TE WHARE WĀNANGA O TE ŪPOKO O TE IKA A MĀUI
VICTORIA
UNIVERSITY OF WELLINGTON

SCHOOL OF GOVERNMENT
Te Kura Kāwanatanga

Kiwis Managing their Online Identity Information

Second and Final Research Report – Interview Findings, Focus Group Findings and Project Recommendations

Professor Miriam Lips, Dr Elizabeth Eppel, Lynn Barlow, Barbara Löfgren, Dr Karl Löfgren and Dr Dalice Sim

Victoria University of Wellington
February 2015

Acknowledgements

This is the second and final report from the research project ‘Kiwis Managing their Online Identity Information’. The research was financially sponsored by the Department of Internal Affairs. A first research report including the research findings of the representative survey amongst New Zealanders was published in 2014. Further information on this research, including electronic copies of the two research reports, can be found on the VUW Chair in e-Government website at www.e-government.vuw.ac.nz

The research was led by Professor Miriam Lips, Chair in e-Government in the School of Government at Victoria University of Wellington. Other researchers from Victoria University involved in this project are Dr Elizabeth Eppel, Dr Karl Löfgren, Dr Dalice Sim, Lynn Barlow and Barbara Löfgren. A Project Advisory Group has been established for this research, including representatives from the Department of Internal Affairs, NZ Police, Office of the Privacy Commissioner, Ministry of Justice, Ministry of Business, Innovation & Employment, State Services Commission, Inland Revenue, Ministry of Consumer Affairs, Statistics New Zealand and Storymaker Institute.

The Chair in e-Government would like to acknowledge the Department of Internal Affairs for their financial sponsorship of this project, the e-Government Chair sponsors, i.e. Victoria University of Wellington, Datacom Systems Ltd and Department of Internal Affairs, for supporting additional research time for this initiative and their continuing support of independent e-Government research projects of importance to New Zealand, and the members of the Project Advisory Group for their most valuable advice and support of this research activity.

Table of Contents

Acknowledgements 2
Table of Contents 3
Executive Summary 10
Introduction 10
High-level research findings 10
Project recommendations 14
Better access to high quality knowledge about online behaviour 14
Education and training 14
Increased transparency about online identity information 15
Authorised secure Internet access and online identity verification 15
Cost of online security 15
A better alignment of digital service design assumptions with user needs or experience 15
Research Design 16
Research motivation and objectives 16
Individual interviews with some participant observation 16
Focus Groups 17
Analysis of results: spiralling approach of the research design 19
Analysis of Individual Interviews 20
Thumbnails of interview participants 21
Interview findings 26
A public space 26
Privacy awareness 26
Online identity 28
Online identity behaviours change over time 28
Bad online experience 29
Maturing online behaviours 30
Security awareness 32
Deliberate strategies to manage privacy and security of transactions 33
Online experience and competence 33
Personal experience with cyber-enabled crime 35
Trust and authenticity 36
Online protection strategies 37
Online risk mitigation 38
Internet knowledge strategies 39
Privacy behavioural types 41
Analysis of the Focus Groups 43

Introduction 43
Composition of each Focus Group 43
Background of the Focus Group participants 45
Internet use of the Focus Group participants 46
  Internet activities 46
  Devices 48
  Location and frequency of Internet use 50
Focus Group findings 52
  Critical importance of Internet use 52
    Reliance on technology 53
    Addictive 54
  Online vs Offline 54
    Online vs offline trust 55
    Offline is of superior quality 56
    Online is different compared to offline 57
    Same behaviours but in different environments 57
    Younger generations behave differently online compared to older generations 58
  Drivers of Internet use 59
    Access to knowledge and information 59
    Communication 60
    Social networking 61
    Online entertainment 62
    Purchasing online 63
    Trading online 65
    Online banking 65
    Applying for jobs online 65
    Online government transactions 65
    Online dating 67
  Sharing identity information online 67
    Context matters for sharing identity information online 67
    Understanding the value of information 68
    No individual choice but to share identity information online 68
    Too much information being asked to share online 70
    Private information being asked to share online 71
    Lack of transparency 71
    Social Networking Sites ‘owning’ your information 72
    Permanency of information 72
    Multi-channel behaviours in online transactions 73

Online privacy ... 73
Financial information is often considered highly sensitive information ... 73
Other types of private information ... 74
Trading off privacy against public safety ... 74
Preference for privacy-friendly sites or apps ... 75
Online security ... 75
Security concerns over Internet use ... 75
Security awareness ... 75
Lack of understanding of online security ... 76
Experiences with cyber(-enabled) crime ... 76
Actual experiences ... 76
Not all illegal activities are considered to be bad ... 79
Protecting online identity information ... 80
Using a safe or protected location ... 80
Using anti-virus software ... 80
Using a safe device ... 81
Using privacy settings ... 81
Friends' policy on Social Networking Sites ... 81
Using minimal information ... 82
Using real vs fake information ... 82
Using pseudonyms ... 83
Using multiple email addresses ... 83
Using passwords ... 84
Using protected WiFi ... 85
Logging out ... 86
Deleting email when you don't know the sender ... 86
Checking the use of language in a suspicious email ... 86
Using a credit or debit card with a limited amount of money ... 86
Deleting credit card details ... 86
Not providing location details ... 87
Not giving permission to use contact information ... 87
Not sharing information online ... 87
Not using online ... 87
Other security strategies ... 87
Monitoring other people's online behaviour ... 88
Trust in sharing identity information online ... 88
Trust is critically important for sharing information online ... 88
Trust in online banking ... 89

Trust in Government 89
Untrustworthy sites 90
A bad experience can lead to distrust 91
Prior experience is of critical importance 91
Location matters 91
Physical presence creates trust 92
Brand recognition enhances trust 92
Reputation is critically important 92
Trust based on experience of people you know and trust 93
Trust can be influenced by media stories 93
Knowledge 93
Lack of knowledge 93
Knowing that they don’t know 94
Knowing what they need to know 94
Privacy knowledge is critical 94
Getting help 95
Receiving help from others 95
Self-help 95
Searching for help online 95
Help for older people 95
Young people sharing their knowledge 96
Teaching children 96
Changing online behaviour over time 96
Becoming more private over time 96
Becoming less private over time 97
Bad experience usually drives changed online behaviour 97
Positive experiences can outweigh negative experiences 98
A positive intervention can negate a bad experience 98
Changing behaviours through learning from bad stories in the news 98
Making mistakes belongs to the learning 98
Learning over time 98
Changing behaviours through learning from others 99
Privacy behavioural types 99
Privacy pragmatists 99
Privacy victims 100
Privacy optimists 100
Privacy fatalists 100
Online behaviours of particular groups of participants 101

Young people 101

Critical importance of the Internet 101

Internet as playground 103

Multi-tasking 103

Struggle to understand government 104

RealMe 104

Online Privacy 105

Privacy savvy 105

Private information 105

Privacy pragmatists 105

Online security 106

Security savvy 106

Lack of transparency 106

Experiences with cyber(-enabled) crime 106

Protecting online identity information 107

Using a safe and protected location 107

Using privacy settings 108

Friends' policy on Social Networking Sites 108

Using minimal information 108

Using real vs fake information 108

Using passwords 108

Using multiple email addresses 109

Using pop-up blockers 109

Trust in sharing identity information online 109

Changing online behaviour over time 110

Growing up in the digital age 110

Hacking experiences and other online jokes do not change online behaviour 110

Bad experience 111

Senior citizens 111

Internet use as necessity to keep up with changes in society 111

Offline vs online use 111

Young people are different compared to older generations 112

Online banking 112

Use of Social Networking Sites 113

Sharing identity information online: privacy victims 113

Online privacy 114

Online security 114

Experiences with cyber(-enabled) crime 114

Protecting online identity information 114
Using minimal information 114
Using antivirus software 115
Using passwords 115
Trust in sharing identity information online 115
Getting help 115
Changing online behaviour over time 115
Bad experience leads to change in online behaviour 115
People from different ethnic backgrounds 116
Māori 116
Critical importance of the Internet 116
Online vs offline use 116
Sharing identity information online 116
Online privacy 117
Privacy pragmatists 117
Privacy victims 118
Privacy optimists 118
Protecting identity information online 118
Using fake information 118
Using pseudonyms 118
Trust in sharing identity information online 118
Changing online behaviour over time 119
Pasifika 119
Critical importance of the Internet 119
Sharing identity information online 120
Online privacy 120
Privacy victims 120
Experiences with cyber(-enabled) crime 121
Protecting identity information online 121
Using real vs false information 122
Concerns for online security 122
Trust in sharing identity information online 122
Changing online behaviour over time 123
Learning about online behaviour 123
Asian people 123
Critical importance of the Internet 123
Online devices 124
Sharing identity information online 124

Online privacy 125
Privacy pragmatists 125
Private information 125
Online security 125
Experience with cyber(-enabled) crime 126
Protecting online identity information 126
Using real vs fake information 126
Using pseudonyms 126
Trust in sharing identity information online 127
Trust in government sites 128
Changing online behaviour over time 128
Learning about online protection 129
Project recommendations 130
Better access to high quality knowledge 130
Education and training 131
Increased transparency about online identity information 132
Authorised secure Internet access and online identity verification 133
Cost of online security 134
A better alignment of digital service design assumptions with user needs or experience 135
References 135
Annex 1 - Definitions of terms used 136
Annex 2 – Individual Interview Guide and Observation Protocol 137
Annex 3 – Focus Group Interview Guide and Observation Protocol 139

Executive Summary

Introduction

The objectives of the study ‘Kiwis managing their online identity information’ are to get an in-depth understanding of the online identity information behaviours of New Zealanders (i.e. what they do online with their personal information, or not do, and why they do it), in commercial transactions, transactions with government, and on Social Networking Sites (SNSs). Another objective is to better understand people’s actual experiences with forms of cybercrime or cyber-enabled crime and how they have responded to these bad online experiences.

This Second and Final Research Report presents the cumulative findings of the enquiry, particularly qualitative research phases two and three, and the recommendations resulting from the research project as a whole. An overview of the research design of this study as well as the results from the first research phase, a representative survey with 467 participants, can be found in our Interim Research Report available via our website (http://e-government.vuw.ac.nz). The findings from each research phase were used iteratively in the subsequent phases to explore the reasons for specific online behaviours and develop an in-depth understanding of the interaction between the individual, their identity information and the contexts in which people share and protect their identity information online. Definitions and explanations of key terms used in this research project are presented in Annex 1 of this report.

The second research phase consisted of 23 in-depth interviews with some participant observation. During these interviews, the online behaviours of an individual could be explored in more depth to understand what people actually do in managing their online identity information and particularly also why they did it. Brief sketches of the online identity behaviours of each (anonymised) participant can be found on p. 21 of this report.

The third research phase was a set of ten qualitative focus groups with 72 participants in total from different age groups, socio-economic and ethnic backgrounds, and geographic locations. A description of the composition and background of each focus group can be found starting on page 43 of this report. The focus groups were used to explore the preliminary findings from research phases one and two in greater depth with groups of like individuals to understand more about the complex relationship between the individual online behaviours described and the sharing or protecting of their identity information in particular contexts and relationships.

The high-level findings of research phases two and three are summarised in the following section. An overview of the recommendations resulting from this project is provided in the Project Recommendations section.

High-level research findings

Although the Internet played a critically important role in the lives of the large majority of the research participants, it also turned out to be a relatively new and highly uncertain environment for most of them: for instance, most participants admitted knowing that they don’t know what information is collected on them, what they can share in online environments, or how it is being used, for example. Knowledge about Internet use and online behaviour came through learning from experience, training, and learning from others. Changes in online behaviour particularly occurred as a result of learning through experience and learning from others. A bad experience usually had changed people’s online behaviour in a profound way. Sometimes, people had changed their online behaviour through learning from stories in the news or what had happened to a close associate.

In general, people's online behaviours were not mature yet but dynamic, with the exception of online banking where the majority of participants demonstrated more 'crystallised' behaviours. Online behaviours were changing over time as people were learning about what to do, or not do, online and based on their online experience. The large majority of participants indicated that they had shifted from more public online behaviours to more private online behaviours over time. For instance, the interview findings particularly show that the more online experience people had, the more likely they were to obscure aspects of their 'real' identity (e.g. by using pseudonyms or providing fake information); less experienced participants more commonly used their 'real identity' as their 'default setting' in varying online relationships. In general, although young people were adventuresome in online environments, they too were privacy savvy and indicated that they had become more private online over time.

In general, we found that people from different age groups, ethnic backgrounds and those with low levels of education or Internet expertise demonstrated different online behaviours, which also revealed differences in privacy perceptions. For example, young people were living their lives not only via (multiple) online environments seamlessly interwoven as an essential part of their offline existence, they also demonstrated strong online privacy behaviours by using pseudonyms and fake information, for instance. Older people on the other hand had much more trust in the offline world, had a clearer delineation between online and offline and perceived offline social interactions as superior in quality. They hardly exchanged any identity information in online relationships and often would back out of a transaction if they thought too much identity information was required. Māori and Pasifika were much more inclined to share identity information in online relationships, compared to Pākehā or Asian people. Pasifika and people with low levels of education or Internet expertise more often have had a bad online experience compared to other participants.

Although (low) income was a significant variable in influencing online behaviours in our representative survey, we didn't find any evidence of significance of this variable in our interviews or focus group findings.

All research participants in the interviews and the focus groups found being private online of critical importance and were privacy aware in their online behaviours. For instance, participants pointed out how important they considered the location of their Internet use for privacy and security reasons, with most of them preferring Internet use, in particular financial transactions, at home or via encrypted WiFi or a device only the individual could access. Several participants deliberately used different online devices for different tasks, considering privacy, security, and usability. Many participants had a preference for privacy-friendly social networking sites or apps. Some of them were also monitoring other people's online behaviours, in most cases their own children, to protect their privacy and make sure that they were secure online.

Most of the participants considered financial information, their children's names, their phone number, home address, and passwords as private information. Photos were also considered by many as private information but only to a certain extent, as participants usually didn't have an issue with sharing photos with close friends and family.

However, although privacy was of importance to all participants, we found that they belonged to different privacy behavioural types, which we have named the privacy pragmatist, the privacy victim, the privacy optimist, and the privacy fatalist:

- **Privacy pragmatist**: depending on the transactional relationship, privacy is a commodity for the privacy pragmatist ("*personal information helps you to get the services you want/need*"). Identity information is traded in for convenience, cost- and time-efficiency, and particular services;

- **Privacy victim**: a loss of privacy is inevitable in order to use the service: a privacy victim sees no choice. They stop using the online service when the informational demands are too intrusive;
- **Privacy optimist**: privacy optimists are willing to keep doing online what they think might be risky until something bad happens to confirm it; and
- **Privacy fatalist**: a major breach of privacy and power imbalance are inevitable and unescapable in the view from the privacy fatalist.

The majority of our participants were privacy pragmatists. Participants indicated that context matters for what (types of) identity information they would share online. Also, that online information-sharing is about trust and who they are dealing with. Most of them understood that identity information has value in the online world: if you want to use an online service, you'll need to provide personal information in exchange.

However, many participants felt that they often don't have a choice other than to share their identity information online, and that they are frequently being asked for too much information. Several of them indicated that when it is too intrusive, they stop and exit the online transaction. For these reasons, multi-channel behaviours were quite common amongst the participants, with people using the Internet to search for relevant information online before concluding the transaction offline. Participants of 35 years and older had more trust in offline channels and preferred offline social interactions to online interactions and social networking.

Participants described how sometimes assumptions and expectations from online service providers, such as government agencies, were not correct and didn't meet user needs. For example, government websites could be very complex for participants to navigate or understand, or required too much form filling, leading to a preference for other channels. Another example that emerged in our discussions was that social welfare recipients are expected to have a cell phone which they can use for online authentication. However, several of our participants pointed out that they did not have a cell phone or had one that they needed to share with several family members. Another design assumption that young people would prefer to deal with government via online channels, is not supported in practice, as one young participant explained:

> "*Facebook is just so easy. But when you start thinking about doing Government stuff it's like, I don't know how it works, their websites are so hard to use. They send you to different places and it isn't clear how to get to where you want to go. Like finding out whether you can have an allowance or not. The sort of question every student wants to ask. You Google 'can I get an allowance' and it doesn't say yes or no. It says well there is this factor and that factor, but it doesn't actually tell you the information simply. Regarding those sort of things I would rather not use the Internet and go in person to the Studylink office and have someone tell you the answer straight away. They know all the information because it is their job*." FG3 female

Compared to experiences from people living overseas[12] , our New Zealand participants had fairly limited actual experience with forms of cybercrime or cyber-enabled crime. Two interview

[1] See for instance for experiences in the USA: PWC (2014) US cybercrime, rising risks, reduced readiness. Key findings from the 2014 US State of Cybercrime Survey, available at http://www.pwc.com/en_US/us/increasing-it-effectiveness/publications/assets/2014-us-state-of-cybercrime.pdf

[2] See for instance for experiences in the UK: a 2013 report from the UK Home Office, authored by McGuire & Dowling, Cybercrime: A Review of the Evidence. Summary of key findings and recommendations, Research report 75, available at

participants had a personal experience with their online identity being stolen: one participant had her photo posted on an online dating site without her knowledge and the other participant had an email account created in her name and used to send annoying emails to her work colleagues and create an online profile that could be linked to her and affect her reputation and professional relationships.

Although many participants had received phishing emails, only a few participants had clicked on the link provided in the email and got into problems. One participant got sucked into a Nigerian scam. A couple of participants had the experience of credit card fraud online or receiving regular credit card bills after buying just one product online. One participant had their bank account information used falsely to obtain goods and money. A few had bought something on TradeMe and the goods never turned up, and one or two had purchased goods via a fake site. Several participants had the experience of viruses or malware downloaded on their device. One participant had been hacked by the recent Adobe hack and another person had their Hotmail account hacked.

A couple of interview and focus group participants had a bad online experience where they were presented with a ‘friend’ request by the user of a stolen identity purporting to be a known friend. However, several participants who had received fake friend requests on Facebook, were aware that their friend’s Facebook account had been hacked and did not accept the request.

For young people, hacking into their friends’ devices or Facebook accounts was a relatively common activity and seen as a way of teasing them. However, these online ‘playground behaviours’ were within normative boundaries: only to friends who would be able to cope with the joke. They indicated that they would not hack into ‘more serious’ online accounts, such as an online bank account.

People used a wide range of strategies to protect themselves online. All participants used anti-virus software although those using freeware more often reported problems with scam emails and popup sites. The large majority of participants made use of the privacy settings of sites, apps or accounts. Some explained that they have uninstalled apps which requested access to their contact information, and many participants had developed a friends policy on Facebook, such as only accepting people who they know. People indicated that they delete emails when they do not know the sender.

Many participants used multiple passwords and had developed strategies for their use: many, in particular older people but also others, indicated having problems with remembering them. Some indicated that they do not store any of their passwords or usernames on their device. Participants also used multiple email addresses, often keeping email addresses revealing their real name for more ‘official’ communications, such as for work or interactions with government. Especially young people and Asian people, but also others, used pseudonyms on social networking sites and other online relationships.

Several participants indicated that they always log out of the online transaction or do not save any sensitive information, such as credit card details, on the site. Some also deleted their credit card details immediately after an online transaction. A few participants explained that they protect themselves in online commercial transactions by using a credit or debit card with only a limited amount of money on the card.

Many participants used protected WiFi, instead of public WiFi. Some also indicated that they use what they perceive as being a ‘safe device’, such as a mobile phone or an Apple product versus an Android product. Especially Asian people perceived their mobile phone as being a safe online device. Some participants had restricted access to their device for other users, using a pin, a password or biometrics (e.g. fingerprint). Quite a few participants indicated that they have turned off their

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/246749/horr75-summary.pdf location when they are online. However, some participants saw the benefits of having their location switched on, such as young people for using online dating services like Tinder, or participants who had experienced the Christchurch earthquakes and wanted to be able to locate where their family members are.

Quite a few participants indicated only using minimal information in online relationships, particularly in relationships with commercial providers where they felt that they had a choice to do so. Similarly, several of them used fake or incomplete information when possible, with the exception of older people, who never wanted to “lie”. Some participants used the protection strategy of not sharing any identity information online, and a few did not use online transactions.

