Disgusted | <input type="checkbox"/> Embarrassed | <input type="checkbox"/> Particularly |
| <input type="checkbox"/> Happy | <input type="checkbox"/> Frustrated | <input type="checkbox"/> Worried | <input type="checkbox"/> Don't Care | Offensive |

 Stock Market "Tips"

- | | | | | |
|----------------------------------|-------------------------------------|------------------------------------|--------------------------------------|---------------------------------------|
| <input type="checkbox"/> Like it | <input type="checkbox"/> Angry | <input type="checkbox"/> Disgusted | <input type="checkbox"/> Embarrassed | <input type="checkbox"/> Particularly |
| <input type="checkbox"/> Happy | <input type="checkbox"/> Frustrated | <input type="checkbox"/> Worried | <input type="checkbox"/> Don't Care | Offensive |

 Online Casino Websites

- | | | | | |
|----------------------------------|-------------------------------------|------------------------------------|--------------------------------------|---------------------------------------|
| <input type="checkbox"/> Like it | <input type="checkbox"/> Angry | <input type="checkbox"/> Disgusted | <input type="checkbox"/> Embarrassed | <input type="checkbox"/> Particularly |
| <input type="checkbox"/> Happy | <input type="checkbox"/> Frustrated | <input type="checkbox"/> Worried | <input type="checkbox"/> Don't Care | Offensive |

 "Nigerian" Fraud (i.e. want to deposit \$xx million in your bank account)

- | | | | | |
|----------------------------------|-------------------------------------|------------------------------------|--------------------------------------|---------------------------------------|
| <input type="checkbox"/> Like it | <input type="checkbox"/> Angry | <input type="checkbox"/> Disgusted | <input type="checkbox"/> Embarrassed | <input type="checkbox"/> Particularly |
| <input type="checkbox"/> Happy | <input type="checkbox"/> Frustrated | <input type="checkbox"/> Worried | <input type="checkbox"/> Don't Care | Offensive |

 Selling Other General Products/Services

- | | | | | |
|----------------------------------|-------------------------------------|------------------------------------|--------------------------------------|---------------------------------------|
| <input type="checkbox"/> Like it | <input type="checkbox"/> Angry | <input type="checkbox"/> Disgusted | <input type="checkbox"/> Embarrassed | <input type="checkbox"/> Particularly |
| <input type="checkbox"/> Happy | <input type="checkbox"/> Frustrated | <input type="checkbox"/> Worried | <input type="checkbox"/> Don't Care | Offensive |

What Are Your Feelings About Spam in General? (forgot to ask to tick selection*)

- | | | | | |
|----------------------------------|-------------------------------------|------------------------------------|--------------------------------------|---------------------------------------|
| <input type="checkbox"/> Like it | <input type="checkbox"/> Angry | <input type="checkbox"/> Disgusted | <input type="checkbox"/> Embarrassed | <input type="checkbox"/> Particularly |
| <input type="checkbox"/> Happy | <input type="checkbox"/> Frustrated | <input type="checkbox"/> Worried | <input type="checkbox"/> Don't Care | Offensive |

Discussion after ticking emotion scale selection (06:57)

A: I know (*work colleague**) next door, she gets a bit of it now, that's actually addressed to her personally, and she said that's because they've sent out email, and it's come through under the company, but because she's been out of the office it sends an auto-reply back, that's got your personal email address on.

Q: That's the organisational one though, not a personal outside one?

A: No.

Q: Yeah, ok, and she thinks it's from an auto-reply or something...

A: Yeah.

Q3 How do you feel about Unsolicited Bulk Emails (Contd...) (07:32)

b.) If you found any of the unsolicited emails you received offensive or objectionable, have you ever opened any of these emails when your work colleague(s) or manager(s) were present, or able to see your computer screen? (07:40)

N/A

c.) If so, how did you feel in this situation? N/A

d.) If not, how do you think you might feel in that situation? (08:12)

A: Oh, it wouldn't worry me.

Q: It wouldn't worry you?