The large majority of the participants trusted the exchange of identity information via online banking, with the exception of the majority of older participants, who were keen on the tangibility of a counter transaction, and those with a bad experience with online banking. Most participants trusted (New Zealand) government sites with their identity information more than other websites. The majority of them also found location an important condition for trust, and therefore trusted New Zealand sites more than overseas websites for reasons of having a local physical presence, being able to look them up or contact them if needed, and having the protection of New Zealand consumer laws. Reputation, brand recognition, and (online) reviews were all important for participants in order to establish trust in a particular site. Also, trust could be influenced by people they know, or via media stories. Untrustworthy sites were considered to be illegal sites, sites with lots of adverts or pop-ups, sites that ask to save your credit card details, or any site participants were not familiar with.

However, varying people experienced a lack of transparency around the collection, use and processing of their identity information in online relationships. For vulnerable people, such as those dependent on a low income or with a low level of education, this sometimes created an increased lack of trust.

Project recommendations

Better access to high quality knowledge about online behaviour

Recommendation 1 – An 0800 number to call for help

Recommendation 2 – Set up an online panel of more experienced users willing to answer questions and share their learning and experience with novices

Recommendation 3 - Set up an authoritative (e.g. government) site where people can find information about (how to manage) online risks and which sites can be trusted or not

Education and training

Recommendation 4 – Pair young people with older people to offer online support to older people and share young people’s knowledge and expertise

Recommendation 5 – Offer more Computers in Homes and SeniorNet courses, in particular more advanced courses on online privacy and security, and how people can protect themselves better online

Recommendation 6 – Offer tailored education and training programmes to people from various backgrounds on how to keep themselves private online

Increased transparency about online identity information

Recommendation 7 – Promote increased transparency and transparency reporting on how organisations, websites and/or apps collect, process and use online identity information

Recommendation 8 – Promote increased transparency on people's digital footprint and how to manage it

Recommendation 9 – Introduce user-centred Transparency Impact Assessments (TIAs), taking into account different training and education needs around online privacy and security for users from varying backgrounds

Authorised secure Internet access and online identity verification

Recommendation 10 – Introduce the option for people to safely interact with government agencies online at all stages of the service transaction

Recommendation 11 – Promote RealMe more extensively as a safe online identity verification and single log-on service

Recommendation 12 – Promote the use of more sophisticated levels of security in online transactions, such as online authentication and identity verification

Cost of online security

Recommendation 13 – Promote the use of anti-virus programmes with higher online protection levels by reducing the cost

A better alignment of digital service design assumptions with user needs or experience

Recommendation 14 – Make sure that digital service design assumptions are closely aligned with actual user needs or experience and user feedback

Recommendation 15 – Undertake more research into the varying online user needs and requirements of different groups of the New Zealand population, including how privacy-by-design in digital service provision could be achieved from a differentiated user perspective and continuously improved through the collection of user feedback

Research Design

Research motivation and objectives

This research initiative aimed to address an important knowledge gap by exploring the actual behaviours of people in disclosing and protecting their identity information in online relationships with government, the private sector and with family and friends. Existing research in this area commonly looks at the attitudes or perceptions of people towards sharing their personal information online with others. However, research has demonstrated that there are differences between people's perceptions and what individuals actually do online (e.g. Viseu et al. 2004)[3].

The research objectives are to:

- *get a deeper understanding of the online identity information behaviours of New Zealanders in varying e-relationships enabled by different online channels;*
- *get a deeper understanding of the actual experiences of New Zealanders with forms of cybercrime and their responses; and*
- *identify effective solutions for the New Zealand government in managing risks around the observed online identity information behaviours and people's experiences with cybercrime*.

There are three distinct phases to our research. The first phase, which has already been reported upon in our Interim research report, surveyed 467 participants about aspects of their online experience and behaviour (Lips, Eppel, Sim, Barlow, & Lofgren, 2014). This report focuses on two subsequent qualitative phases of our research into the online identity behaviours of Kiwis. Through this qualitative research we were able to delve deeper into understanding why people are doing, or not doing, particular things online. In these phases, we explored the online behaviours of New Zealanders and their actual experience with forms of cybercrime and cyber-enabled crime, such as phishing, spam and identity theft, to flesh out the findings of the quantitative, representative survey.

The second phase consisted of in-depth interviews with some participant observation, which we undertook with a relatively small number of individuals. During these interviews, the online behaviours of an individual could be explored in more depth to understand what they did in managing their online identity information and why they did it. The third phase was a set of ten focus groups in which the preliminary findings from phases one and two were explored to greater depth with groups of like individuals to understand more about the complex relationship between the individual behaviours described and their identity information in particular contexts and relationships. The findings from each phase were used iteratively in the subsequent phases to explore the reasons for specific online behaviours and develop a deeper understanding of the interaction between the individual, their identity information and the contexts in which people share and protect their identity information online. The specifics of the research methodology and design for the qualitative phases two and three are described in detail in the following two sections.

Individual interviews with some participant observation

Semi-structured interviews with 23 research participants with some participant observation were conducted prior to August 2014. These participants came from varying age groups, geographic locations, and ethnic backgrounds to reflect all the population segments represented in the quantitative survey in research phase one.

Electoral roll data was used to randomly select potential interview candidates within the stratified samples of different age groups, from geographic locations across New Zealand, and from Māori or

[3] Viseu, A., Clement, A., & Aspinall, J. (2004). Situating privacy online: Complex perceptions and everyday practices. *Information, Communication and Society, 7*(1), 92-114.

non-Māori backgrounds. We used Māori and Pasifika networks within the university and wider community networks to help us find young Māori and Pasifika willing to partake in this research initiative.

Potential candidates were telephoned to ask for their willingness to participate in the research. As our earlier survey results showed a slight under-representation of young Māori and Pasifika participants, deliberate attempts were made to identify more young Māori and Pasifika to participate in this second research phase. All participants were offered a $50 supermarket voucher for their participation.

The aim for these interviews was to explore and observe what identity information individuals are sharing and managing online, when, where and how they are doing this, and why. Each individual was also asked whether they have had any actual experience with forms of cybercrime or cyber-enabled crime, and if so, what their response had been. Each interview took between 40 and 80 minutes, depending on the variety of online activities in which each participant was engaged. Research participants chose their preferred interview location (e.g. their home, university, public library, Internet cafe, public space with Wifi). A place with Internet access was requested to give the researchers the opportunity to ask the participant, during the course of the interview, to demonstrate some examples of how they share and manage their identity information online in varying relationships. The aim was to correlate what people said they are doing online with what people actually do in sharing and managing their identity information online.

As preparation for the interview, each participant was asked to keep a diary of their online identity behaviour in the seven days prior to the interview, and to share this diary with the researchers during the interview meeting. The researchers focused on what types of personal information (e.g. name, email address, bank details) the participant shared and managed online and not the specific content. The interview guide and observation protocol are presented in Annex 2.

Human ethics approval for the research was obtained from the Victoria University Human Ethics Committee. Potential privacy risks were managed by asking each participant to show examples of how they share and manage identity information online and let them further explain why they do what they are doing. This gave participants the opportunity to show examples which they felt comfortable with sharing. Names and other identifying characteristics of participants were kept confidential.

The participant contributions from these interviews were later transcribed into narratives identified by pseudonyms. These narratives were then analysed for recurring themes and explanations of the motivations for particular online behaviours. The findings from these interviews are discussed in the relevant section of this report starting on p.20.

The interview findings were rich in their detail for the themes they yielded for understanding individual motivations and behaviours in managing identity information online. However they were limited in their generalisation by the context, general knowledge, preferences and dispositions of each individual. Therefore in the third phase of our research, we aimed to bring together groups of superficially similar individuals to explore findings from the survey and the interviews to build a more in-depth understanding of the different online behaviours of different age groups, ethnicities and other background factors, such as geographical location and education.

Focus Groups

Ten focus groups with 72 participants in total (6-8 participants per group) were convened from mid August to end October 2014. The selection criteria for participants were derived from the survey and interview data to enable us to further explore and understand the findings from these two earlier research phases. The following selection criteria were used for the recruitment of focus group participants: age, ethnicity, income, education and geographic location (urban/rural, North Island/South Island). Also, all our focus group participants needed to have at least some experience with Internet use.

Two groups represented particular age groups identified as demonstrating significantly different online behaviours in our phase one quantitative survey: seven people aged 65-75; and six students aged 18-24. We also convened mixed age groups by ethnicity: eight European/Pākehā; eight Māori; seven Pasifika people; and eight Asian people to enable us to further explore online behaviours which seem to be more specific to particular ethnicities. For all of these groups the people were located within a North Island urban area or in the case of the older group, a suburban satellite. We also convened a group of seven city-based business people and two groups of lower income people: one group of seven people in a minor provincial city and the other group of seven in an urban area. The tenth group of eight people with mixed demographic and ethnic backgrounds was based in a rural area of the South Island.

These groups were arranged by identifying an agent to locate suitable people to meet our selection criteria. Thus, we worked with Computers in Homes[4] networks in different geographic locations to form the two low income groups and SeniorNet to form the older age group. We worked with a rural school to convene the rural group; the university Marae to convene the Māori group; university networks to form the younger people/student group; a community-based Pasifika person to convene the Pasifika group and an Asian person to form the Asian group. A local Business Association and local government colleagues facilitated finding participants for the remaining two groups.

The discussion protocol developed for each focus group was varied to reflect the differences already noted from the survey and interviews for each of these focus groups (see Annex 3). Each focus group participant actively participated in a qualitative collective interview of around one and a half hours and, prior to this, also completed a survey with a sub set of the same core information that we had collected from the survey participants to allow some points of comparison between these small groups and the wider survey group segments. After an introduction to the research, we started each focus group by asking participants why they went online, what sort of activities they did, what identity information they shared, and what information they would not share, and for what reasons. They were also asked about any changes to their online behaviour over time and whether they have had any bad experience and if so, what influence that experience had on their behaviour. We then asked what they did to protect their online information and finally whether there were any ways in which they thought they could be helped to manage their online information better.

Caveat: The focus groups took place from 15 August through to 31 October 2014. During the earlier part of this period, New Zealand was preparing for a General Election for the Parliament of New Zealand to be held on 20th September. The 50th Parliament had its last sitting day on 31 August and the Parliament was then dissolved to let the election process get underway.

On the 13th of August, a well-known journalist and political commentator, Nicky Hager, released a book called '*Dirty Politics: How attack politics is poisoning New Zealand's political environment*'. According to One News' website "the book details the extent of political dealings between the [Prime Minister] Key administration and members of the right-wing blogosphere. Hager reveals that certain media events that appeared to be isolated instances of scandal were in fact part of a systematic effort by National to create political smears against their opponents." The book is based

[4] Computers in Homes is an initiative of the 2020 Communications Trust which receives support from government agencies, businesses and the community to increase digital literacy in low income and recent immigrant families.

on a set of emails which another anonymous source had hacked from the website of a political blogger Cameron Slater who publishes under the Blog name *Whale Oil.*

The book and its content attracted a great deal of media attention at its launch because of the nature of the claims. The heightened attention of the media to matters which might have bearing on the election outcome meant that one aspect or other of the contents of the book, the political implications of the book, or the ethics of hacking information from a personal computer was in the media every day between the launch of the book and the election. Several of our focus group participants made reference to these events either directly or indirectly and it appeared to be colouring views about online information security.

Analysis of results: spiralling approach of the research design

The analysis of the findings from the three phases reflects the spiralling approach of the research design. With results analysis of each phase, we drilled deeper into understanding the complex and context dependent relationship between individual identity information behaviours and the variety of online relationships they develop over time with commercial and government organisations, and with their friends and family. Thus the analysis of the individual interviews weaved these findings into what was gleaned from the online survey of 467 participants. In the analysis of the focus group results we delved deeper into these already noted and discovered further themes which help us understand Kiwis' online identity information behaviours and how these vary with age, ethnicity, education and Internet experience, and the nature and context of the online relationship.

Analysis of Individual Interviews

This section begins with a brief overview of our 23 interview participants. As described in the research design section (see p.16), they were selected to cover all the age and ethnicity segments used in our initial survey population (see Table 1 below). They all lived in one of the larger cities in New Zealand, or the suburban fringes of these cities. A pseudonym was given to each of the 23 interviewees to protect the personally identifiable nature of the data we collected and these pseudonyms are used throughout the following report of our findings.

Table 1: Age segments and ethnicities of interview participants

Age by Ethnicity	**18-24**	**25-34**	**35-44**	**45-54**	**55-64**	**65-74**	**>75**
Māori	*Bono*				*Rewi*	*Tamati*	
Pasifika	*Leila*		*Tracy*	*Louise*			
Asian	*Judith*	*Andrew* *Harry*		*Candice* *Portia*			
Pākehā/ European	*Angela*	*Anton* *David* *Karen* *Nancy* *Paul*	*Catherine* *Chris*	*Emma*	*Roberta*		*Claudia* *Jack*

The interview participants varied in their income level but all bar four had some post school education (see Table 2).

Table 2: Income and education level of interview participants

Education by Income	**No response**	**No education**	**Primary only**	**3 years secondary**	**4 years secondary**	**5 years secondary**	**Some tertiary**
No answer					*Tamati*		*Roberta* *Nancy* *Rewi* *Portia* *Harry*
No income	*Andrew*						
$1-10k						*Leila*	*Paul* *Judith*
$10-20k							
$20-30k					*Catherine*		

$30-50k						*Bono*	*Jack* *Angela* *Claudia*
$50-70k						*Anton*	*Kate* *Tracy* *Louise*
$70-100k							*Candice* *Chris* *David*
$100-150k							*Emma*
$150k+							

In addition to the age and ethnicity profile of our interview participants we begin the presentation of our interview analysis with a brief thumbnail description of each of the interviewees. Following this introduction we have identified a number of themes in the interview narratives. These are illustrated wherever possible with direct quotes from what these people said. In cases where the description was less pithy, summaries of what was said are used to illustrate the findings. The themes we have identified below should be read as adding another level of detail to our understanding of people's online behaviours reported through the survey, by revealing more about the thinking and motivation guiding people's online behaviours.

Thumbnails of interview participants

The following sketches are presented in order of age segments from youngest to oldest.

Bono
Bono uses his smart phone to do just about everything. It is never out of his hands. He looks up information he needs, catches up with the latest news or the activities of his friends, plans his social life, and arranges his finances. He also has a computer at work and at home but his phone is his preferred device. He is always logged into his email account and his social media accounts and his 3G roaming is turned on so that he can receive emails and messages immediately all day. He likes to leave comments on blogs and news stories and *"gets a kick out of people agreeing"* with him. He has three different email accounts he uses for specific purposes like email, banking or purchasing online, and multiple passwords which he commits to memory. He uses public Wifi when it is available and thinks it is safe because he is "*pretty quick*". He uses a banking App on his phone to check his account and transfer funds, buy things and make bookings.

Leila
Leila uses her smart phone all the time, even downloading reading and assignments she needs for her university work onto her phone. Her phone accompanies her everywhere, except when she had to work for income at the weekends. She uses her phone to message friends and find out what they are doing, arrange her social life, look up information she is interested in like animals and music. She uses public Wifi when nothing else is available because she has limited funds to pay for data roaming. She uses a banking App on her phone to check her credit.

Judith
Judith mainly uses a tablet and a smart phone although she also has a desktop computer at home and at university where she is studying. She reads news on her desktop and phone and uses her tablet to participate in a number of social media sites, such as Instagram, Facebook and Linkedin, seeks entertainment online (e.g. YouTube), and plays online games. She buys things online, checks her bank account and applied for her student loan on her tablet. She trusts the shared university computers and network but is careful to log-off when finished. She has three email accounts which she uses selectively.

Angela
Angela prefers her laptop to go online although she does have a tablet. She does not have a smart phone which she acknowledges made her a bit of an oddity among her friends. She uses her social media accounts to stay in touch with known friends and takes care to limit what she posts to friends only. She seeks out entertainment and news online and an Internet search is her first choice for finding out information. She has only one email account but uses a different password for different uses. She has taken part in online surveys and transacts with government online (her tax and her Census form), but does not make purchases online because she does not trust herself to manage the temptation of spending more money than she has. For the same reason, she does not have a credit card.

Paul
Paul has a desktop computer, tablet and smart phone to access the Internet for home and study at polytechnic where he is doing a degree in computer science. Because he is on the go between polytechnic and home he prefers his smart phone for banking, mostly because of the convenience. He plays games online with Xbox, uses Facebook and watches videos online, but because of his study does not have much time for this. His limited income restricts what he buys online. He does not share photos or other information publicly on his social media accounts and generally tries to keep personal information "*fairly private*".

Andrew
Andrew has a laptop, tablet, smart phone and desktop he uses at home and university to go online. He finds his phone the most flexible device and uses it for all non-work and non-university purposes, such as keeping in touch with a network of known friends through social media sites, watching videos and playing games. He makes purchases online and uses the location-finder App on his phone to locate businesses he needs, such as food when in an unfamiliar place, or find his friends to meet up. He has one email account and multiple passwords of varying complexity, which he uses for different purposes: more complex passwords for services like banking, and more simple passwords for instances where he considers less need for security of his information.

Harry
Harry is a full-time student studying information systems and an enthusiastic early adopter of the Internet. He uses a smart phone, tablet, laptop, as well as university and home desktop computers to access the Internet. His smart phone is his preferred device for secure transactions, because Harry believes this to be his most secure device: he is the only one who uses it, it is password protected and it is with him all the time. While he is still an everyday heavy Internet user, he has become more guarded about the personal information he puts online over time as he learns and understands more as part of his studies and also based on his experiences and those of his friends (e.g. stolen identity information). He now only puts information online he is happy to be public, is very selective about the sites he uses, and takes steps to delete his Internet use history and cookies. He goes online to read emails, keep up with family and friends, search information, and do banking. When he has time it is also where he goes to buy things.

Anton
Anton is self-employed and makes little distinction between his work-related and private uses of the Internet. He uses a laptop and, more recently, a smart phone but does not consider himself very computer literate. He is very active on the Internet with his activities concentrated on checking emails, using Facebook, looking for directions when travelling, reading articles about his hobby, occasionally posting a comment online under a pseudonym, and watching YouTube clips. He also makes online purchases, although he tries to avoid making online payments, preferring to make bank account transfers instead. He also does his business banking and tax online. He has not had any bad experiences online.

David
David uses his smart phone and laptop to access the Internet for personal use and work. He maintains a large network of online 'friends' many of whom he has not met. He embarked on this path for semi-professional interest reasons but now regrets that he has been so open, especially since experiencing one of his online friends having their identity details stolen and used fraudulently. He spends his day using the Internet to do searches for information related to his work so his at - home use is limited to checking news updates, making bookings or purchases. He generally prefers secure Wifi to do transactions, especially banking or any transaction involving transfer of personal data, but uses public Wifi for looking up news, travel routes or event details.

Karen
Karen is a 24/7 user of the Internet, mainly on her smart phone although she also has a tablet and home desktop. She uses email and social media accounts to interact with family and friends and keeps up with a number of blogs and news sites for information about the world and travel, although she never comments, more from lack of interest than any aversion. Because she is planning to travel overseas, she has shared a personal profile of herself online to help her arrange her travel accommodation. She also does banking, books events and purchases goods and services online and transacts with government, such as for her taxes, student loan and paying for motorway tolls. She has experienced someone she knew stealing some of her identity information and using it online as a joke on a dating site, and consequently is very wary of such sites.

Nancy
At home Nancy prefers her tablet and smart phone to access the Internet although she also has a laptop for work and home. Because she has recently had a baby and is on maternity leave, she has time for using the Internet every day: for shopping, finding information, entering online competitions, and looking at videos. She also uses the Internet to do her banking and government transactions, such as her tax, and has a Real Me account. Looking for things she needs for the baby has increased the amount of shopping she does online because it is so convenient and, based on experience, she has become more relaxed about providing her 'real' identity information to the sites she uses. She is happy to have her personal profile information used by trusted brands to target information to her. She uses encrypted Wifi, a firewall and antivirus software on the devices she uses at home and she shares personal information such as photos with known friends and family.

Tracey
Tracey mostly uses her laptop for Internet access but she also has a tablet device and a smart phone. She has a work and private email account, which she checks frequently as well as keeping up with family and friends on Facebook. She uses the Internet as a first port of call to find information she wants and seeks entertainment online from YouTube. She also has a Linkedin profile, uses Internet banking and does her tax return online. Her online purchasing is limited to purchasing tickets from organisations she trusts because she worries about the security of some sites. She has experienced somebody else using her personal information to create a fake online identity for her, which created much nuisance in her work and professional life and was hard to shut down. She wants to have an online identity for personal and professional reasons but worries about how to know if her information is secure.

Catherine
Catherine has only a home laptop to go on the Internet. She has signed up to Facebook and has an email account for staying in touch with family and friends. She admits that she does not understand how to use the Internet, so she relies on her daughter to help her to keep her Facebook settings private and provide guidance on what she should and should not do. She has purchased the odd thing through TradeMe but she likes to buy from a local vendor so that she can view the goods and pay in person rather than over the Internet. Although she trusts banks, she does not do online banking: she does not think she knows enough but would be open to learning as it seems convenient. She is similarly open to other services online if she knew more.

Chris
Chris is new to New Zealand and Internet use. He has a laptop at home for Internet access and uses it nightly to keep in touch with family and friends overseas. He also does online banking, finds and orders books online from his local library and does some online shopping: mainly goods or services where quality is more reliable, such as books, CDs, tickets for shows or travel. He limits his online transactions to reputable, known companies and seeks advice from others before shopping anywhere new. It is convenience of these online services that most attracts him. He does most government transactions offline but is open to online options in the future.

Louise
Louise has no Internet connection or computer at home, mainly for cost reasons and fears about managing the security of her teenage son's online activities. She uses her work computer after hours for personal online activities, such as keeping in touch with family through a social media account, doing online banking because of the convenience, and keeping up with news. She also uses YouTube or a search engine like Google to look for information to support her hobbies and community activities. She tries not to provide information about herself in online interactions, unless required to get a service she wants.

Candice
Candice has a tablet, laptop, smart phone and a work desktop for Internet access. She uses them every day to read news, look at online versions of newspapers and magazines provided through her public library, and stay in touch with family and friends through her social media account, which she has limited to her known circle of friends. She does online banking, purchases goods online and does government transactions online "*because it is so convenient*". She looks around to compare prices when she is intending to purchase something online, but is choosy about the sites she will actually transact with and looks for evidence of their location, security and reliability of service, such as the use of Paypal, or reviews from other customers. She has five or six email accounts and separate passwords for different online activities, and she chooses which email account to use and the strength of the password according to her risk assessment of the online transaction. Her home network is protected by a firewall and antivirus software, which she updates regularly.

Portia
Portia has a laptop she uses to go online and watch news and television series in her home language as well as keep up with family and friends overseas. Because the Internet is the main way Portia can hear and speak her home language and keep in touch with her former home, she uses a lot of data in these activities. To manage the cost she limits herself to 80GB per month, which she easily exhausts. She does not have a smart phone but is thinking she might need one to be able to follow her friends who are now using a smart phone App rather than Facebook to stay in touch. She is enrolled for online banking but only checks her balance, because her bills are mostly paid by automatic payments. Her son acts as her Internet adviser and maintains the firewall and antivirus software on her laptop, as she confesses to "*not know much about the Internet*."

Emma
Emma has a laptop at home and a PC at work to access the Internet. She has decided against a smart phone because she does not want 24/7 intrusion of email and other Internet uses into her life. She does online banking three to four times a week, does her tax online, buys tickets online and watches a video online now and again with her children. She does not do online transactions with sites based overseas and checks the authenticity of sites she does use as well as their payment process. She finds her Linkedin profile useful for work but is generally very careful about what information she provides and to which sites. She has not had any bad Internet experience other than spam emails and tries to avoid "*things like popups*" which may generate spam email in her view.

Rewi

Rewi is an IT professional who uses a wide range of devices, such as laptops, desktop PCs, tablets and smart phones, to access the Internet for work and personal use. He uses email and social media accounts to keep in touch with family and watches videos on his tablet. He also does his tax online using a RealMe account to identify himself, does internet banking, and pays his bills online. He has made online purchases but is more cautious now after suspecting that his bank account data might have been stolen and misused. Because of his work, he is conscious of how exposed the devices can be to viruses and malware, even with up-to-date software, how insecure personal information can be online, and how reliant the user is on the actions and policies of the sites they use. He has more than one email account and uses proxy user accounts all the time.

Roberta
Roberta is a self-employed professional working from home. She mostly uses her PC for Internet access. She also has a smart phone and a tablet device she uses when travelling. She sends and receives emails, and keeps up-to-date with online news, weather information, and information about travel. She is not a big fan of shopping online because she had her credit card details stolen in the past, but does buy online through a small number of trusted vendors. She shares her personal details when conducting online government transactions, such as income and GST tax returns, registering with Travel Safe before travelling overseas, paying fines and stopping mail. She has a reasonably high level of trust in government services online. She is quite protective of her online privacy, so she tries not to give out any identity information, does not have any social media accounts, and has not used her real name in her email account name.

Tamati
Tamati has retired from fulltime work but is still active in community-based activities and at director-level in voluntary organisations. He uses a laptop and a desktop PC for communicating with friends and family, and for finding information he needs or to inform his interests. He does online banking and has made purchases over the Internet, such as e-books. He has recently begun to also use an e-reader and a tablet device. He does not have any social media accounts and does not seek entertainment online. He prefers to use face-to-face channels to pay bills and for accessing other services. He has a fairly relaxed attitude to providing personal information online because he has had a national media profile and considers much of his personal information to be already publicly available.

Claudia
Claudia uses a desktop computer to access the Internet daily at home. She sees it as an invaluable tool for her community work and hobbies. She also uses a shared tablet device as part of a community watch patrol to transmit photographs and messages to authorities via the Internet. She gets help with maintaining the security of her computer from technical services she purchases and she does online banking and filing of tax returns online. She participates in online consultations in her local community but often obscures some part of her real identity information, such as her address or date of birth. She has had two bad experiences with buying and selling online and has decided not to try this again.

Jack
Jack is retired from work and uses a laptop and tablet to go online to search for information around his hobbies and interests, and to stay in touch with family and friends through email. He does online banking and purchases tickets and subscriptions online. He is unimpressed and uninterested in social media or online entertainment, and fails to see the attraction others see in it, preferring the offline way of doing these things. His son is more knowledgeable about the Internet and devices than Jack, and acts as his technical adviser. Jack limits what he does online to the areas where he feels safe.

Interview findings

A public space

All the participants viewed the Internet as a public space and considered all of their Internet communications potentially discoverable.

> *"Everything you do on the Internet is visible to somebody with the right tools." [Chris]*

Some were also aware of the discoverability of an online presence. One mentioned the data trace left by the IP address of the device used, even if no other information is overtly exchanged.

> *"Sometimes they have this 'ActiveX' filter thing you can click on and I worry whether it can then access my Internet number thingy, my IP address." [Tracey]*

While participants acknowledged the huge diversity and range of information and services offered by the Internet, even experienced high-end users tended to make a limited every-day selection.

> *"I don't visit a lot of websites – just a few news sites like Stuff and Reddit, a search engine like Google." [Bono]*

Privacy awareness

All the participants we interviewed were cognisant that using the Internet involved exchanges of some personal information and that this information could be available to others.

> *"At the end of the day [not storing usernames and passwords] is the safest way to go, because it's the Internet, and who knows who is looking at it." [Bono]*

For most, this awareness of publicness of the Internet translated to an awareness of privacy and consideration of how much information an individual might provide in certain circumstances. There were a variety of different views about which information, in which range of exchanges, an individual considered private. An email address was seen by most as the minimum requirement for an online transaction and therefore seen as an implicit consequence of working online. A typical response was to provide the minimum information possible.

> *"I tend to give them the minimum information I have to. Some of them will have the red asterisk indicating this is the information you have to give. Some of them ask for age and occupation and I tend to avoid giving them information I don't have to. Most of them have a minimum of name, telephone number and address. I am reasonably happy to give that." [Chris]*
>
> *"I am not known as a blogger. If I am going to share stuff, I share it privately. I wouldn't share it out with the general public – because of security…. I am well aware about what to share or not share…. I might share age, but I don't share date of birth. I don't share my cell phone number across Facebook because I think that is inappropriate but I do share it with my friends so they can text me on it. I don't usually share my email out unless it is requested specifically. Mostly I wouldn't share much personal information at all. First name, last name, age is OK, and maybe an address if I want something delivered." [Peter]*

Some older users had also adopted the strategy of keeping their real identity information private by changing some personal identity information.

> When Claudia does online surveys, she does not necessarily provide accurate personal information for all questions, for example she might put "*any old number*" for income or she might not provide occupation, because she is aware that "*someone could steal my identity*."[Claudia]

Or not providing personal information at all:

> Jack does not provide information to websites he visits: *"I wouldn't hesitate to cancel out of them if they asked for it. I like to be in control of where my information goes*." *[Jack]*

Views about the privacy of other information, such as location information, date of birth, and age was much more variable and context specific. For example, participants would provide information they considered private to a trusted site.

> *"It depends on who I am providing the information to. If it is a government department, or an organisation I trust, then I will provide things like date of birth, address. I would only give my IRD number to IRD." [Tracey]*

Some participants were aware of their dependence on a site's privacy policy and settings and remained vigilant in respect of some sites, such as Facebook.

> Leila checks her privacy settings about once a month to see if they are what she wants*, "because I thought that I was really private and then I found that I was public.… So I changed my settings and changed my name so that you couldn't search on my name and find me." [Leila]*
>
> *"My Facebook page is generally very restricted all of the time. Last year I did upload about 130 photos from a camp I attended. Most of them were fairly reasonable and only my friends could see them. Generally I don't share photos publicly. I wouldn't show any dodgy photos to anyone. If someone tries to tag a photo of me I just un-tag it and get rid of it."[Peter]*
>
> *"Unfortunately, the way Facebook is configured you are exposed. We have tended to use the default privacy settings, but every now and again I get so annoyed with it I will go in and cut the options down a bit. But it is such a changing beastie, it's very frustrating, because they are changing the settings all the time." [Rewi]*

Only a few have actually read the privacy statements provided by a site. Most tended to 'tick the box' if that was a requirement for proceeding with a transaction.

> *"Life is too short to read all that stuff" [Bono]*
>
> *"I read them, but I can't say that I always understand them. If it looks pretty standard, I just tick the box. If it was something weird or different, then maybe I'd call them to find out." [Candice]*
>
> *"It ends up being a bit of a reflex to tick 'yes I agree'." [David]*
>
> *"Never read privacy policies that pop up on websites." [Tamati]*

Other, largely younger users, falsified some personal information to protect their privacy.

> Angela's Hotmail username and email address contains her real name but she might change other information such as date of birth. If she doesn't think it is a necessary thing for whichever site to know then she does not provide the real information. When it is important that the information is accurate, such as in Government transaction, then *"of course I provide the real information."* In other instances, such as when making comments, Angela might further obscure her real identity by using her less personally identifiable email username and by providing some inaccurate information like name or age. She would not share her passport number, health information or citizenship status. *[Angela]*
>
> When Harry transacts with other services, such as Facebook, or purchasing from Amazon, he chooses to use a different email account and not to provide fully accurate personal identity information; he might change his birth year, name or some other identifying information. *"By being selective about the 'real me' information I give, I can get the services I want and ensure that the profile created works for the services I want, while also protecting my real identity information." [Harry]*

Mainly younger interviewees had location finders on their mobile devices but they tended to be deliberate and selective about when and under what circumstances they would use this function.

> Andrew allows his mobile phone to use his current location information, for instance to find his friends while he is on WeChat or find some service he is seeking, but he does not leave it on all the time and would definitely turn it off if he was travelling out of town. *[Andrew]*

Online identity

Individuals varied in their approach to online identity. At one end of the spectrum, experienced users sometimes chose to operate anonymously and also had multiple online identities using selective aspects of their real identity and pseudonymous elements. These users tended to be younger, better educated, and technically very well informed.

At the other extreme, individual users made little distinction between their online and off-line identity. They used their real name online and provided accurate information about themselves, if they decided to provide it at all. These users tended to be relatively inexperienced Internet users, older, or less well educated and unfamiliar with how the Internet operates.

> Jack has only one email account which uses his first and second names…. He does not have any social media accounts: "*I cannot see any sense in Facebook. People complain about their loss of privacy but at the same time they belong to those types of things. That doesn't make sense to me."* [Jack]

Online identity behaviours change over time

Identity behaviour was not a constant. It changed according to the transaction and it changed over time. Participants told us that they have changed their online behaviour as a result of what they have learned about the online environment over time.

> *"I don't put photographs on Facebook anymore. When I was in high school I did but now I don't like putting my information out there. My Facebook profile is really private, so if you are not a friend then you can't see anything." [Justine]*

Participants in their twenties and early thirties, particularly high Internet users and enthusiastic early adopters of online services, described how their behaviour today differs from an earlier, less careful behaviour. They are now more privacy aware, less likely to share information with an unknown audience, more likely to make use of a pseudonym or other non-real information, more deliberate in their use of privacy settings on social media, more considered in whether or not they will provide information under particular circumstances, and more deliberate about the devices they use, the security settings of their chosen device and the websites they will go to or transact with.

> *"I began to think, do I really want everyone in the world able to see my [Facebook] profile?"* They were initially set to the default of everything public but Tracy has now tightened this, first to 'friends of friends' and now 'friends' only. *[Tracey]*

They made judgements about which Internet connections and sites they might use with confidence about their security, and adapted their behaviours accordingly. Some remained sceptical about whether anything can be secure:

> *"I tend to believe the security specialists who say that there are two types of organisations: those that admit that they have been hacked and those that don't know they have been hacked." [Emma]*

Others tended to adapt their online behaviour according to their own experiences and what they learnt from the news media, friends and other sources over time.

> Having experienced unsolicited emails offering new services which he now surmises were sent because of information he had unwittingly provided as part of online shopping, Harry has become more savvy about how to protect himself. For instance, Harry would only post a photo or other information on Facebook if he was happy for it to be public, and he actively uses his privacy settings to limit information to 'friends' or 'friends of friends'. *[Harry]*

Some participants described a relaxation in their behaviour over time as they gradually reassessed their security fears in the light of their experience of specific, convenient, or repeated uses, such as purchasing items from a particular known or trusted site or online banking, and also learned from the experiences of their friends and family members.

> Nancy explained that in the past she might have used a false name and a more anonymous address such as her father's work address for her online purchases, whereas *"I am now more relaxed, or perhaps it's lazy",* and she usually provides her real, name and address for online purchases and competitions she enters. *"At first there were only a few things where I would provide a real name and address, and gradually it has become more universal. There might be the odd occasion that I still get things sent to another address but it's now more for convenience, like if I am not going to be home, not for security reasons." [Nancy]*

Life course changes (e.g. parenting, retirement and travel) also lead to changing perceptions about the desirability of using online services and a reassessment of the balance in perspectives on information security and privacy.

> Kate has joined Couchsurfing because she is intending to go travelling and would like to meet and stay with people through Couchsurfing so has updated her profile. While she would not generally give out information about herself like her friends, hobbies and likes/dislikes, she sees this venture as requiring her to put a little more information about herself 'out there' in order to gain advantages from Couchsurfing. She has checked out the site's safety policy and talked with other people she knows who have used the site to check out its reputation. *"I haven't put where I work but I have provided more information about myself because I know I will get more profile views, and what you say is verified by people who know you." [Kate]*

> *"Before the baby, I hardly ever shopped online, but it is so much easier to find baby things and there are not the problems with fit there might be with adult clothes."[Nancy]*

> *"There are about three different versions [of instant messaging Apps] and each son favours a different one to send messages and photos…. I introduced my sons to this stuff and now they have gone on and surpassed me. They are always going on about 'dad, you shouldn't do that or use this'. They are probably even more careful and paranoid about putting their private information out there." [Rewi]*

Bad online experience

Fourteen of the interviewees described bad or unsettling experiences in the course of using online services which had led to changes in their online behaviour. These experiences ranged from being duped by a bogus email or social media account, having a personal email account used by others or having the financial aspects of a transaction turn out badly for them. The latter included matters that apply equally in the off-line world, such as instances of mismatches between the user's expectations and experience.

> *"The first I knew of this is that my 'friend' emailed me asking me for money. That was when I knew it wasn't my friend. It also made me think because everything on my friend's page was*

> *public. She uploaded so many photos, it would be easy to make a profile of her, so I wasn't really surprised…. We went away on holiday and she put photos of everything up … and I made her take them all down. She has so many people as Facebook friends that she doesn't know and I just don't want them seeing our photos of where we stayed and my family's house and all that sort of thing. It's like someone walks into your house and is looking around. It freaks me out and it is unnecessary." [Leila]*
>
> *"The time it happened, an email message appeared saying this person was being held hostage or something like that. In retrospect I don't know why I replied saying something like 'that's unusual'. Then I got the follow up – 'you need to wire me money'. I just ignored it after that. Another time, I accepted a friend request from someone I was already friends with. I did it on my phone without thinking and then I immediately removed them because it was apparent that was a bogus account. There was an opportunity there, had I not acted quickly to remove them, they could have gone to my friends list and so it would have gone on. I like to consider that I am reasonably savvy and yet I still did that without thinking! It is part of the risk of the App, because apart from putting the passcode into your phone, you are always logged in. So you can go there quite easily and be quite flippant. It is also why I don't use the banking App so much because I believe that I could be flippant and accidentally move a large sum somewhere I don't intend to."[David]*
>
> *"The last time Telecom had a problem, the first I knew about it was one of my friends said 'why did you send me that', and I didn't." [Candice]*
>
> Karen has had someone pretend to be her by posting information and an image (just her eyes) on a dating site. The information was posted by a friend who later confessed what he had done it as a joke but *"there were so many responses and some of them were disgusting. That is the problem with dating sites." [Karen]*
>
> *I am not a great fan of shopping online because I had a credit card hacked a couple of years ago." [Roberta]*

Maturing online behaviours

Internet banking was the one service most commonly used across all of our participants (22 out of 23). Participants said that they were encouraged to take up online banking by their bank and were coached by the bank in the steps needed to enrol and protect the security of information (such as a unique, strong password).

> *"I went into the Branch one day, and they suggested Internet banking and set me up with a little thing that said use this to set it up. So I went back to the office and set it up and ever since I have used it. It is just so simple. I can do it at any time of the day and I do text banking with another bank as well. "* Paying bills online *"is very handy." [Louise]*

As a result, participants had a set of mature behaviours they used for these transactions. This meant they used strong passwords, did not reveal them to others and changed them more often.

> David tries to have a strong password for banking with a combination of letters and numbers but admits he does not change it very often*. "At work we have to change our password, it seems every five minutes, and I am constantly at risk of forgetting what my current password is."* He uses a similarly strong password for all his other serious accounts. *[David]*
>
> Nancy has a RealMe log in, does her tax online and checks her student loan online. She has registered her car, paid Council rates and also ordered books from her local library catalogue online*. "I generally do any of those transactions where you have to pay for stuff online because it is just so much easier."[Nancy]*

The same participants also regularly 'unsubscribed' from unwanted emails and sites to eliminate the potential risk these might present.

> *"You know how sometimes when you buy something in the shop and they sign you up to a newsletter – I try to get rid of all of those."[David]*

Several participants also had considered the security of the devices they use, including the requirement for secure connection and encrypted Wifi rather than public Wifi, and the location of the devices on which they transacted online.

> *"I use my iPhone a lot because I find it is quite a convenient device, and I have the touch ID on it, which is more secure than a password*." [Candice]
>
> Bono uses his phone to do online banking and pay bills but he is selective about where he does that. He would not use a public Wifi or do it on the bus, but he would definitely for example do his banking in a public place using his 3G: *"I am pretty quick. I just get in there, do the transaction I want then sign out. I am only about 20 seconds and I check that there is no one around me." [Bono]*
>
> Harry limits his online banking, and other activities requiring the use of personal information, to his smart phone because he reasons it has more layers of security. He said he would never connect to these services through a public network preferring instead to use the 3G network on his phone or his home network*. [Harry]*
>
> *"When I first got my own bank account when I was at college I was introduced to phone banking and then I realised it was easier if I just did Internet banking. So I downloaded the App and it just automatically does it for me although I do have to re-sign each time. It just makes life so much easier. Like there is Wifi all over central Wellington, so if I don't have data I can just stand out on the street and use it. I usually do it at uni or before I come into uni at home and it's just one time I have used the CBD Free network…. I realise that it's probably not that good because other people can 'see' if they know how to hack into other people's devices. That is why I have only done Internet banking on the CBD Free once. The same probably applies to uni as well but as I haven't got very much money in my account it probably doesn't matter that much!" [Leila]*
>
> *"Most of the time when I need to do banking I am usually away from the computer at home, so I use it when I am on the go, to check how much I have or what I need to pay." [Paul]*

Many participants who used online banking regarded it as a high benchmark against which to measure other online services and experiences.