A: No. It's just something that happens to everybody I think that has a computer. Life's too short to get hung up over silly little things.

Q: It's one of the hazards of life these days.

A: Mmmm... (agreement).

Q4 What do you do with Unsolicited Bulk Emails? (09:10)

a.) If participant has indicated they have received any unsolicited emails requesting personal information including a login/password (e.g. for a bank account, Paypal account etc) in section 2), then ask:

For any of the unsolicited emails you indicated you have received that requested you provide login/password information for a bank or other online financial website, have you ever:

(i) Clicked on the link provided in the email?

(ii) Entered your login ID and password?

Q: Have you ever actually received any that have perhaps got through, that asked you to click on a link saying it's from a bank or something, and they want you to click on a link and put your details in?

A: No

Q: Never received anything like that, no. So you've never clicked on anything like that.

A: I have heard of them, but I've never had one

Q: You've never personally received one?

A: No

(i) No

(ii) N/A

b.) For any other non-financial unsolicited emails, have you ever clicked on any links included in unsolicited emails you have received? (09:45)

A: No

c.) If “Yes”, what was the reason you clicked on it? e.g. it was an “Unsubscribe” or “Stop receiving” link, or you wanted to see what was on the website because it looked interesting, what? N/A

d.) Have you at any time ever purchased any products or services offered in an unsolicited email? (10:12)

A: No

e.) What do you normally do with the unsolicited emails you receive: (10:22)

Delete them?

Report them to the IT Department?

Forward them to the IT Department?

Reply to them?

Other?

A: Just delete. No I just go “delete”.

Q: Just delete them, ok. So you don’t forward them to the IT department or anything?

A: I don’t, no, and we can actually see without opening something who it’s from, and if I don’t know them I just delete.

Q: Just delete it, ok.

A: I don’t have enough time in my day to go to read every one.

Q5 What are your opinions about Unsolicited Bulk Emails? (11:04)

a.) Do you think that unsolicited emails waste your time at work? (11:06)

A: Yes

b.) Do you think they are a waste of your organisation’s time and money? (11:12)

A: Yes

Q: Now in relation to that, that’s not actually on my sheet here, but I’ve discovered that was a question I probably should have been asking, because it came up with some of the other interviews. If you have received any spam emails and things, if you’ve received any from external, perhaps clients or customers of some sort, have you, to the best of your knowledge, do think you’ve ever, or do you know if you’ve ever accidentally deleted any customer emails along with spams or spam messages that you’ve been deleting?

A: We do have to be careful because some of the stuff that, like for instance our (*external company**) reports that come through, they actually come through from (*parent company**), and they’re marked, they’re labelled as “spam”, but yet they’re not, so we’ve got to be careful that we’re not deleting, so it is, it’s one (1) It’s a waste of time, but I don’t think we’ve actually deleted any, no.

Q: So they're legitimate emails that have been...

A: Yes

Q: ...tagged as spam...

A: Yes

Q: ...but they're not?

A: No

Q: As far as you know you've never accidentally deleted anything from anybody?

A: No, not that I know of.

c.) How well do you think your organisation is doing in controlling the amount of unsolicited email being received? Is it doing a good job, a poor job? (12:30)

A: Oh, I think it's doing a good job, yes.

d.) Do you think more could be done by your organisation to control unsolicited email? (12:42)

A: Probably not by them, I think, I don't actually know how you'd go about stopping it, because it's just a form of advertising isn't it, so, it's just technology's way of sending out stuff via your Inbox rather than your letterbox. It's just a shame that ninety percent of it is useless.

Q: So you think they're probably doing as much as they can do?

A: Yeah. I don't know what can be done about it.

e.) If "Yes", what more do you think they could do to control it? (13:23) N/A

f.) Do you think your organisation could provide you with more information about unsolicited email? (13:35)

A: I wouldn't want it.

Q: No?

A: No. You have enough to do and read and whatnot without getting stuff that's not work-related to do, so I'd rather...

Q: So, you don't really think they could give you...

A: No

Q: ...you've indicated before you pretty much know what to do with it now anyway, you usually just delete it so...