> Tamati does online banking and is open to doing transactions with government online: *"You learn new things all the time, and we would if they said that is the way we gotta go." [Tamati]*

For some who did not use Internet banking encouragement and training might lead to a change in behaviour.

> *"I don't do internet banking because I am not up with it, I don't know what I am doing…. It's not that I don't trust the banks. If I had someone show me I might think about doing that." [Catherine]*

Security awareness

Security of Internet transactions was referred to in some respect by all the interviewees. Awareness of security translated to particular behaviours, such as using multiple passwords, selectivity about security of particular email accounts, location of the user (e.g. home or public), and security of the Internet connection used for particular transactions (e.g. preference for encrypted WiFi). Home Internet connections tended to be password protected and anti-virus software was installed on devices.

Most chose to do online banking transactions only on a personal computer or device they trusted, eschewed public computers for that purpose and did not use public Wifi connections.

> Angela was thinking about whether to take her laptop when she travels to Europe next year. She is weighing the risk of doing that with the risk of using public computers to do sensitive transactions like online banking. *[Angela]*

Many participants had created a pseudonymous email account which they used for all transactions they thought might be less secure.

> Bono has three email accounts: one primary one he uses for most private purposes, a work one, and one he uses when visiting a site he is only going to use once or occasionally and he does not want to use his main private address, e.g. when a site demands an email just to allow you to proceed to get some information. His private email obscures his real identity by not containing his full name. He has two or three passwords he uses for most things; one he reserves for online banking. He keeps his passwords in his head and uses a basic idea to generate them like some numbers and a "*tough word that no one else would ever think of*". [Bono]
>
> Candice has five or six email accounts which she uses for different purposes. Only one or two of these contain information linked to her real identity, such as her name in some form, and these email accounts are reserved for trusted business such as banking or transactions with government. Email accounts containing no information linked to the real Candice are used in instances where an email is required, but there is no reason that the information needs to be accurate. "*When I am asked for an email address from a website I provide one of those email addresses that don't matter and they can't identify me*." [Candice]
>
> "*But let's say I am going into Expedia and just need an Expedia profile, I will use a password that is quite separate from passwords for purposes I consider are more important in terms of security, like banking and things like that."* [David]

Many participants were also quite conservative in their use of the email account they used for transactions they wanted to be secure, such as banking and government services.

> *"I would not use my uni email for stuff other than work because I don't think that is the right thing to do, and I keep my personal email pretty tight. If I have to give an email address and I feel they are just going to send me a whole pile of stuff I don't want, then I use my 'spam' email account." [Judith]*
>
> Louise has three email accounts. As well as her official work one she has a private Gmail account and another she uses for work when she is offshore. All have separate passwords. She uses words from her home language as part of her password "*which makes it a bit less likely that someone might guess it or hack it. I make it something I am connected to so that it is easier to remember that way." [Louise]*

Deliberate strategies to manage privacy and security of transactions

Participants described why different devices are preferred for different tasks. They took into account security and often usability. Six of the 23 participants (David, Leila. Judith, Nancy, Paul, Rewi) used RealMe to facilitate transfer of identity information with government agencies securely.

> Rewi has registered with Real Me and he does his tax and business requirements online. He and his wife try to do as many other government registration processes as possible online, e.g. registering a car, travelling on the tunnel going north. "*It's quick and efficient. It means you don't have to spend money on gas driving to the Post Office to do things, so we do as much of that online as we can because most of those are government sites and you would expect the security to be pretty good." [Rewi]*
>
> David does online banking quite frequently. He has an App for Internet banking but he prefers to log in using the Web address*: "I don't really like using the App to make transfers because online I can see that the right amount has been transferred to the right place." [David]*
>
> Harry has taken to cleansing the cookies from his computer daily to make it less likely that a profile of his activities could be built. He also keeps his ear to the ground for information about Apps that might be a risk. He has never used 'Angry Birds' or 'WhatsApp' because of things he had read about how they could compromise his security. All the Apps Harry uses are on his cell phone because it then stores his username and password. "*Every time you enter a username and password there is a risk of someone stealing them, so I tend to use my cell phone for Twitter or Facebook so that I don't have to log in every time, rather than my computer.*" Harry said he was even more wary about shared public computers because the previous user might have visited websites or downloaded software that has compromised the computer. *[Harry]*
>
> *"When I provide the information online, I double-check before hitting the submit button. Whereas when someone else is doing the data entry, poor handwriting and keying errors can lead to errors. If I do the transaction face-to-face, the information is still going to end up in a database somewhere but because of transcription errors, it might not be accurate." [Harry]*

Online experience and competence

In the main, the most experienced Internet users were younger, IT savvy, more educated, or Asian. Their default environment was online: a smart phone provided them with 24/7 connectedness. A few "*can't live without the Internet.*" For these users, the Internet was the first place of reference for every information and service need. They shopped online, ordered food online, organised their social lives online, caught up with existing friends online and met new friends online.

Older people by contrast said they trusted the offline world more. They were more 'digital by exception' and were only gradually induced into the online world through the urging of family and friends (e.g. joining Facebook), the desire to access the wealth of online information to advance interests and hobbies, or the ease of doing something time consuming (e.g. online banking, bill paying, purchasing tickets, buying goods where the quality and fitness for purpose is not likely to be an issue, such as books).

> Jack is cautious in what he does online. He does Internet banking, and has a high level of trust in his bank transactions. He also makes a few purchases from trusted sources, such as movie tickets, New Zealand wines and pays for a few subscriptions such as Chamber Music New Zealand using a low balance debit card so as to limit his financial exposure. *[Jack]*

We noted different behaviours between experienced and better educated users and those less experienced and less educated about the Internet: the more experienced, the more likely the individual was to obscure aspects of their 'real' identity (e.g. use multiple email accounts and passwords, use pseudonyms, provide fake information, and delete cookies and browsing history regularly).

> *I usually give a false date of birth. If it is not that serious, I make up the details – actually, a lot of the times. If I put a phone number in it is just random numbers. So it might be just my name and the rest of the details are made up. [Leila]*
>
> Harry actually has three email accounts and he limits one of these to his more trusted friends and more trusted transactions, such as applying for a passport online. He guards this account closely and changes the password regularly. There are lots of other transactions where he is also required to provide an email address, for example, so he can post an online comment. But he reasons, based on his experience that he does not need to provide access to all of his personal identity information in these instances. *"If they ask for your birthday, it doesn't matter whether its 1980 or 1981; it doesn't matter whether you say you are male or female. It is not illegal. If you were doing that transaction face-to face you wouldn't be asked to provide that information so I don't feel obligated to provide it online."* Instead he will use one of his other email accounts. His reasoning is that should a hacker get access to his email account through what Harry regards as less secure sites, they can reconstruct an identity profile for the user. By limiting the identity and private information such as bank account numbers associated with a particular username or email address, Harry believes that he is limiting his exposure, and he will be less concerned if he receives spam mail to those alternate addresses. *[Harry]*

Less experienced and older participants more commonly used their 'real identity' as their default setting.

For most participants, online communication was a means to an end (e.g. staying in touch with friends and family).

> *"I am never passionate or interested enough to make a comment online. I would rather strike up a conversation face-to-face!"[Karen]*

For most participants, online 'friends' were almost exclusively people they knew in the off-line world. David was an exception in this regard and he regretted his earlier openness.

For some of the younger participants [Bono, Karen, Nancy. Angela, Andrew, Leila], online communication extended and continued face-to-face communication to 24/7 connectedness.

> *A lot of the time my friends and I won't have credit. So we message each other to meet up. And it is easier with a group message on Facebook. [Leila]*

A few of the participants had created messages or content other than photos for public audiences they did not know. For four younger participants, commenting on blogs or news site posts was seen as a way of sharing and communicating their ideas more widely and putting themselves 'out there':

> "*A place to demonstrate who I am and what I can do or what I have to say…. I get a kick out of people agreeing with me."[Bono]*

The less experienced and educated relied on others with more experience and knowledge to instruct them, take care of settings or give them rubrics to operate by.

> *"I rely on my daughter to do some things, like I got sent a jpg the other day and I didn't know what that was so I had to ask her to help me with it….I've been told to have different passwords, so I have…. And if I don't know the email sender, I don't open it." [Catherine]*

Personal experience with cyber-enabled crime

Across the participants, several described incidents of attempted or actual cyber-enabled crime such as:

Password security breach, with email account password being compromised.

> *"My original Hotmail account which I had when I was doing a business course got hacked but I closed that down and killed it. I thought, well that's been hacked so I will close it down and start a fresh account."[Paul]*

Stolen identity: individuals' identity information, such as name, phone number, place of work, or photo was used to create a false online identity, which others were misled to believe is the real individual concerned. Examples include a partial photo of Karen, posted without her knowledge on an online dating site; an email account created in Tracey's name and used to send annoying emails to her work colleagues and create an online profile that could be linked to her and affect her professional reputation.

Victims of other's stolen identity: presented with a 'friend' request by the user of a stolen identity purporting to be a known friend.

> *"The first I knew of this is that my 'friend' emailed me asking me for money. That was when I knew it wasn't my friend." [Leila]*

> *"The time it happened, an email message appeared saying this person was being held hostage or something like that. In retrospect I don't know why I replied saying something like 'that's unusual'. Then I got the follow up – 'you need to wire me money'. I just ignored it after that. Another time, I accepted a friend request from someone I was already friends with. I did it on my phone without thinking and then I immediately removed them because it was apparent that was a bogus account. There was an opportunity there, had I not acted quickly to remove them, they could have gone to my friends list and so it would have gone on. I like to consider that I am reasonably savvy and yet I still did that without thinking! It is part of the risk of the App, because apart from putting the passcode into your phone, you are always logged in. So you can go there quite easily and be quite flippant. It is also why I don't use the banking App so much because I believe that I could be flippant and accidentally move a large sum somewhere I don't intend to." [David]*

Bank account information had been used falsely to obtain goods or money, which led to caution about making financial transactions online.

Bogus phone calls attempted to get the user to allow others to access their home computers.

> *"I have several times experienced phone calls trying to get me to log onto my computer" to share private information. "A friend told me to just hang up so that is what I do." [Catherine]*

Trust and authenticity

For our interviewees, trust in an online site was a subjective mix of belief, knowledge, experience, and look and feel.

> "*Trust doesn't come into it when dealing with government, there is no other option. If I want to buy a CD however, I have options. I will choose to buy it from one company rather than another based on their reputation and my experience of them."* One of the things Harry might do is check for the company's security certificate. For Harry, trust is a case by case thing. So for example, even though he considers EBay a site with a good reputation, he views each transaction differently because each presents a different risk profile. Therefore he weighs each transaction and relies on his 'gut feelings'. *[Harry]*

> "*I don't do overseas transactions, because I don't know who they are. I want to know physically where they are and to be able to ring the 0800 number and check on something. … And I check who the payment is going through like Paypal or similar." [Emma]*

Reputation was important in choosing 'safe' sites for transactions. Large international companies such as Amazon, Apple, known recording companies and airlines were trusted because of their reputation.

> *"I only deal with a few that I know to be legitimate business such as TradeMe and Amazon." [Bono]*

The more experienced users (e.g. Candice, Harry, Andrew, Rewi) would look for the track record and approval ratings awarded by other users.

Trust was also determined by familiarity with the (quality of) the product offered or easily established standards of quality.

> *"I tend to buy products that I know and trust the quality of: games, CDs, books" [Chris]*

Interviewees might 'look around' to canvass what was available but they took steps to establish the credentials of the sites they actually dealt with.

> *"If I find a company that has something I want and I don't know them then I tend to do a search on the company and check that they are legit(imate) or speak to people at work about whether they have bought from that website"[Chris]*

Participants were alert to signals of a site's reliability, such as the 'padlock' symbol for secure transactions, the security certificate checks done by their own software, or the use of Paypal as the means of payment.

> *"Normally I use eBay or similar because they have consumer protection things. Using Paypal means that if something goes wrong you get your money back. And they have a solutions centre so that anything goes wrong you can report it. If I am going to buy something, I do some research first. I only buy things from people with the top rating which is more secure for the money I spend… and I keep a low-limit credit card for online transactions…..When I want to purchase airline tickets, I might go to some of the other sites to check out who has the cheapest airfares but then I always go to the official airline site to purchase the tickets." [Candice]*

Location of online service lended authenticity and trust to interviewees. Generally New Zealand based sites with a *.co.nz* domain name and where a physical address is provided, were trusted over *.com* or other domain names.

> *"I am fairly wary of overseas sites."*

> *“Because we are from overseas, and we are quite new to it, we are a bit wary about which websites we will use, especially if it is an overseas one. If it is a Kiwi one, I will tend to trust it more. Like if is a ‘.co.nz’ kind of address, if it is something that I have heard of, and the currency is in New Zealand dollars. I have tried buying things from the likes of Amazon and eBay and they always seem to have problem with shipping to New Zealand. You get to the checkout, and create your online address and then they go sorry we don’t deliver there. You get frustrated with that, so I try to stick to the ones that are New Zealand, or possibly Australian, based ... the currency and the shipping costs tend to eat into things, so if you can do it locally it is always a lot better.”* [Chris]

> *“If its .com I am more wary” [Candice]*

Several participants expressed high trust in online government transactions.

> “Something like .govt or a school site I would trust more.”[Candice]

Two participants (Chris, Emma) did not see any difference between government online service providers and other services and tended to trust paper-based transactions more.

> *“It is not necessarily secure online just because it is a government site. It is probably more secure on paper.” [Chris]*

One interviewee saw security of online data as much to do with human error as cyber security.

> *“Security breaches are nine times out of ten human error and that can happen whether it's the public or the private sector. I trust that they are doing everything they can (to manage information security) but I am cynical about whether they can.”[Emma]*

Online protection strategies

Nine of the 23 interviewees used multiple online identities (e.g. multiple email addresses). Their real name was only used in official, work or ‘serious’ relationships.

> Candice has five or six email accounts which she uses for different purposes. Only one or two of these contain personal information linked to the real Candice, such as her name in some form, and these email accounts are reserved for trusted business such as banking or transactions with government. Email accounts containing no information linked to the real Candice are used in instances where an email is required but there is no reason that the information needs to be accurate. *“When I am asked for an email address from a website I provide one of those email addresses that don’t matter and they can’t identify me.” [Candice]*

In trying to maintain control over what identity information was provided in particular contexts, five participants mentioned specific choices they made about when to use a pseudonym, provide fake or incomplete information and/or use particular devices to obscure identity information.

> *“Like date of birth – if it is a required field that you have to provide – I lie. I just change the month or something.” [Emma]*

Six participants stayed anonymous or used pseudonyms when providing comments in online public spaces.

Two exercised caution about what they said online because they realised their comments are public.

> *"I do not post much. What do you say to people in another country when they might not have the same advantages of health care we do in New Zealand. It's too easy to be flippant."[David]*

Some participants chose to use or rejected a particular Social Networking Site (SNS) based on the level of user control of privacy settings

> *"If someone wants to join your [WeChat] group they have to ask you if they can join. Just like Viber and Skype, your friends can leave you a message or you can chat to them directly … you can select the people you want to be able to see the photo…. I know that once you upload a photo on Facebook the privacy is not something that belongs to you. So that is why I hardly use it – because you are not protected."[Candice]*

Online risk mitigation

Online security risk awareness led to risk mitigation strategies like changing settings on Facebook, selective use of online transactions, restricted use of credit card details online or no use at all, use of fake information or pseudonyms, deletion of search histories and cookies, and unsubscribing from unwanted information.

> Harry deletes cookies from his computer daily to make it less likely that a profile of his activities could be built. He also keeps his ear to the ground for information about Apps that might be a risk. For example he has never used 'Angry Birds' or 'WhatsApp' because of things he had read about how they could compromise his security. *[Harry]*
>
> *"I only run one debit card for purchasing online and I don't use a credit card. It's just too risky." [Louise]*
>
> *"I wasn't comfortable doing it at first and I do look for the little verification thing…. I just came across it the first time and read what it was about and thought that's good and from then on I looked for it…. I don't do overseas transactions, because I don't know who they are. I want to know physically where they are and to be able to ring the 0800 number and check on something. … And I check who the payment is going through, like Paypal or similar." [Emma]*

Device security risk awareness also led to risk mitigation strategies, such as using firewalls, using anti-virus software, not storing usernames and passwords on the device, using an encrypted router, limiting device access to other users through using a password or biometrics (fingerprint), not using public WiFi, and 'find my iPhone' activated.

Passwords were used and allocated according to perceived risk: most participants chose strong and/or different passwords for particular uses, and changed passwords more frequently. A few participants only had a few passwords, including one for banking, and didn't use them strategically.

> *Roberta has just one email account and it does not contain any information linked to her personal identity such as her name. She uses multiple passwords of three levels of sophistication: the most complex are used for banking; a less complicated version is used for lower risk transactions and a simple one for other interactions over the web which demand a user name and password. She remembers her passwords by generating them through a system that only makes sense to her. [Roberta]*

While most participants were aware that information exchanged over the Internet can be intercepted and seen by others, the more experienced and better educated users constantly adapted their behaviours according to their assessment of online risk.

> "*We were having this conversation yesterday at work. We were working at the Airport Conference Centre and the only Wifi they could offer was unsecured and we were not happy using that to share confidential information*." [David]

> *"Every time you enter a username and password there is a risk of someone stealing them, so I tend to use my cell phone for Twitter or Facebook so that I don't have to log in every time, rather than my computer." [Harry]*

All the participants referred to having firewalls and virus filters or similar on their home networks and devices.

The younger, more experienced and better educated Internet users were selective in the devices they used according to their understanding of the security of the network connection and the device itself.

> *"I use my iPhone a lot because I find it is quite a convenient device, and I have the touch ID on it, which is more secure than a password." [Candice]*

The distinction made between the security of a smart phone or iPad and the security of a laptop or a desktop computer was not always on the basis of a sound reason or evidence for doing so.

> "*Often I will go into emails on my phone that I wouldn't on my computer, or dodgy websites. I am not sure why but I have never heard of people getting viruses on their phones or their androids but surely you could?" [Karen]*

Internet knowledge strategies

Participants had different knowledge backgrounds and strategies to overcome these. Some of the older, less experienced users could be summed up as 'Don't know what they don't know'. They show little curiosity about the online world, and appear to have had little interest in learning beyond a few usually family-orientated uses, and they had minimal or no strategies for online identity management.

Other relatively new, and generally older users (e.g. Chris, Tamati, Claudia)were more curious and active learners, tentatively 'learning by doing' and therefore came to the Internet at a pace they felt comfortable with. For these people, good first experiences and convenience were overcoming their fear of the unknown.

> *"We use it [home laptop] for keeping in touch with friends and bank accounts mainly."* Tamati uses email for communication and does not have any social media accounts. For some recent travel overseas they purchased an iPad: *"it was fantastic for staying in touch by email and sending some photos home." [Tamati]*

'They know that they don't know': many relatively new and generally older users were aware of their lack of knowledge and they looked for help from family or other more expert users and/or limited what they did online.

> When Louise needs information about how to do something online she finds that almost *"anyone under 25 can help." [Louise]*
>
> Jack uses his son-in-law as a source of advice when he is in doubt because he knows that his son-in-law has made it his business to be informed on computing things. He has never

> consciously done any backup of his computer files: *"My son-in-law might have done it for me, into the Cloud, I suspect. I really don't understand how all that works."[Jack]*
>
> *"I rely on my daughter to do some things, like I got sent a .jpg the other day and I didn't know what that was so I had to ask her to help me with it."* Catherine has been cautious with her privacy settings on Facebook: *"I got my daughter to set it up for me so that only friends can see my information."* Her daughter is also the one who put up pictures on Facebook and is going to put up a virus-check. She has only one e-mail account, but uses different passwords for e-mail and Facebook: *"I've been told to have different passwords, so I have." [Catherine]*
>
> If Tamati was forced to use online alternatives in transactions with the government he would probably do it: *"You learn new things all the time, and we would if they said that is the way we gonna go." [Tamati]*

More knowledgeable participants treated the Internet as the 'go-to' place in their everyday lives.

> *"I go online every day: checking my emails and Facebook and read news on Stuff would be the main things I do every day. I would probably also upload videos on YouTube and watch movies or videos. America is so much faster than New Zealand with TV programmes. It's just so much easier to find it online". [Angela]*
>
> *"I have just found that it is really easy to apply for a passport online. They have a chart that makes it easy to create a photo of the right size and quality. It checks whether the photo you provide meets the requirements before you submit it." [Candice]*

Cross referencing and comparing the output from different accounts was a strategy used by some to counteract accuracy concerns.

> Louise judges online credibility in different ways according to type of material*: "Academic stuff is more about the site and how it is written, how it is set out and the evidence behind it. A few of those sales type sites it is harder to tell. I look for based in New Zealand, phone numbers, something that is reasonably well known like Unity Bookshops or something like that. That is, I already know something about them in the offline world and that translates into the digital world." [Louise]*

Parents among the participants played a role in the education of their children about the online world and vice versa: digital-native children were a source of information, know-how and advice to their parents; parents were the voice of experience to their children.

> *"They all get hacked in some way at some time and you have to clean them out. Sometimes it requires a rebuild of the system because some of the viruses are pretty nasty. So because I am aware of it, I try to emphasise that kind of security to family and friends, but you can't control the sites they visit." [Rewi]*
>
> *"My son was a little worried when his father sent me some photos from a rugby tournament recently. He didn't realize that he [father] had been on to Facebook, seen the photos and sent copies of them to me. So that was a bit of a wake-up call for my son about his privacy settings." [Roberta]*
>
> "*Just recently our son corrected me on something, 'no do it this way' because he has been taught how to do it at school. I can also do lessons with him, like maths on line, which is way more fun than me trying to remember how to do it from my school days." [Louise]*

The older and less experienced Internet users were fully aware of the limitations of their own knowledge and competence and tended to limit their activities accordingly.

> *"I'm pretty old-school….. A couple of my friends emailed me and asked me to join Twitter, but I don't know what that is, so I haven't joined." [Catherine]*

Privacy behavioural types

In analysing each individual's online identity information behaviour, we concluded that participants fell into three different 'privacy' behavioural types. We have named these behavioural types the privacy pragmatist, the privacy victim, and the privacy optimist. We describe these three types and give examples below.

Privacy pragmatist: makes a pragmatic, willing exchange of personal information to get more or better personalised services; depending on the transactional relationship, privacy is a commodity. Also, location information is traded strategically for convenience and particular services.

> "*Profiling helps you get the services you want".* Andrew is aware that online trading sites he interacts with are building a profile of his preferences but he sees this as part of modern commerce: *"you have to give some information to get some more information".* He considers the unwanted emails that often follow registering with a particular site as annoying but not a threat to his privacy*. [Andrew]*
>
> Chris is aware that online trading companies he deals with are building a profile of his preferences and estimate that perhaps 50% of the email he receives is generated by his signing up to one site or another. *"Currently, I just delete it. I am aware that you can turn it off, and if it got too much I would". [Chris]*
>
> *"I find Linkedin useful for work…. All the information I provide there is publicly available anyway. I don't put my CV on there. There is a work history and a photograph but all of that is available anyway in other areas. I generally contract so I prefer to manage my own brand and I use it to promote my work."[Emma]*

Privacy victim: is less willing in the exchange of personal information and frequently decides not to proceed because of the amount or type of personal information they are asked for; for a small number of highly selected services, they see loss of privacy as an inevitable quid pro quo in order to get the service, but as a general rule these participants would rather not put any identity information into an online space they cannot completely control.

> *"I have an aversion to information about me being on the Internet. I try to minimize what I provide."[Roberta]*
>
> *"I wouldn't hesitate to cancel out of them if they asked for it. I like to be in control of where my information goes." [Jack]*
>
> *"I don't put photographs on Facebook anymore. When I was in high school I did, but now I don't like putting my information out there. My Facebook profile is really private, so if you are not a friend then you can't see anything."* She has not posted any comments online either *"because normally when you do that they ask for your email and I don't like giving out my email."* She has googled herself*: "and not much comes up, just my Linkedin profile, which is good…. I was a bit shocked that the photo of myself on Linkedin then appeared on Google Images."* So she has changed her privacy setting on Facebook and Linkedin. She has experienced other people posting pictures of her online and she would consider asking them to remove a photo she did not like*. [Judith]*

> *"I Googled myself and sadly I come up not only in Linkedin but also in some media releases as well…. And now it is there and it can't be removed." [Emma]*

Privacy optimist: people pay little attention to privacy even though they are aware of concerns expressed by others and are willing to keeping doing what they think might be risky until something bad happens to shake their faith.

> Leila is generally happy with using public Wifi: *"I realise that it's probably not that good because other people can 'see' if they know how to hack into other people's devices. That is why I have only done Internet banking on the CBD Free. The same probably applies to uni as well but as I haven't got very much money in my account it probably doesn't matter that much!" [Leila]*

We 'discovered' these privacy behavioural types on the basis of just 23 individual interviews. Clearly we needed to obtain more evidence of the existence of these types. This is one of the objectives we pursued in the focus groups, which we describe next.

Analysis of the Focus Groups

"The internet is like the world, really. We've all got the creepy corners and spooky corridors to get down." FG2 male

Introduction

We have described in the Research Design section (see p.16) how the ten focus groups were formed and conducted. In this section we present an analysis of the data collected through these focus groups. We begin with a general overview of each of the focus groups and identification of the characteristics of the participants. We then proceed to identify themes which emerged from the discussions in these groups. These expand on the themes already identified in the analysis of the survey and the interview data.

Composition of each Focus Group

Focus Group 1

This Focus Group involved a group of seven senior citizens of 65 years and over, who lived in an urban area on the North Island. All participants were of Pākehā descent and the large majority of the group had 3 years of secondary education. The group were participating in the local SeniorNet initiative, a community training network that supports and motivates people aged 50 years and older to enjoy and use technology in their everyday lives. Communication with children and grandchildren was an important driver for these participants to use the Internet. Financial information was often considered private. If they shared their identity information online it was always real and not fake information.

Focus Group 2

Focus Group 2 involved five women and two men of various ages, ethnicities and educational backgrounds. Most participants had low or nil income. They lived in an urban area on the North Island and were all participants in the local Computers in Homes initiative. All were fairly new and inexperienced Internet users who recently had been through an Internet course. Most had a personal computer supplied to them through Computers in Homes and these came with at least three free computer protections (AVG Anti-virus or BitDefender, Malware Bytes and C-Cleaner) installed. Time was spent in class going over these three pieces of software.

Focus Group 3

Four female and two male university students currently living in a city on the North Island participated in Focus Group 3. Some had travelled to that city for their study from other parts of New Zealand including other cities and rural areas. Five of them were between 18 and 24 years of age and one belonged to the 25-34 age group. They had different ethnic backgrounds with the majority of the group being from NZ European descent. Participants had either a low income or no income at all. This group all used multiple devices, often simultaneously and as well as the Internet being the go-to place for every information need, it was also used to maintain a constant network of communication with friends to support their social lives.

Focus Group 4

This Focus Group consisted of two males and four females living in a rural area on the South Island. The group included one individual of Māori and Pasifika descent with the rest of Pākehā/European descent, and ages ranged from 18 to the 55-64 age group with the majority in the 35-44 and 45-54 age segments. The location of the group was particular for two reasons. First, because the places people lived and worked were spread over considerable distances, the Internet represented an additional, quicker, cheaper and more time efficient way of connecting with the participants' local community and environs.

The second reason was that this group was also within a feasible day's journey from Christchurch and most had been affected in some way by the earthquakes in that area which occurred after 4 September 2010 and caused loss of life on 22 February 2011. Apart from the trauma of loss of life, physical and psychological injury, there was major damage to infrastructure, such as roads and buildings, as a result of the major quakes and the thousands of aftershocks that occurred after September 2010 disrupted people's lives in a multiplicity of ways. As a result, most of the people in this Focus Group had changed their Internet use. For some it was now a way of staying in contact more closely with affected friends and family, avoiding the areas that were most damaged and disrupted, or a way of continuing an activity that no longer had its former infrastructure or location.

Focus Group 5

The five women and two men involved in Focus Group 5 were all Pasifika and lived in an urban area on the North Island. Across the group the participants were using a range of devices online: personal computer (6), laptop (6), tablet (4), smart phone (6), public kiosks (3) and games console (1). Five participants had either 4 or 5 years secondary education while two had some tertiary level education. Only two participants provided income information and this was in the $50-70,000 and $100 - 150,000 brackets.

Focus Group 6

Eight Asian people (two men and six women) living in an urban area on the North Island participated in Focus Group 6. Seven had a tertiary level education and one had four years secondary education. The participants used a range of devices and mostly more than one: personal computer (6), laptop (7), tablet (6), smart phone (7), and internet-enabled TV (1). Incomes ranged up to $100,000 and one provided no data: $1-10,000 (2), $30-50,000 (2), $70 -100,000 (3).

Focus Group 7

Five Māori men and three Māori women in a North Island city participated in Focus Group 7. Five had tertiary level education, 2 had five years secondary education and one 4 years secondary education. All used more than one device to go online: personal computer (8), laptop (6), tablet (7), smart phone (8), public kiosks (1), internet-enabled TV (2) and games console (1). The participants incomes were spread across the range from $30,000 to $150,000: $30-50,000 (2), $50-70,000 (3), $70-100,000 (2), $100-150,000 (1).

Focus Group 8

Five men and two women made up Focus Group 8. All were fairly new and inexperienced Internet users who had recently been through a Computers in Homes Internet course. Some had purchased their personal computers through Computers in Homes and these came with at least three free computer protections (AVG Anti-virus, C-Cleaner, and Malware Bytes) installed and classes had covered the purposes and importance of these three pieces of software for online protection. Several members used more than one device for Internet access: personal computer (7), laptop (4), tablet (1), smart phone (5), and internet-enabled TV (2 and public kiosks (1).) Their main reasons for using the Internet were Facebook, Skype (and video calling in Facebook), convenience (banking and appointments), games, contact with overseas friends (including health issues), children's homework, email, and news channels.

Focus Group 9

The six men and one woman in Focus Group 9 were all operating a business in an urban centre on the North Island. They were spread across the age groups from 25-65 but most fell into the 35-55 groups. Their incomes were also varied from $10-20,000 (1), $30-50,000 (3), $70-100,000 (2) to >$150,000 (1).

Their need to use the Internet was primarily a business-led one but they also used the Internet for communication, banking, awareness of business practice and marketing. Most used more than one device to go online: personal computer (6), laptop (4), tablet (5), smart phone (5), e-book reader (2), internet-enabled TV (1) and kiosk (1). Five had tertiary level formal education and one had five years secondary education.

Focus Group 10

The five women and three men in Group 10 all worked in a North Island city. All had tertiary level education and all had an income above $50,000, except one who had an income under $10,000. Their reasons for using the Internet, which they did for many hours a day every day, were seeking Information (news, general info, browsing), help with interests, all parts of life, contact, entertainment, and Facebook for a couple of participants. They used multiple devices: personal computer (7), laptop (6), tablet (6), smart phone (7), e-book reader (3), internet-enabled TV (2) and a games console (1) .

Background of the Focus Group participants

Table 3: Age, ethnicity, location, income and education range of focus group participants

Group	Number	Age Range	Ethnicity	Location	Income	Education
FG1	7	65-74yrs = 3 75+yrs = 4	NZ Euro = 7	NI Urban	$10-20k = 1 $20-30k = 2 $30-50k = 1 Decline = 2	3yrs secondary = 6 Tertiary = 1
FG2	7	25-34yrs = 1 35-44yrs = 3 45-54yrs = 2 55-64yrs = 1	NZ Euro = 3 Māori = 2 Pasifika = 2 Other = 1	NI Urban	$0 = 1 $1-10k = 1 $10-20k = 2 $30-50k = 1 Unknown = 2	None = 1 Primary = 1 4yrs secondary = 2 Tertiary = 3
FG3	6	18-24yrs = 5 25-34yrs = 1	NZ Euro = 3 Māori = 1 Asian = 1	NI Urban	$0 = 2 $1-10k = 3 $10-20k = 1	5yrs secondary = 5 Tertiary = 1
FG4	8	<18yrs = 1 35-44yrs = 3 45-54yrs = 3 55-64yrs = 1	NZ Euro = 1 Māori = 1 Pasifika = 1 Other = 2	SI Rural	$0 = 1 $20-30k = 1 $30-50k = 2 $50-70k = 2 $100-150k = 1 $150k+ = 1	3yrs secondary = 1 5yrs secondary = 2 Tertiary = 5
FG5	7	25-34yrs = 1 35-44yrs = 1 45-54yrs = 4 55-64yrs = 1	Pasifika = 7	NI Urban	$50-70k = 1 $100-150k = 1 Decline = 5	4yrs secondary = 3 5yrs secondary = 2 Tertiary = 2

FG6	8	25-34yrs = 1 35-44yrs = 2 45-54yrs = 4 55-64yrs = 1	Asian = 8	NI Urban	$1-10k = 2 $30-50k = 2 $70-100k = 3 Unknown = 1	4yrs secondary = 1 Tertiary = 7
FG7	8	25-34yrs = 2 35-44yrs = 5 45-54yrs = 1	NZ Euro = 2 Māori = 8 Pasifika = 2	NI Urban	$30-50k = 2 $50-70k = 3 $70-100k = 2 $100-150k = 1	4yrs secondary = 2 5yrs secondary = 1 Tertiary = 5
FG8	7	18-24yrs = 1 35-44yrs = 1 45-54yrs = 3 65-74yrs = 2	NZ Euro = 2 Māori = 6	NI Region	$10-20k = 2 $20-30k = 3 $30-50k = 1 No response = 1	Primary = 1 4yrs secondary = 1 5yrs secondary = 1 Tertiary = 4
FG9	7	25-34yrs = 1 35-44yrs = 2 45-54yrs = 3 65-74yrs = 1	NZ Euro = 5 Pasifika = 1 Other = 1	NI Urban	$10-20k = 1 $30-50k = 3 $70-100k = 2 $150k+ = 1	5yrs secondary = 1 Tertiary = 5
FG10	7	25-34yrs = 1 35-44yrs = 2 45-54yrs = 3 55-64yrs = 1	NZ Euro = 6 Other = 1	NI Urban	$1-10k = 1 $50-70k = 3 $70-100k = 1 $100-150k = 2	Tertiary = 7

Internet use of the Focus Group participants

Internet activities

The Focus Group (FG) participants used the Internet for a wide range of online services (see Figure 1), usually with more participants being active users but with a similar distribution compared to the survey participants (see Table 3). All FG participants used the Internet for accessing information, whereas 96 percent of the FG participants used it for communication with family and friends, and 87 percent to enjoy online entertainment. Other popular online activities amongst FG participants were online banking (84%), buying things online (84%) and social networking (83%). The least popular online activities were pretending to be someone else (2%), followed closely by online dating (6%) and hacking (6%). Other not so popular online activities were conducting a business (24%) and participating in online public consultations (25%).

Figure 1: Online activities in the last 12 months by focus group participants (n=72)

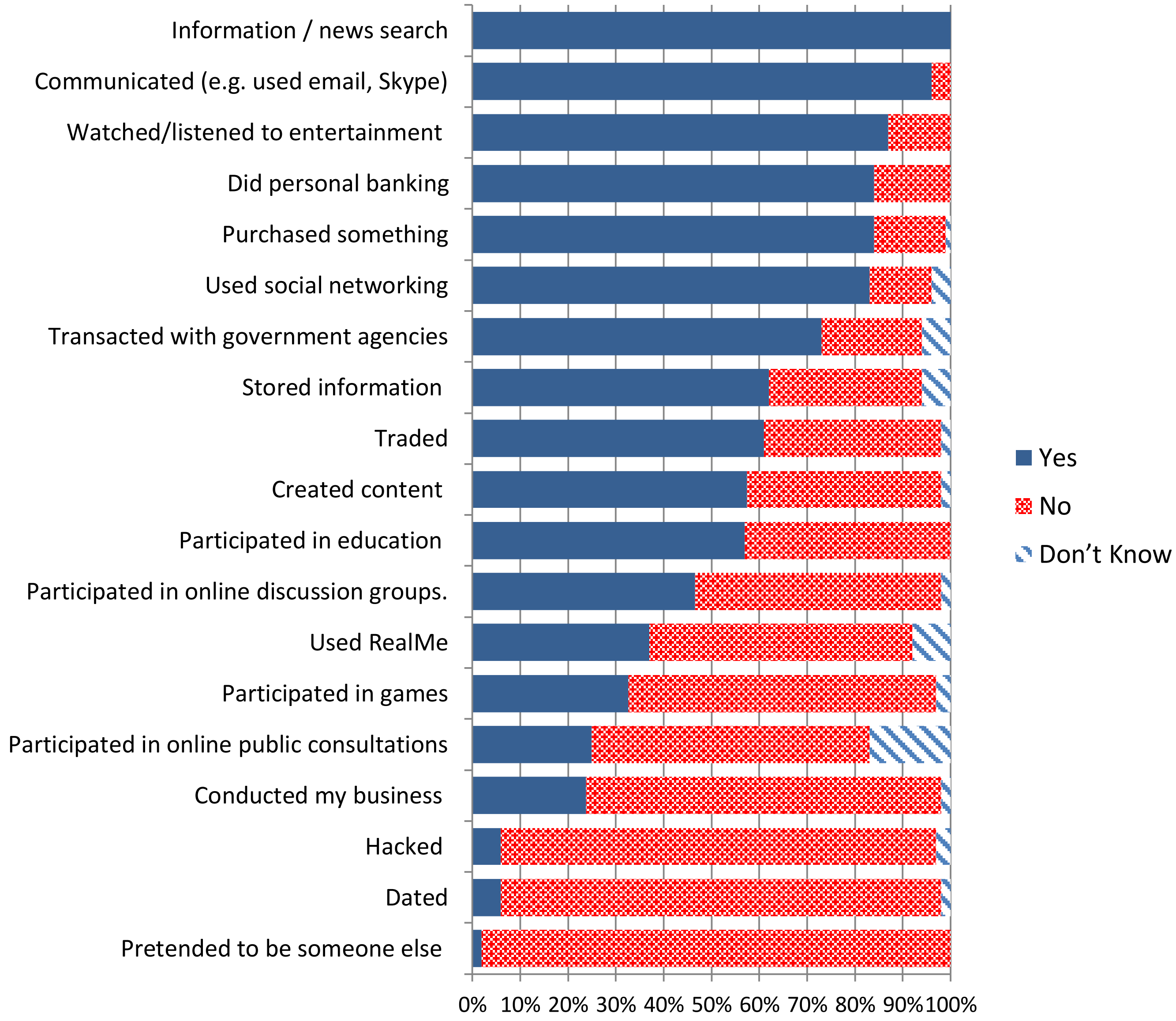


Table 3. Comparison of Internet activity

Internet Activity %	FG n=72	Survey
Information / news search	100	99
Communicated (e.g. used email, Skype)	96	94
Watched/listened to entertainment	87	79
Did personal banking	84	83
Purchased something	84	87
Used social networking	83	74
Transacted with government agencies	73	68
Stored information	62	35
Traded	61	68
Created content	58	43
Participated in education	57	36
Participated in online discussion groups.	47	23
Used RealMe	37	20
Participated in games	32	25
Participated in online public consultations	25	16
Conducted my business	24	15
Dated	6	4
Hacked	6	2
Pretended to be someone else	2	1
Other	0	3

Devices

FG participants used devices to go online slightly differently compared to survey participants (see Figure 3 and Table 4). The personal computer was by far the most used device by FG participants (92%), followed by the mobile phone (76%) and the laptop (72%). Also, compared to survey participants, a relatively higher proportion of FG participants used a tablet (57%) and Internet TV (19%) to go online.

FG participants gave the following explanations for their relatively high uptake of mobile phones and also other devices to go on to the Internet.

> "*Your phone has taken over a lot of jobs that a desktop or laptop would do*." FG4 male

Many indicated that they had more than one device to go online.