A: Yep, exactly, so...

Q: So that's a "no".

g.) If "Yes", what information do you think they should provide? (14:07) N/A

References

- Andrew, C. (2003). *Consumer attitudes regarding unsolicited commercial email (spam)*. Retrieved August 7, 2007, from http://www.tacd.org/db_files/files/files-296-filetag.doc
- Antonius, R. (2003). *Interpreting quantitative data with SPSS*. London: SAGE.
- Ashkanasy, N. M. (2002). Studies of cognition and emotion in organisations: Attribution, affective events, emotional intelligence and perception of emotion. *Australian Journal of Management*, 27(2), 11-20. Retrieved August 7, 2007, from <http://www.agsm.unsw.edu.au/eajm/0209/pdf/ashkanasy.pdf>
- Biegel, S. (2001). *Beyond our control?: Confronting the limits of our legal system in the age of cyberspace*. Cambridge, Massachusetts: The MIT Press.
- Bryman, A. (2004). *Social research methods* (2nd ed.). Oxford: Oxford University Press.
- Campbell, A. (1989). Emotions and Adjustment. In Campbell, A. (Ed.), *The opposite sex* (pp. 182-189). Sydney: Doubleday.
- Cannon, J. C. (2005). *Privacy: What developers and IT professionals should know*. Boston, MA: Addison-Wesley.
- Cerf, V. G. (2005). Spam, spim, and spit. *Communications of the ACM*, 48(4), 39. Retrieved August 8, 2007, from <http://delivery.acm.org/10.1145/1060000/1053314/p39-cerf.pdf?key1=1053314&key2=4547156811&coll=Portal&dl=ACM&CFID=26140886&CFTOKEN=45316407>

- Consumers' Institute of New Zealand. (2007). *Spam*. Retrieved August 7, 2007, from <http://www.consumer.org.nz/topic.asp?docid=1639&category=Computers%20%26%20Phones&subcategory=Internet&topic=Spam>
- Cournane, A., & Hunt, R. (2004). An analysis of the tools used for the generation and prevention of spam. *Computers & Security*, 23(2), 154-166
- Creswell, J. W. (2003). *Research design: Qualitative, quantitative, and mixed method* (Second ed.). Thousand Oaks, California: Sage Publications.
- Dantin, U., & Paynter, J. (2005). *Spam in email inboxes*. Paper presented at the 18th Annual Conference of the National Advisory Committee on Computing Qualifications, Tauranga, New Zealand. Retrieved August 7, 2007, from http://www.naccq.co.nz/conference05/proceedings_05/papers/dantin_spam.pdf
- de Vaus, D. A. (1995). *Surveys in Social Research* (4th ed.). St Leonards, Australia: Allen & Unwin.
- Dye, K. (2007). Organizational stress. In Mills, A. J., Mills, J. C. H., Forshaw, C. & Bratton, J. (Eds.), *Organizational behaviour in a global context* (pp. 241-264). Peterborough, Ontario: Broadview Press.
- Employers and Manufacturers Association (Northern). (2004). *Small business Internet security survey results*. Auckland: Employers and Manufacturers Association (Northern).
- Employers and Manufacturers Association (Northern). (2005). *Symantec and EMA Internet security survey 2005*. Retrieved August 7, 2007, from http://www.ema.co.nz/Internet_Security_Survey_2005.pdf