> "*Usually you've got more than one device, by the time you've got your laptop, iPad and your phone…*" FG4 female

> "*I use two at the same time. Today I was looking up an address and writing an email. So I do the email on my iPad and check the address on the laptop*." FG4 female

Figure 2: Devices used to access the Internet by focus group participants (n=72)

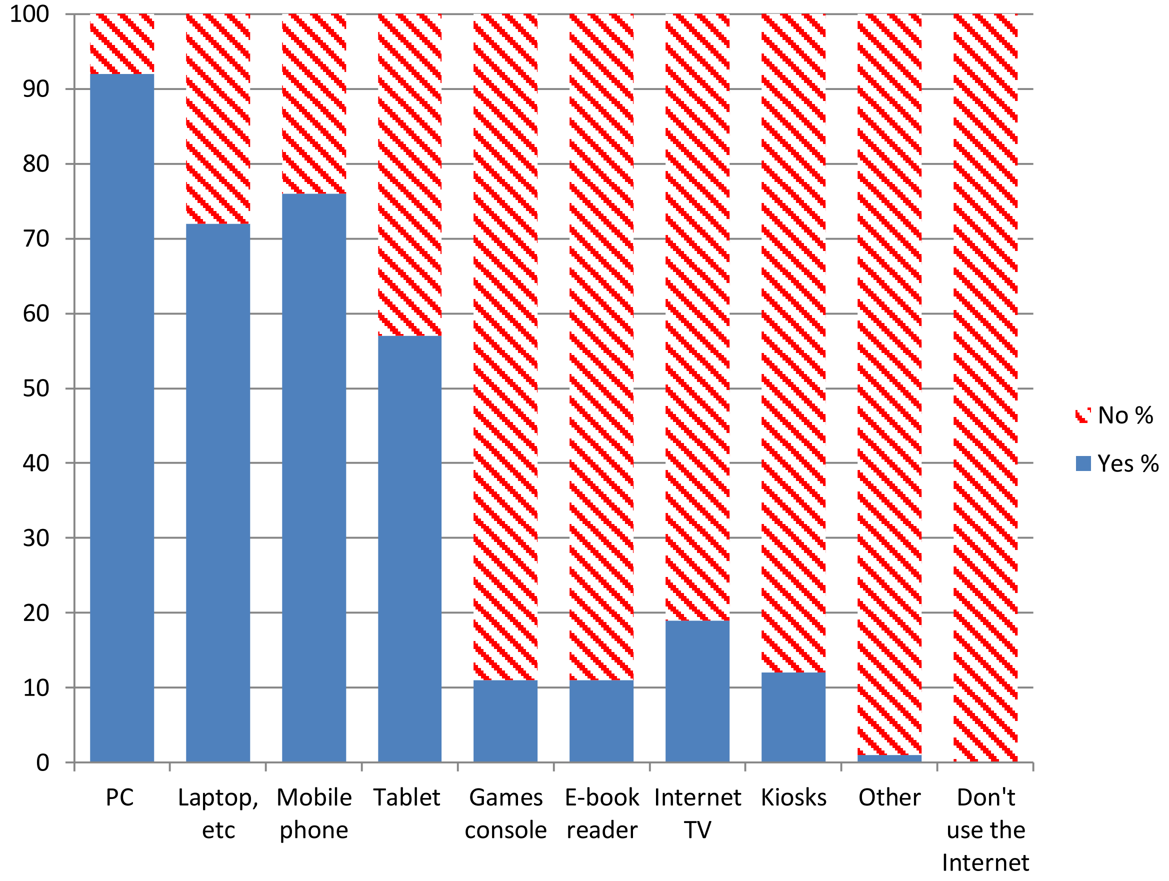


Figure 3: Comparison of online devices

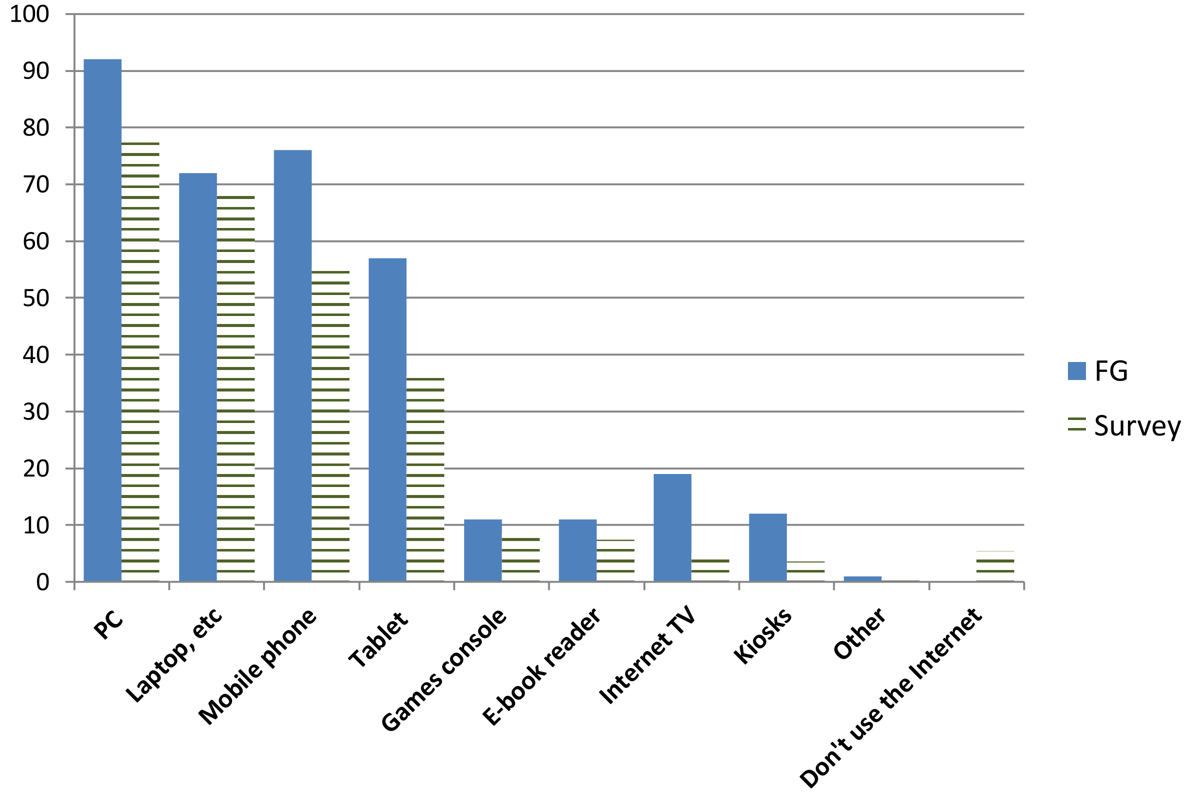


Table 4: Comparison of online devices

Use of device %	FG	Survey
PC	92	78
Laptop, etc	72	68
Mobile phone	76	55
Tablet	57	36
Games console	11	8
E-book reader	11	7
Internet TV	19	5
Kiosks	12	4
Other	1	1
Don't use the Internet	0	5

Location and frequency of Internet use

FG participants much more frequently used the Internet at multiple locations (see Figure 4), compared to survey participants (see Figure 5). Most FG participants used the Internet on a regular basis at home.

> "*It's just easier to do it from home, or wherever*," FG8 female

Many FG participants indicated using the Internet differently at varying locations.

> "*I use it differently at work from at home. I use it more efficiently at work because I'm getting paid… whereas at home I can spend hours and not even realise. Whereas at work I've trained myself not to check Facebook, because I might get hōhā*[5] *with something I see and have to reply. I'm certainly more efficient about how I search, and how I think about the Internet at work*." FG7 female

Privacy and security were other important reasons for preferring to use the Internet at home.

> "*Banking or Studylink or transactions like that I pretty much stick to doing at home on my laptop or my phone. Basically no one is watching over my shoulder when I am doing it at home*." FG3 male

> "*I only use [WiFi] at home to pay the bills*." FG6 male

> "*I don't use other people's computer for banking or credit card details. I always use my home computer or work computer. It's quite obvious. There's no free food!*" FG6 female

FG participants used their mobile device much more frequently compared to the survey participants. Several participants, in particular Asian people, indicated finding a mobile device more secure.

> "*First I choose a safe device – like iPad is safe – and I use my mobile phone since I've got anti-virus. For internet banking I only do it on my work PC because I work for a bank! It's very secure. And I try not to do too many transactions*." FG6 female

> "*I do it on my phone, because it's tiny. I do it quickly and no one can see anything*." FG3 female

[5] Māori term – annoyed.

Only a few FG participants didn't have Internet access at home. However, this didn't stop them from using it.

> "*I haven't got Internet – we can't afford it where we're staying. It's too expensive….She [indicating wife] uses it*." FG5 male

Pasifika, but also a few other participants, thought that Internet use in New Zealand is too costly.

Figure 4: Location and frequency of Internet use of focus group participants (n=72)

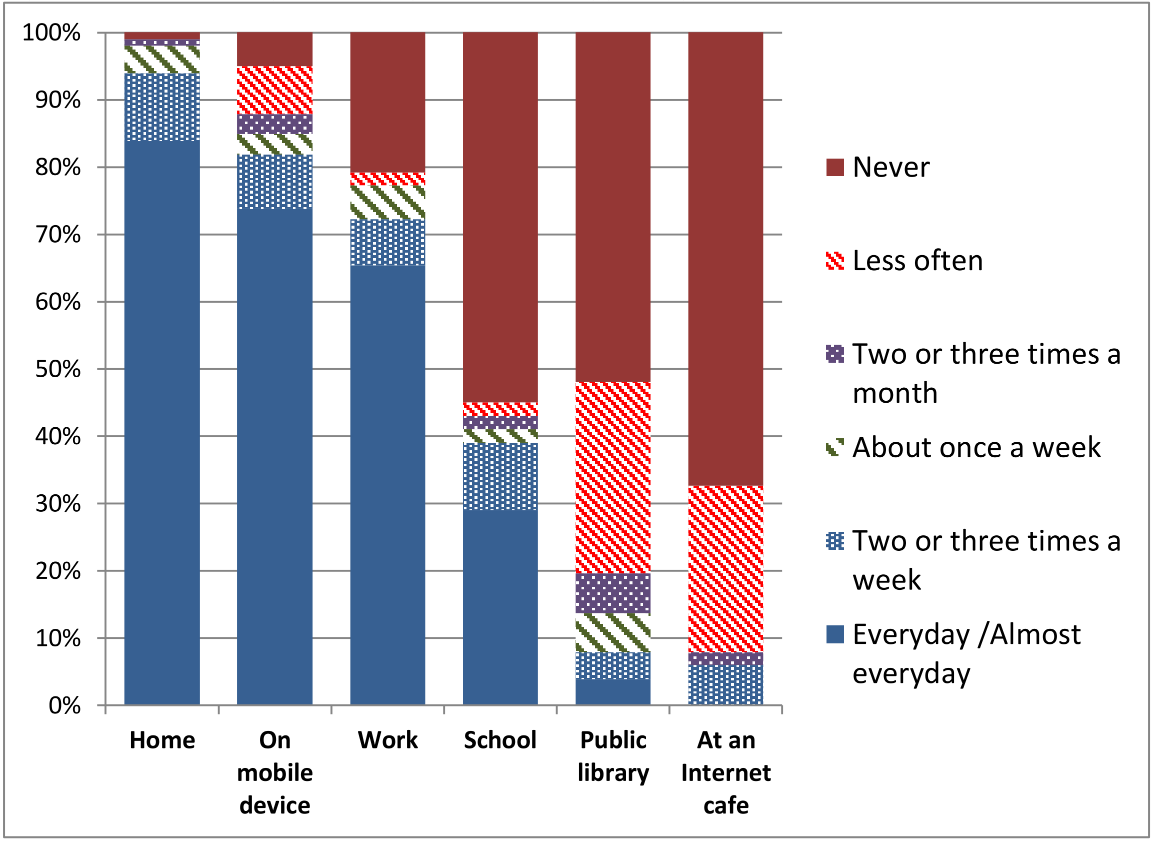
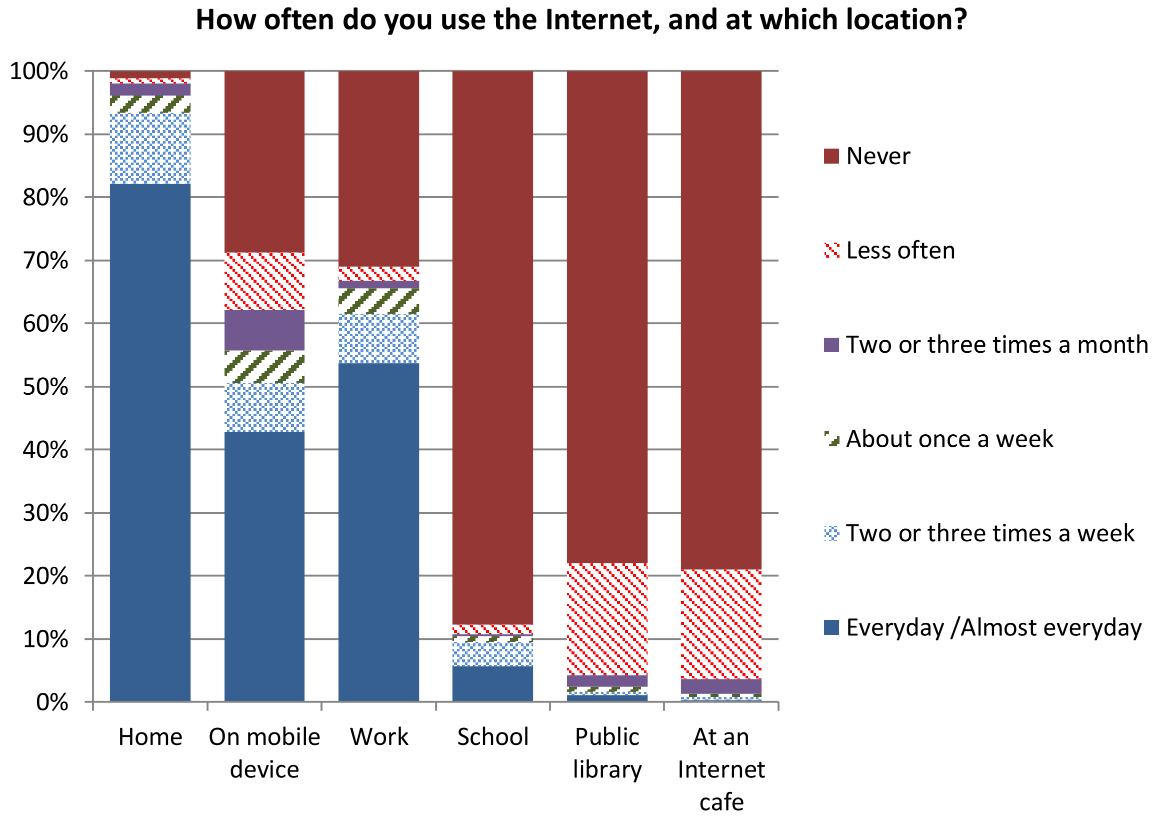


Figure 5: Internet location and frequency of survey participants



Focus Group findings

Critical importance of Internet use

For the majority of participants, the Internet played a critically important part in their lives.

> "*Day to day functioning, not necessarily financial. The sports clubs that my kids are involved with – that's the main mode of communication*." FG4 male

> "*It [Internet use] is organic. For me it started off with information but has moved on to more of a 'life-style assistance' tool. Everything from gathering information to buying things, planning to holding and storing information*." FG10 male

> "*It brings the world for us, closer*." FG6 female

For those with family or friends living overseas, the Internet was critical to stay in touch.

> "*Helps me keep in close contact with my grandkids, and my nieces and nephews in America. It's like my lifeline – I couldn't imagine being this far away without that*." FG2 female

> "*I've got Facebook. I've got a brother over in Aussie and keep in contact through that*." FG8 female

> "*One of my children's over in Australia and a lot of my family, so we communicate through Facebook and Skyping.*" FG8 female

Several participants gave examples of how Internet use empowered them. For example, an older participant (FG1) frequently skyped with one of his children when they were travelling in a campervan. He and his wife could not only directly see and communicate with their child and his family on a regular basis, but also see the environment they were visiting.

Online devices even helped one participant to get his stolen belongings back:

> *"We got broken in to when the family was out of the house. They stole iPhones, iPads, computers. A day or so later the people started turning them on and they were pinging up where they were. There'll come a time when there'll be a location device in the crockery! And people will stop stealing stuff."* FG9 male

Some indicated that those who are not using the Internet could be worried about being excluded or missing out on opportunities.

> "*My mother doesn't have any Internet connection at all and it winds her up that everything you see on TV – if you want to talk to a counsellor it's this email. Well where is that? 'I need to go and speak to you.' All they have is an email. There's so many competitions she would enter!"* FG4 male

Reliance on technology

Several participants described how they have become more reliant on the Internet over time.

> *"[My online behaviour] has just got worse. I purposely left my phone in the car so I wouldn't be sitting in here getting notifications, letting it vibrate and quickly checking my phone while you guys were talking…!"* FG8 female

> *"I started when I was 13 and I'm 23 now, and it's just gotten worse over time, especially with Facebook."* FG8 female

Some participants were reminded of the critical importance of the Internet in their lives through recent significant events, such as the Christchurch earthquakes.

> "*I used it more after the earthquakes because I didn't want to go to Christchurch to do things*." FG4 female

> "*All your maps became obsolete*." FG4 male

More recently, power cuts in Auckland made several participants aware of their reliance on technology.

> "*There were big power cuts in Auckland two weeks ago. We have a hardware store so everyone came in to ask for gas and that sort of thing. But the one complaint that everybody had was not that we were without power or without food, it was 'I can't charge my mobile phone'*." FG9 male

> "*Reliance on technology – that was highlighted the other week in Auckland. Pull the plug and millions of dollars in commerce just stops. As a kid I was brought up in a rural area. If the power was off all day it didn't matter – didn't make much of a difference. But now …"* FG9 male

> "*I wouldn't even be able to ring my husband – I can't remember his phone number*." FG9 female

Several participants, mostly younger or Asian people, said that they could not live without the Internet.

> "*Can't live without it*." FG6 female

> "*It's addictive*." FG6 female

Especially young people would be lost without the Internet and rated it as critically important in their personal life.

> "*10 out of 10*" FG3 female

> "*We are so used to it being around now that I think if we suddenly didn't have Internet everybody would be lost*." FG3 female

> *"Everything is just so much more difficult to do without the Internet. If you want to get in touch with your friends, it doesn't matter where they are; you want a book from the Library, instead of having to spend time going there and looking for it, you go online and there it is. I might spend all that time going there to check out what is in the book and what I am looking for might not even be there. You just Google it from home. That is much faster and more efficient."* FG3 female

Young participants pointed at the critical need of using the Internet for their education.

> *"You also need it [the Internet] for Uni. Like all the resources and lectures are on Blackboard."* FG3 female

> *"It would certainly be impossible to pass your Course without Internet. That is how the course co-ordinators talk to us. Online quizzes and tests. Online pre-quizzes for science courses before and after the labs. If you don't get a high enough grade you are not allowed in."* FG3 female

> *"The lecturer has made a Facebook group for everyone in the Course. You get reminders of when essays and assignments are due and if you have questions the Lecturer will answer them on the Facebook page. He is online all the time and chances are that everyone is going to see everything anyone posts."* FG3 female

However, one young participant admitted that she sometimes would like to break away from this permanent state of online connectivity.

> "*Sometimes I wish I was not so contactable. Everyone can get your mobile, your email, your Facebook and so on. Sometimes you need a break and you want to throw everything away and have it that if people want to see you they have to come over [in person]*." FG3 female

Addictive

Several participants described how addictive the Internet has become for them.

> *"You know when you're sitting around with nothing to do, you just search something… I'll see something on TV and go 'I wonder if that's true' and I'll go do a little google. And then when you go on that one you go 'oh look at that' – pick that one… then you pick that one, and suddenly I've gone from what I started looking for and I'm looking at something completely different… I feel scattered when I'm on it…. That's why I don't go on it every day."* FG5 female

> *"I don't know how many sites I've signed up to for a one-day special or sale. Those ones like Treat Me, they're addictive. You always have to look at a bargain."* FG7 male

> *"[I] love YouTube of course. You'll be mucking around on that and then look down and see it's been hours. Random stuff can be a bit addictive like that… It's alright if the weather's a bit bad, but you've got to police it a bit."* FG8 male

Online vs Offline

Several participants described how the Internet is increasingly replacing traditional channels.

> “*A lot of things that used to be done by paper, phone call or fax, now it’s all been and gone*.” FG4 male
>
> “*We’ve got a phone line at home we hardly ever use … I don’t even know what our phone number is. We become lazy. [The landline] is a free call but we use the mobile anyway….I’ll text [wife] from the lounge and she’s in the bedroom*!” FG7 male
>
> “*I started reading the papers online so I don’t actually buy the physical newspaper. And certainly from my husband’s business point of view, he’ll read the overseas newspapers as well – on a daily basis*.” FG4 female
>
> “*For me phone calls are being replaced by face-time – Skype*.” FG7 female

Whilst recognising the critical importance of the Internet in their lives, many FG participants, in particular those of 35 years and over, continued to appreciate the offline world.

> “*I still prefer to sit down in a cafe and open a newspaper. We get the paper delivered and I find 10 or 15 minutes somewhere in the day to open the newspaper*.” FG9 male
>
> “*I prefer that too, with physical paper. My daughter, who’s 28, does everything online. She would never pick up a paper – everything is done through her phone. It’s different generations*.” FG9 male
>
> “*I’ve stopped reading the newspaper. I’m that 28 year old group*.” FG9 male

Several participants, including the majority of older people, preferred offline interactions and transactions over online transactions.

> “*I want to go to the bank and see what I’m getting*.” FG1 male
>
> “*I signed in to [Facebook]. But I don’t have the time to play with it… I can see the potential there for communication with people you otherwise wouldn’t see. It isn’t possible for people in Auckland to have a cup of tea with you*.” FG1 male
>
> “*I’d rather get out and do my shopping*.” FG2 male
>
> “*I don’t have a Facebook account at all. I occasionally find things on it for work, but I don’t use it at all… I’d much rather have the face-to-face communication with friends – call them up or arrange to meet them. I don’t feel the need to have that big network out there. But privacy is a big thing for me*.” FG10 female

A few participants made a distinction between family or friends living nearby and those further away for their channel preference.

> “*For family [living nearby], I think text and email is just an add-on to the relationship we already have. But for people who live a bit further away, it can start to replace the effort to call or make other contact – just because it’s so convenient to flick someone an email or text*.” FG7 female

Online vs offline trust

Several participants had more trust in offline channels compared to online channels.

> “*I was doing online buying as well and we had a little scare where people were hacking into our credit card numbers so I just stopped it altogether. I prefer the face-to-face thing when it comes to something like [banking]*.” FG8 female
>
> “*There’s too much in the press about people hacking these things. I have one account in the bank down the road and I go there to check it out*.” FG1 male

Some participants preferred offline channels so that they have an opportunity to check on possible errors.

> “*I’ll go back to paper if there’s something I don’t trust – I’ll ask them to send me something.*” FG8 female
>
> “*I know when we’re doing our government tax, GST and so on, we prefer to do it by paper because if the girls do it online and make a booboo it’s there and gone. Whereas at least we can have somebody else double-check what we’re doing [with paper], and I think that’s important*.” FG9 male
>
> “*If there’s something important that you’ve got to edit I’d much rather do it on a hard copy than online*.” [FG9 male

Offline is of superior quality

Several participants, in particular older people, pointed at the superior quality of offline social interactions over online social interactions. They were fearful for a development in society of people having less social interaction as a result of Internet use.

> “[*Social networking is] taking people away from having social interaction. It’s much nicer to sit down and have a cup of tea with somebody and have a chat. We had a family occasion last week and I had all my granddaughters there. So I took a bucket out and said: “put your phones in there – and you’re not having them back until you go home.” They were all twitchy*.” FG1 female
>
> “*My other grandkids who have gone off to uni, they’re continually doing this [face down over phone] and for me, from back in the day, I don’t like it. It’s like having the TV on when we’re sitting down to eat. It’s just not on! It has [stopped] so we can have time. Otherwise I feel as if I’m losing my grandchildren to technology. Where’s the help when they’re down and feeling depressed? What can [technology] do for them? Whereas people can do for people.*” FG8 female

Several participants pointed at the limitations of online channels in order to build trusted relationships with people. For example, one participant described her work experience on a school Board of Trustees trying to improve whānau engagement in the school.

> *“I’m convinced nothing can replace that face-to-face in that environment where you’re building relationships with people who perhaps haven’t had a great experience with the education system themselves. Getting them through the door isn’t going to happen with a text message or Facebook message or an email*.” FG7 female

Young people also considered a face-to-face meeting of higher quality compared to online interactions.

> “*I would rather have a conversation with someone in person than online. It’s just all the little things like when are we meeting … making arrangements to meet face-to-face*.” FG3 female
>
> “*We’d definitely prefer to hang out with someone in person rather than have a long conversation with them on Facebook*.” FG3 female

> “*Meeting up with people that you have only met online. No. If you want to meet people, you can’t work out if they are a psychopath online. You need to check them out first*.” FG3 female

However, there were a few exceptions amongst young participants who preferred the online environment over offline interactions.

> “*I feel like I’ve kind-of lost touch with people… They say that Facebook is the new social thing but you’re not just shutting the laptop door, you’re shutting yourself off from life. You could have 700 friends, have good chats with them but you could see them in real life and walk right on by… [using the Internet] it’s easier to shut people off. Shut off the drama, the nuisance. Hide stuff if you don’t want them to see it. Block people*.” FG8 female

Online is different compared to offline

Several participants pointed at substantial differences between the new online environment and the traditional offline world.

> “*At school, if you were being bullied you would go and tell the teacher and they would do something about it. But on the Internet… My sister was getting bullied for about three months and I just went on to her account and looked at all the stuff and showed my mum. Up until then she had kept it a secret. You can get bullied so hard on the Internet*.” FG3 female

> “*Just watching my kids do homework – Mathletics and all those cool ideas. It’s interesting now instead of boring*.” FG4 female

> “*I don’t think the Internet has made [crime] more prolific, it just made it more faceless*.” FG4 male

According to the participants, these substantial differences have led to some fundamentally different behaviours.

> “*Our whole behaviour has changed, from prior to the Internet*.” FG4 female

Same behaviours but in different environments

Participants discussed that some behaviours have not changed much compared to the situation prior to the Internet.

> “*I’m fascinated by the idea that although buying online is a really new concept, it’s all motivated by the old-fashioned notion of reputation – the reviews. I would always check somebody’s reviews before I buy off them, whether it’s the second time they’ve sold something or the thousandth time they’ve sold something*.” FG10 female

> “*There was a survey in the UK that 30% of mostly girls under 16 had taken some stupid photographs of themselves and posted them online… It’s mainly common sense, but when you’re young you don’t have a great deal of common sense. So the behaviours are the same but because it’s a bigger forum, the consequences are somewhat more.”* FG9 male

> “*It’s a move on from the conventional ‘hand your cash over, or credit-card’. You do that willy-nilly in a shop – why would it be any vastly different? When you’re not doing that face-to-face you can’t detect all those signs that normally come with a purchase, like a smile or whatever. I don’t see much difference. Most of the sites I deal with are vast multi-national (for good or evil) that can’t afford to have their reputation sullied by screwing up or ripping you off*.” FG10 male

> “*But a catalogue would arrive in the mail and you’d write a cheque and send it away. We’re doing the same thing, we are just doing it more immediately*.” FG4 male

> “*Kids can’t access inappropriate stuff at school, but that doesn’t stop them bringing inappropriate stuff to school. But that’s no different from 20 years ago, when kids brought their father’s magazines to school. It’s the same thing going on just in a different way*.” FG4 male

Although some participants were suspicious of information available online, they had similar considerations with information provided via offline channels.

> “*You have to be careful though. Just because it is online doesn’t mean it is true. It is the same as reading something in the newspaper, you don’t say, ‘OK, it’s in the newspaper, it must be right*.’ FG1 male

Many of the older age-group participants transferred their logic and experience of the way the world worked from their offline experience to the online world.

> *“For someone of my age, it’s quite a hard change to go from someone talking with me and taking me step by step through to the solution to my problem, versus looking at a screen and trying to figure out the jargon on there and going from screen to screen … I have a hard time doing that.”* FG2 female
>
> *“The Internet is like the world, really. We’ve all got the creepy corners and spooky corridors to get down.”* FG2 male

Younger generations behave differently online compared to older generations

By contrast, younger, ‘digital native’ participants simply took the online world for granted as is and did not create any offline translation. Older people often realised that young people are quite different compared to them.

> “*When I was a kid in my room I was reading a book or doing homework. When my teenaged daughter is in her bedroom she has access to the whole world. They’re talking until one o’clock on these websites. We’ve warned her about the dangers of the internet*.” FG9 male
>
> “*At home we only have one computer and it’s in the lounge and the screen faces out so I can see everything that’s happening. If the kids are using it the sound is on… My two-year-old knows how to swipe my phone to open it, and to get to the camera and take selfies! So they’re like sponges*.” FG7 female
>
> *“A staff member I employ in the office, I’ve noticed she’s constantly checking the notifications on her phone. And I’ve had to change my attitude to that sort of response, because she can’t stand not knowing. But she does it quickly and gets back to work. It’s changed my perception with how you deal with staff who are constantly on their phones. It’s not that they’re rude, it’s how they’ve been brought up.”* FG9 male
>
> “*Then I’ve got to try and stop [the children] trying to buy things. I get emails from club Penguin and stuff... My little one is 5, it’s not like he knows how to spell but he knows how to write my email address. So I get this ‘your child wants to go on this Mickey Mouse site’… or especially YouTube stuff – they must be trying to subscribe to certain things. So I’ve got to stop them from using my email address. I keep thinking I should set up a dummy email address so all the rubbish stuff goes in there.”* FG5 female

Some participants suggested a ‘playground’ mentality amongst kids.

> *“I don’t think the kids have enough restraint. They’ll stick anything on there. I think kids should be taught more. Stuff just goes viral and they stick all sorts of rubbish on it. And when they get to party age and getting drunk and doing stupid stuff with their mates, like my son, they stick it on. I say what if you’re going to an employer and have an interview and they’re*

> *going to look on Facebook. And it's blasted all over there – you being a drunk idiot*." FG9 female

> "*Thing that worries me is my nieces, some of the fights they'll have online. And you read it and it's all public out in Facebook. Like the kids don't know when that isn't appropriate. We had an issue where we had a family member die and the kids sent it through Facebook! And we were like – 'that's just not appropriate'. But just the fact that they didn't think it was – that's really hard for me. I know that's their way of communication but some things, for us, it just isn't appropriate*." FG5 female

> "*I reckon a lot of the young people are doing that [things online that they wouldn't do in person]. I haven't seen any older generation do that stuff… It's like bullying, aye*." FG5 female

Also young people acknowledged the difference in Internet use with older generations.

> "*Parents: They are a lost cause really. My dad just joined Facebook a few weeks ago and added me*." FG3 female
> "*Add him to the family list and block what he can see*." FG3 male
> "*I did it straight away*." FG3 female

Drivers of Internet use

Participants used the Internet for a large variety of online activities. The main reasons for using online channels were the ease and convenience of accessing information and services; the opportunity of connectivity, in particular through communication and social networking with family, friends and colleagues, and within online communities; the cost-efficiency of using the Internet; and the time-efficiency and immediacy of Internet use.

Access to knowledge and information

Accessing and searching for information was the most popular online activity amongst participants.

> *"Information is so easy to get and you can get it quickly."* FG10 female

> *"I use it to find stuff. What I need to know. How things work. How things are done."* FG5 male

> *"I use it for information. It's great fun just looking at Wikipedia. From a little bubble in your head you can find out something. I'm involved in visual art, so it's great to see what's happening amongst colleagues and internationally."* FG10 female

> *"Different ideas like for kids' parties"* FG5 female

> *"I've just had a baby, so I've been on the Ministry of Health website. You can look at all sorts of things you need for a newborn.... There's a part called MyHealth with lots of tips for breastfeeding, sleeping and things for the baby. Stuff I wouldn't have a clue about otherwise."* FG10 male

> *"News. Keeping up to date with what's going on in the world. It's the fastest way of doing that."* FG10 male

> *"It's like a magazine, but it's what you want to look for, not the magazine. Nice short stories, short bites."* FG5 female

The large majority of participants used the Internet to search for information. Being able to '*just quickly google it'* is a given for most participants.

> "*A lot of information you can't find in the library, so you go online*." FG6 female

> *"Searching – if the kids have a sore throat, blah blah"…* FG5 male
>
> *"'Trouble-shooting' information – how to sort this out, or health information – 'Doctor Internet'."* FG4 female
>
> *"I would say now the children in our household would mostly use internet for information. The kids always have questions, and sometimes it's hard to answer children's questions, but a simple google search can find it."* FG7 female
>
> *"Being able to access research internationally. I do a lot of genealogy stuff and instead of travelling to Europe I can do a lot of research online."* FG10 female
>
> *"DIY stuff around the house is all on YouTube now."* FG7 male
>
> *"If I've heard someone talking about something art-related that I'm interested in then just go on the Internet. Then that opens up a whole thread."* FG4 male

To Pasifika, the Internet was a critical source of information related to their Island.

> "*I like to look up Island songs and lyrics 'cause you can find a lot of those online*." FG5 female

Participants also used the Internet to support their children with their education.

> "*We've got two kids who are having some difficulty at school, so we've got on to some learning sites for them. And I go on it a lot for research. [The kids] ask me anything so I go online and find that information for them.*" FG2 male
>
> "*Kids use it for a lot of their homework so they don't have to go to the library*." FG2 female
>
> "*My six-year-old daughter is enjoying the learning apps*." FG2 female

Participants who had experienced the Christchurch earthquakes, but also others, used the Internet to look up critical information about earthquakes.

> "*After the earthquakes I spent a lot of time watching where all the earthquakes were*." FG4 male
>
> "*The app on the phone that would tell you… that was a 4.6…*" FG4 female
>
> "*For a period of time we were very linked to that.. 'cause if you looked at it and it was under 5…*" FG4 male

The Internet was also fulfilling more immediate information needs, according to several participants.

> "*It also fulfils that need to know now. Finding out what the [Napa Valley] earthquake is tomorrow morning when the newspaper comes out is not sufficient anymore*." FG4 male
>
> "*It's the immediacy of the information. You don't even need to know what the question is – you can just throw random words at Google and it gives you information*." FG4 male

A few participants also pointed at the bad sides of having information immediately available online. For example, one participant described a story in the newspaper about a young man who was killed in a car crash after a party, and friends had the news up online and spread before even the family was aware there had been a crash.

Communication

For the large majority of participants, communication was one of the most important reasons to use the Internet.

> *"For me it's definitely communications. I have a lot of friends around the world and it means that you just forget about the fact that there is 3000km between you: Skype each other and they are right there."* FG3 female

Many participants discussed the cost-efficiency that comes together with the convenience of using the Internet to connect with people.

> *"When my family went away to Holland, they just had to do a couple of things on the laptop and we were in contact all the time. And it hardly cost anything."* FG1 female
>
> *"Keeping in touch with people. Not just email but Skype – a lot cheaper than calling."* FG10 female

For Māori, the Internet was an important tool to connect and communicate with the whānau and iwi – wherever they are.

> "*Someone wrote out a history of our meeting house, and we were going to print it all out and post them out – what a hassle! So last night I just pdf'd it, put the link on Facebook and there it is, have it, it's out there. And now I don't know how many people have accessed it – from all around the world. I've got messages from people all around the country and overseas who've got it*." FG7 male

Communication was also a critically important feature of Internet use for Pasifika.

> "*Where we're situated it's quite isolated. And that's our comms to the rest of the world*." FG5 female
>
> "*They couldn't get hold of me when Dad passed away. I wasn't on the phone or the email. So my sister did a blanket email to our little island – 'anyone on this island who can get my sister to call me urgently'. Oh yeah, I got like 5 calls*." FG5 female
>
> "*When Mum left her bag somewhere. I thought I'll text people. Or then I'll email, but I didn't know everyone's email. So I thought I'll put it on Facebook – 'mum's lost her bag with all her pills. It will cost heaps to replace them'. In ten seconds I got a reply saying 'they're here'… It's the fastest way to get out some information*." FG5 female

Asian people also communicate online with their family and friends in their own language:

> "*We have WeChat for talking to people face to face [via the Internet]. You can use your data – it's much cheaper, and you can see the people*." FG6 female

Young people liked group chats with multiple people at the same time.

> "*You can be having Facebook chats with multiple people so everyone sees everything at the same time. Whereas with texting you have to send it to each one individually. You can do group texts but then the others can't see the replies other make. Same with email*." FG3 female

Social networking

Most participants talked about the critical importance of social networking in their daily lives. The large majority of participants used one or more Social Networking Sites, such as Facebook, Twitter, Skype and LinkedIn, to connect with family, friends and colleagues, or even with individuals and communities wider afield. Also messaging service apps were used by several participants.

> “*When I wake up in the morning, I log onto Facebook, scroll through to see what’s happening*.” FG3 female
>
> “*I’ve just started on Facebook. My whole family is on there. And Skyping too. You can talk to the whole whānau. That’s been a good one*.” FG8 male
>
> “*Certain communities aren’t available locally or even nationally. Even if they are you can expand those communities exponentially [through social networking]. I have a strong interest in photography*.” FG10 male
>
> “*I enjoy the Whatsapp messaging service on my phone. I’ve got a sister in Dubai, another in Sydney, my mother up the road. We can set up messaging groups and send photos and stuff. Whether it’s completely and utterly private, I don’t know. We don’t post anything too personal on there, but it’s a nice message service that we use every single day to say hello, and how are you going, and share a photo*.” FG10 male

Some participants used social networking for promoting their business or sharing community notices.

> “*Our company puts ads on Facebook. And then I’ll go on and share it with my friends if there’s a promo going on. Or ‘like’ it, when a lot of people can see what you’ve liked*.” FG9 male
>
> “*One of the girls has got our [company] site on Facebook, so it can do promotions*.” FG9 male
>
> “*I put community notices on too, like if the breast-screening truck is coming*.” FG9 female

Social networking use amongst older participants was fairly minimal. Some had tried and then left.

> “*I’ve got family on Facebook and they put up pictures of the kids. That’s what I’m mainly interested in on Facebook. I got bored with Twitter. I don’t bother with Twitter anymore*.” FG1 female
>
> “*I signed in to [Facebook]. But I don’t have the time to play with it… I can see the potential there for communication with people you otherwise wouldn’t see. It isn’t possible for people in Auckland to have a cup of tea with you*.” FG1 male

Some participants considered the use of social networking as a distraction or even as a waste of their time. A few of them tried to avoid Facebook as much as possible as it was offering too much information to them.

> “*Can see what someone had for breakfast*!” FG9 male
>
> “*I go on there for information on what my friends are up to, but I avoid it often because there’s too much information about what my friends are doing every second of every day*.” FG10 female
>
> “*I try to avoid Facebook as much as possible… [Facebook] is just too much information*” FG7 male
>
> “*I don’t use Facebook anymore. I look over my wife’s shoulder if I need to know what people are doing. She’s on it all the time. I see enough people and interact with enough people, I don’t need the distraction. So that’s my privacy setting!*” FG9 male

Online entertainment

Many participants were using the Internet for online entertainment.

> “*Certainly entertainment. Lots of TV shows and other things. Between what I can access on the Internet and MySky at home, I don’t think I’ve watched an advert all year*.” FG10 male

> “*Once we have movie night we go on to a movie site and watch a movie off there – at least once a week*.” FG5 female

Several participants described how online games were a regular activity for the whole family, often with some monitoring of the parents involved.

> “*I’ve got a 13-year-old, a 12-year-old, an 8-year-old and a 3 year-old. All of us are on the internet every day. My 13-year-old and my husband use the Playstation with the Internet for their game [like Modern Warfare and Call of Duty]. You can actually call up other people and talk and play the game. They’ve also got the Playstation Vitas, which gets the Internet too. Plus all the other little devices the kids get. The 3-year-old uses it for games but not Internet related games – just in case she taps on something while she’s on the Internet and brings up something I don’t want her to see. So she’s the only one not on the Internet. The others are allowed on the Internet but only on certain sites and I block off all the other ones. And they’re only allowed on at certain times. But they take [the Vita] into their rooms… They’re not allowed on Facebook until they are 16*.” FG8 female

> “*With the younger ones, it’s trying to find safe sites [for game help] for them especially on YouTube. They’re in to big things like Minecraft… Some of the guys on the YouTube videos have really good information but they’re swearing all the way through it and I have to find a site where the guy’s talking and his language is modified. Sometimes I comment on them and say ‘you know my kids like your site, lots of information, but my kids are this age so could you tone down the language’. Some of them tell me to eff off*.” FG5 female

One older participant played an Internet game (Minecraft) with her grandchildren based in New Zealand and the United States as another way of socially connecting with them.