- Fallows, D. (2005). *CAN-SPAM a year later*. Retrieved August 7, 2007, from http://www.pewinternet.org/pdfs/PIP_Spam_Ap05.pdf
- Fawcett, T. (2003). "In vivo" spam filtering: A challenge problem for KDD. *SIGKDD Explorations Newsletter*, 5(2), 140-148. Retrieved August 7, 2007, from <http://delivery.acm.org/10.1145/990000/980990/p140-craven.pdf?key1=980990&key2=9244846811&coll=GUIDE&dl=GUIDE&CFID=26093390&CFTOKEN=29270817>
- Ferrera, G. R., Lichtenstein, S. D., Reder, M. E. K., August, R., & Schiano, W. T. (2001). *Cyberlaw: Your rights in cyberspace*. Cincinnati, U.S.A.: Thomson Learning.
- Fisher, C. D. (2000, Mar2000 Special Issue). Mood and emotions while working: Missing pieces of job satisfaction? *Journal of Organizational Behavior*, 21(2), 185-202. Retrieved June 27, 2007, from <http://libproxy.unitec.ac.nz:2048/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=buh&AN=13620093&loginpage=Login.asp&site=ehost-live&scope=site>
- Fitzsimons, M. (2002, February 10-12). *The medium and the message: Harassment at work*. Paper presented at the NetSafe: Society, Safety and the Internet Conference, Auckland, New Zealand. Retrieved August 7, 2007, from University of Auckland, Department of Computer Science Web site: <http://www.cs.auckland.ac.nz/~john/NetSafe/Fitzsimons.pdf>
- Fontana, J. (2003). *Tallying the true cost of spam*. Retrieved August 7, 2007, from <http://www.networkworld.com/news/2003/1117spamcost.html>

- Framingham, G. K. (2007). *Spam spikes wreak havoc*. Retrieved June 21, 2007, from <http://computerworld.co.nz/news.nsf/scrt/D9BA4FBB4377E31DCC2572F00077281A>
- Framingham, J. B. (2007). *New type of image spam hides in email wallpaper*. Retrieved June 21, 2007, from <http://computerworld.co.nz/news.nsf/scrt/499A0A628DEE44ACCC2572FB000D43FE>
- Garfinkel, S. (2007, June). Spam, a Lot [Electronic Version]. *CSO*. Retrieved August 8, 2007, from http://www.csoonline.com/read/060107/col_mch.html
- Gibbs, M. (2003a). *What spam really costs, part I. Backspin*. Retrieved August 7, 2007, from <http://www.networkworld.com/columnists/2003/0630backspin.html>
- Gibbs, M. (2003b). *What spam really costs, part II. Backspin*. Retrieved August 7, 2007, from <http://www.networkworld.com/columnists/2003/0707backspin.html>
- Graham-Cumming, J. (2005). *People and Spam*. Retrieved August 7, 2007, from <http://www.jgc.org/pdf/spamconf2005.pdf>
- Grandey, A. A., Tam, A. P., & Brauburger, A. L. (2002). Affective states and traits in the workplace: Diary and survey data from young workers. *Motivation and Emotion*, 26(1), 31-55. Retrieved August 7, 2007, from <http://www.personal.psu.edu/faculty/a/a/aag6/M&E.pdf>
- Harris, D. (2003). *Drowning in sewage*. Retrieved July 26, 2007, from <ftp://ftp.usm.maine.edu/pegasus/misc/spam.zip>
- Harvey, D. (2003). *internet.law.nz: Selected issues*. Wellington: LexisNexis NZ.

- InternetNZ. (2006a). *The four golden rules*. Retrieved August 7, 2007, from <http://www.stopspam.net.nz/rules.htm>
- InternetNZ. (2006b). *Reducing Spam*. Retrieved July 26, 2007, from <http://www.stopspam.net.nz/reducing.htm>
- Klotz, R. J. (2004). *The politics of Internet communication*. Lanham, Maryland: Rowman & Littlefield.
- Le, Z., Jingbo, Z., & Tianshun, Y. (2004). An evaluation of statistical spam filtering techniques. *ACM Transactions on Asian Language Information Processing (TALIP)*, 3(4), 243-269. Retrieved August 7, 2007, from <http://delivery.acm.org/10.1145/1040000/1039625/p243-zhang.pdf?key1=1039625&key2=6987846811&coll=GUIDE&dl=GUIDE&CFID=26100038&CFTOKEN=44048619>
- Macnair, E. (2003). *The lawsuit hidden in the inbox*. Retrieved August 7, 2007, from <http://technology.guardian.co.uk/online/spam/story/0,13427,1105242,00.html>
- MessageLabs Ltd. (2007). *MessageLabs Intelligence: May 2007 "Spam Spikes – The Battering Ram of Spam"*. Retrieved June 21, 2007, from http://www.messagelabs.com/mlireport/2007%2005%20May%20MLI_final.pdf
- Messaging Anti-Abuse Working Group. (2007). *Email Metrics Report: Third & Fourth Quarter 2006*. Retrieved June 20, 2007, from http://www.maawg.org/about/MAAWGMetric_2006_3_4_report.pdf
- Nucleus Research Inc. (2003). *Spam: The silent ROI killer*. Retrieved August 7, 2007, from <http://www.nucleusresearch.com/research/d59.pdf>

Nucleus Research Inc. (2004). *Spam: The serial ROI killer*. Retrieved August 7, 2007, from <http://www.nucleusresearch.com/research/e50.pdf>

OECD Directorate for Science Technology and Industry. (2005a). *Anti-spam law enforcement report*. Retrieved August 7, 2007, from <http://www.oecd.org/dataoecd/18/43/34886680.pdf>

OECD Directorate for Science Technology and Industry. (2005b). *Spam issues in developing countries*. Retrieved August 7, 2007, from <http://www.oecd.org/dataoecd/5/47/34935342.pdf>

Owen, D. H. (2003). Cognitive Ergonomics. In O'Driscoll, M., Taylor, P. & Kalliath, T. (Eds.), *Organisational psychology in Australia and New Zealand* (pp. 239-261). Oxford: Oxford University Press.

Rudman, R. (2003). *New Zealand employment law guide* (2003 ed.). Northcote: CCH New Zealand.

Saarinen, J. (2006, November 20). *Ihug still fighting to sort out spam fiasco*. Retrieved June 21, 2007, from <http://computerworld.co.nz/news.nsf/news/DA2189F09441164ACC257229000DE7BD>

Simpson Grierson x-tech group. (2002). *A guide to e-commerce law in New Zealand*. Wellington: Brookers.

- Siponen, M., & Stucke, C. (2006). *Effective anti-spam strategies in companies: An international study*. Paper presented at the Proceedings of the 39th Annual Hawaii International Conference on System Sciences (HICSS'06), Hawaii. Retrieved August 8, 2007, from <http://csdl2.computer.org/comp/proceedings/hicss/2006/2507/06/250760127c.pdf>
- Slane, B. (2003). *Letter to the Minister of Communications*. Retrieved August 7, 2007, from <http://www.privacy.org.nz/library/letter-to-the-minister-of-communications>
- Spammer-X. (2004). *Inside the spam cartel: Trade secrets from the dark side*. Rockland, MA.: Syngress.
- St Sauver, J. (2004). *How UO deals with spam: A brief strategic overview with some tactical suggestions*. Retrieved August 7, 2007, from <http://www.uoregon.edu/~joe/icplspam/icpl-spam-presentation.pdf>
- The Internet Safety Group, & MYOB. (2004). *NetSafe Internet security survey*. Retrieved August 7, 2007, from http://www.netsafe.org.nz/Doc_Library/publications/ISG_-_MYOB_results.pdf
- The New Zealand Department of Internal Affairs. (2007). *The Unsolicited Electronic Messages Act 2007. Spam*. Retrieved July 27, 2007, from <http://www.spam.govt.nz>
- Ward, B. (2003, July 9-12). *The problem of spam and the counter measure options for New Zealand*. Paper presented at the NetSafe II: Society, Safety & the Internet Conference, Auckland, New Zealand. Retrieved August 7, 2007, from http://www.netsafe.theoutfitgroup.co.nz/Doc_Library/netsafepapers_bradward_spam.pdf

Ward, M. (2003). *Sexual spam could spark lawsuits*. Retrieved August 7, 2007, from <http://news.bbc.co.uk/2/hi/technology/3256814.stm>

Yin, R. K. (2003). *Case study research: Design and methods* (Third ed.). Thousand Oaks, California: Sage.

Zikmund, W. G. (2003). *Business research methods* (7th ed.). Mason, Ohio: South-Western.