> “*I’m not very good at the game…For me that’s a good way to have some connection. Because there aren’t a lot of things in common between the generations when one is computer literate and one is computer illiterate*.” FG2 female

Purchasing online

Most participants have had at least some experience with the online purchasing of goods or services, or paying bills online. However, for a variety of reasons, participants usually were selective in what they did online.

> “*For me shopping online is much easier: you can open up lots of websites and you can see lots of the goods you want. You don’t have to go to specific stores to pick up. Comparing process is so much easier*.” FG3 female

> “*I don’t think I’ve bought an item of clothing in a shop for about two years. There’s a few sites that once you know what their sizing is like, you can go to town. The prices are so much cheaper than the shops here. They’re insanely cheaper, and the range … It becomes semi-addictive I guess – once you figure out you can buy three pairs of these jeans for the same as one in the shop you end up going back and buying another pair*.” FG10 male

> “*I bought a car and a boat. The boat was direct with a boat place in Auckland, the other was an ex-rental car place. They take photographs and send you all the information. I said I’d buy it and they sent it down to Wellington for you… I had driven that same car type at a*

> *dealership, so I knew I wanted that car. It had a full warranty and all that sort of stuff*." FG10 male
>
> "*There's a book series I followed when I was in Ireland that you can't get here. So those things I'd buy online. And likewise for the shopping. There's a lot of things I used to get over there which I can't get here – so it brings the world a bit closer to have things shipped to you*." FG10 female
>
> "*Booking.com is fabulous when you're travelling. You can book a place a couple of days in advance*." FG10 male
>
> "*I don't [buy online] because I morally feel it's a bad thing to do. But I'll re-order something online that I've got from a shop, like shoes. But most of the time I prefer to try things on*." FG10 female

Some participants wanted to support the local economy and did not buy particular goods online for that reason.

> "*One thing I won't do is buy books online, because one thing we've got to do is support our local bookshops otherwise they won't be here. You can get them from the book depository at half price and sent to you in five days, but I'd rather go to our local bookshop and support them*." FG10 male

Several participants pointed at the cost-efficiency of using the Internet for shopping.

> "*I download a lot of my books online. Find a lot of the free ones that I don't have to pay for. It's amazing what's free out there if you have a look*." FG5 female
>
> "*You don't have to spend money travelling to the shops. They just post the things to your door straight away. Sometimes you can order things from Australia or China and it is much cheaper than shopping locally*." FG3 male

Free shipping was mentioned by several participants as a means to save money.

> "*A lot of sites offer free shipping as well. So the item ends up being much cheaper than if you went to the shop. We live out of town. Just paying for the train to get into town costs a lot and more than shipping. And the exchange rate also helps so that it is much cheaper to buy something online*." FG3 female
>
> "*I think some New Zealand domain stores have a bit to catch up with overseas sites. The sites I go to might ship from Hong Kong, and I don't know if the shipping price is embedded in the cost, but I generally get free shipping. That feels great to me, especially knowing that it's coming from overseas. Yet to buy something from the Warehouse, a one day sale when you think that's a good price for $19.95, and then it's like $27.95 because there's shipping costs on top. Then you buy another two of them and it's another $7 and it's in the same parcel when you get it!*" FG10 male

Some participants mentioned the discounts they were getting when they buy goods or services online.

> "*It's often cheaper to do it with them [airline's web site] because you get a cheaper fare. There's a lot of discounts*." FG1 female

A few participants however have had a bad experience and decided to stop buying things online.

> "*I was doing online buying and we had a little scare where people were hacking into our credit card numbers so I just stopped it altogether.*" FG8 female

Trading online

Several participants also had experience with online trading. Most of them were on TradeMe, but also other sites were used.

> "*We've got a PreLove site on Facebook. It's called PreLove but you can buy and sell stuff within the local area. It has really, really good bargains and I'm on there every day*." FG8 female

One participant had set up an online store as part of his business.

> "*Our business has an online store so that's good. People are buying and selling and placing orders online. Often the invoices will come back online*." FG9 male

Online banking

Many participants liked online banking for its ease and convenience, and considered banks to have secure sites.

> "*Convenience for banking. Online is much faster and easier*." FG6 male

> "*Banking. I haven't been into the bank for ages*." FG5 male

> "*I just got sick of standing in queues just to move ten bucks from this account to that account*." FG1 female

Some however, in particular several older participants and those who have had a bad experience, did not trust online banking and preferred traditional channels.

> "*It's just easier… I've used online banking for ages. My husband won't use online banking but that's only because he's had a bad experience with a bank once that the money went out and it wasn't supposed to… But nothing's ever happened to me so I'll keep doing it*." FG8 female

> "*I want to go to the bank and see what I'm getting*." FG1 male

> *"[It's scary that] my personal details are in there. And from what I've heard and seen people can hack in to there*." FG8 female

> "*I prefer the face-to-face thing when it comes to something like [banking]*." FG8 female

Applying for jobs online

Several participants described the convenience and time-efficiency of applying for jobs online.

> "*I don't have to get out in the car to do things. There are so many websites I can go on to apply for work. I applied for five jobs in one day and got two responses*." FG2 female

Online government transactions

Many participants had experience with online government transactions, such as doing their tax return online, applying for a passport or visa online, registering a vehicle online, using RealMe or managing their student loan. Most participants pointed at the convenience of these online government services.

> "*Convenience for IRD returns or even paying for a passport. Online is much faster and easier*." FG6 male

> *"Doing PAYE returns online is much easier because it calculates it all for you and lays it out on the document so you don't have to do multiple writing out and filling in."* FG9 male

> "*When I was doing our last one [PAYE return online], they had all the information there anyway – what did they need me for?"* FG9 female

> "*Paid the rates online. It's convenient not having to go down in person.*" FG5 female

In general, participants felt comfortable about sharing their identity information with New Zealand government agencies online. Some also pointed out that the New Zealand government could do a much better job in promoting existing online services.

> "*I think the government agencies are doing some good things already, like they ask you questions to check who you are*." FG6 female
>
> "*I think now the IRD will record your voice when you ring up. So next time they will match your voice and know it's you… I think that is very good in terms of government agencies*." FG6 female
>
> "*This whole RealMe setup I think needs a lot more promotion and that could make life a lot easier as well, if people knew what that was and how to use it. Have you guys heard of RealMe* [directed to other participants]? – couple of others said no, so then an explanation was given as "*a government identification system that could evolve into something quite good*". FG9 male

Most participants trusted New Zealand government sites more than other websites.

> "*Government you automatically trust more because you expect they're going to have that extra security. Even though they do have failures, they can't really afford to jeopardise that sort of thing*." FG9 male
>
> "*I think for me the only site I'd trust is to do with New Zealand government departments… and TradeMe, but only those ones." Why trust TradeMe? "I've used it for years and I've never had any issues*." FG2 male

Some participants also had a good experience with online government transactions overseas.

> "*I had to get my English passport renewed, and that was one of the easiest things I ever did online. I went through page by page, and half an hour later they sent an email confirming 'your account has been debited'*." FG1 male
>
> "*I did an Australian visa online very simply, in about half an hour. I found the form and printed it off and then took it in somewhere. I had no problem with that*." FG1 female

However, online government transactions were not always that easy for participants, and sometimes pushed them towards other channels.

> "*I've tried doing passport renewal. It looks pretty good. I sat with a consultant from Immigration. What was frustrating was uploading the photos…. But other government websites like for tax returns – it'll take you from one page to another then another and by the end of it all – ring! It's frustrating. But I do the kids StudyLink online for them. I've got their passwords. Actually I set it up for them and I do all of their applications online*." FG5 female
>
> Referring to government websites "*They've got ten pages of stuff [to fill out]. By the time I do that I could walk up to town and do it. I haven't got time for all that*." FG1 female
>
> One participant was learning about Immigration NZ in order to become a volunteer with Citizen's Advice Bureau. She found you have to move from place to place, then find the right forms and whether they're going to do what you want.
>
> "*There's nothing that says 'if you need a visa it's going to cost you this'*." FG1 female

Also, searching for government information online was not always easy, as several young participants pointed out. They made comparisons with online banking and Facebook and wanted Studylink to be as easy as them to use.

> "*It's much harder finding information about that on the Internet. If I didn't know something about my Student Allowance I'd just go to Studylink and ask my questions and they just tell me*." FG3 female

Digital service design assumptions held by government agencies were not always in accordance with user experience or user expectations.

> "*There's a social welfare site as well, obviously. I was on it but then they changed it and you had to have a New Zealand cell phone number to access it. And I don't have a cell phone.*" FG8 male

> "*Oh yeah, they send a code to your phone, and it's stupid when your phone is flat*." FG8 female

> "*But I'd rather ring [StudyLink] up and get stuff done through them rather than going online. It's ring them up and get it sorted rather than waiting a week for them to reply to something*." FG8 female

> "*StudyLink. They're useless. Heaps of emails and then you end up calling them*." FG3 female

Online dating

A few participants, in particular young people, indicated that they have used the Internet for online dating.

> "*It's a bit personal but I've given out my information to dating sites…I've trusted it enough to give all my information to them. It hasn't worked out [the dating], but they've still got all my information*." FG2 male

Several young people have used the online dating app Tinder.

> "*My guy friends will go into town and they will get out their Tinder and click 'yes' on absolutely everyone, just to see what happens. Guys usually take the piss out of Tinder quite a bit*." FG3 male

> "*My friend has had boyfriends from Tinder, and they have been lovely*." FG3 female

> "*It's not for stalking purposes. You just check out people, for entertainment*." FG3 female

Sharing identity information online

Context matters for sharing identity information online

Participants explained how they make fine-grained assessments about online information-sharing depending on the context and the organisation or individual they are sharing the information with. Trust was an important condition for sharing their identity information online. They applied a rough categorisation of different levels of online relationship.

> "*You're not going to be sharing the same stuff with your family as with the IRD*." FG4 female

> "*It's about trust and who you are dealing with*." FG2 female

> "*You assume you can trust the government agencies – falsely or not – and you would tell them more*." FG4 female
>
> "*I don't question it if the department of stats is asking for [your income]. You just put it in. So it does depend who it is, and are they what they say they are*." FG4 male
>
> "*I'm in the process of getting a birth certificate, so I'm giving my information to Internal Affairs. So I've got no problem to a certain extent, but I won't give my bank account details to someone I don't know*." FG2 male

A good example of how context, trust and relationship matter for sharing identity information online, was provided by a few participants who shared their identity information online with their partner so that they were able to track their behaviour. These participants only saw the convenience of these information-sharing arrangements.

> "*Even five years ago you'd put things into your Outlook calendar and say here's what I'm doing. Now that's uploaded to a cloud and my wife can check on the iPad and see what I'm doing in my calendar*." FG4 male
>
> "*We use [Google+] locations… so I can see when [he] is on his way home and I know where to be at with the dinner. It's that whole 'up-to-date-ness', isn't it*? *That was very handy after the earthquakes because I was very reassured to know where he was. And if a building went down and he was in town, I'd know what building he was in…. Yeah, if he's moving it's a good sign*." FG4 female

Understanding the value of information

Several participants understood the value of information nowadays and treated online transactions as situations of give-and-take where both sides benefit.

> "*We're in the information age. Information is valuable to companies – they're willing to pay for it. But information is valuable to us as well – so that we can get what we need as fast as possible too. It's the era we're in*." FG4 male
>
> "*I'm pretty [mercenarily] motivated I guess. If there's a reward for me at the end – and there really is a reward – you can pretty much get whatever you want from me. If I don't see the value in signing up or subscribing, I won't. I see it as, if you want something from me, what are you giving me? Then it's on me – if I've chosen to subscribe, then I've given you my information*." FG7 female

Some saw the gains from the online exchange falling purely on one side.

> "*That's the crux of the matter. It's all to get money out of people – financial gain, there's no other reason for it. Nobody's really interested in what you feed your dog for breakfast but they're interested in getting ten dollars out of you*." FG9 male
>
> "*Anyone is just as likely to sell my details to someone else so that I end up getting a whole lot of rubbish in my inbox. So I won't put my details on*." FG9 male

No individual choice but to share identity information online

Many participants felt that they often do not have a choice other than to provide their identity information in a variety of online transactions: if they wanted to use the site, they needed to share their personal information.

> “*I’m certainly cautious about what I put in, but sometimes you’ve got to. It’s a bit of common sense about whether you want to use the site or not*.” FG1 male

> “*A lot of sites when you order, say you have to give this information. You can’t go on to the next step until you’ve done that asterisk thing*.” FG4 female

> “*Sometimes you can’t fill in some of those fields because they don’t apply to New Zealand, and then there’s a song and a dance at the bottom – ‘you haven’t filled the field in’. So I just give up*.” FG1 male

Participants understood that some information-sharing was critical in order to successfully complete the transaction.

> “*You don’t have a lot of choice these days [with the information you put online]. I ordered something from eBay the other day, but if you don’t put your name and address how’s the thing going to come to you? It duly arrived in a couple of weeks – it was wonderful*.” FG1 male

> “*But if you’re buying something you have to give your address… That’s the thing with purchasing you have to put your credit card on and then some of the sites are asking for those three digit security numbers. I’m not sure about this one. Isn’t it meant to be with me – with my credit card? Because once you give them out, if anyone wants to clone your credit card, they’ve also got your security number off the back. But a lot of reputable places ask for that, so they must have a reason for it*.” FG4 male

A few older participants thought it doesn’t really matter what information they share online.

> “*I don’t think it matters terribly. I don’t have anything to hide*.” FG1 male

A few participants explained that they felt obliged to use a particular online channel because all their friends were using it.

> “*That’s why I’ve stayed on Facebook and haven’t deleted my account, because some of my friends can’t fathom the idea that someone isn’t on Facebook so I can’t get invited to things, like 40th birthdays, if I’m not on Facebook. I’ve found it easier to stay on it for that, but not much else*.” FG10 female

Several participants pointed out that, in many cases, if they downloaded and used an app on their smart phone, they were implicitly giving permission for that app provider to use their identity information, such as personal contact details.

> “*Initially you feel bullied in to it…You’ve given up a bit of yourself as far as individual choice is concerned. And you do get to the point that you either have to accept that either they have the potential to throw more of your information out there, or I just can’t use this app anymore. You still have a choice – use it or don’t use it*.” FG4 male

> “*They won’t give you a choice – do you want the app or not? You end up giving in to them because they’re all the same – they all want your [contact] details*.” FG9 male

> “*What do they [apps providers] need that [contact] information [on your phone] for? It’s just marketing*.” FG9 male

To some, this ‘forced information-sharing’ was an important reason why they will not download certain apps to their smart phone.

> *"So I go – no! There'd be some [apps] I'd use but I wouldn't allow [them] to have access to everything on my phone*." FG9 female

Forced information-sharing also applied when a Facebook log-on was required in order to undertake activities online, such as signing a petition or work-related activities, as a couple of participants have noticed.

> *"I find it quite annoying that you're being forced to use a particular product to be able to communicate for different things. It's annoying because I like to choose in terms of consuming. The Internet has definitely created a more accessible consumerism but these big corporations like Google, Facebook do monopolise the Internet. So it's not allowing us as much choice*." FG4 female

> *"Up to a point you think, oh no I'll resist this, I won't do that. Like if you want to continue messaging in Facebook you have to go to this new messenger app. They are not going to allow you to use Facebook to message. If you want to use it – accept it*." FG4 male

> *"I don't generally mind joining up to Spotify or other things with my Facebook account, but I'm loathe to bombard my friends with 'Bob's just listened to this song', or 'Bob's just done that'. That's the difficulty – do you turn it off at the Spotify end or the Facebook end. That's how they get you with that. I don't want to be one of those noobs who doesn't know what's going on – and every song I listen to gets posted up on my friends' wall*." FG10 male

Too much information being asked to share online

Many participants, in particular those of 35 years and over, commented that they are often being asked to share too much identity information. This situation applied to a variety of online transactions.

> *"There's the classic NYDB – None of Your Damn Business. Like when you put an application form in to say borrow money to get a bed from Smith City, they've got all these personal questions! I just want to borrow this, for this. Why do you need to know the name of my cat and how much I earn … Just put in NYDB*." FG4 male

> *"Those generic questions are alright – like, 'did you find this information useful? Yes or No'. But as soon as they start asking personal information that's a bit much. Though it does depend on who's asking and I'm a bit anti-establishment. I don't want to help big power companies out with their marketing research so that they can target their advertising to us. But if it were a government agency or a charity asking a question, I might be a bit more flexible*." FG7 female

> *"I find with Facebook it's got all these updates – update your profile. It's got all these little captions things – you're friends with so-and-so. I'm not interested but it's coming at you, prompting you to finish off your profile. 'You're only 72% completed'. I don't. I just go on Facebook to see what's going on. It's starting to get annoying."* FG5 female

Older participants particularly believed there was too much information-sharing requested. Most participants agreed that when it is too intrusive they just stopped and got out of the online transaction.

> *"There's too much of your information out there anyway. I just don't bother [by not providing any more information*]." FG1 male

> *"Even things in the government website. Sometimes I won't even go there because it asks you lots of questions*." FG5 male

> "*I sometimes draw the line at credit card information. I was going to sign up to LightBox for a free trial but before you can continue you need your credit card. Nah, pass. I did one where I signed up for a year's subscription of a British newspaper. But I obviously didn't read the terms and conditions properly and didn't tick a box which said I didn't want to continue this next year so suddenly on my credit card was a bill for another hundred and forty dollars for another year's subscription… It's a cunning move*." FG7 male

> "*Blowed if I'm going to give you personal information just so I can know if it's going to rain today*." FG1 female

> "*Doesn't happen if you go into a shop does it*?" FG1 female

Private information being asked to share online

Participants did not like organisations to ask for their private information in online transactions. Usually, this was a reason for them to stop the online transaction or not use that particular site.

> "*I tried [online shopping] once but I stopped because it asked me something I didn't want to share, like bank details*." FG8 female

> "*When you're signing up for a site I'm always dubious when they have to know your birthday and things like that. I don't mind them asking what month you were born in, but specific information like birthdays I don't like... I would think twice about joining the website*." FG10 female

> "*We're going to France next year and I've been booking lots on AirBnB. They wanted to validate who I was by sending them a scan of my driver's licence and passport and I didn't do that. It's the first time I haven't done something. I just didn't feel at all comfortable about scanning my passport or drivers licence*." FG10 female

Lack of transparency

Without exception, participants had difficulty understanding how organisations process or use the identity information they had provided online.

> "*Now Flybuys has my telephone number. I don't know how they do that. How do they do that? So I asked to be taken off their calling list*." FG2 female

> "*What I do have a problem with is when I've made some donations online. For some reason my information gets passed around other organisations and all of a sudden I've got a big influx of 'would you like to make a donation'… I don't know how that information got passed on… I'm a bit wary when it comes to that sort of thing*." FG2 male

> "*When I was doing our last one [PAYE return online], they had all the information there anyway – what did they need me for?*" FG9 female

> "*A lot of sites would ask you if you have a Gmail or Facebook account, and I used to click, Yes, until I realised that all the information I have on Facebook then goes to this company. And how many people actually make that connection? So there's consciously handing over your information, and then there's unconsciously handing it over because of speed or not clicking something.*" FG7 female

> "*On Facebook I only have my name and a couple of things. But I noticed the other day they had filled in some things that I didn't necessarily check*." [Connecting with some people about a reunion led to 'graduating college' being filled in] FG2 female

> “*What do they [app providers] need that [contact] information [on your phone] for? It’s just marketing*.” FG9 male

> “*There’s those pop-ups that say you’ve won a 50 inch LCD TV… well I clicked on the X to get rid of it and it automatically takes you to that site!*” FG8 female

One parent was alarmed that advertisements for dating sites in Asia popped up on a kids’ game site.

> “*Children shouldn’t be seeing that*.” FG2 female

Also young people had difficulty understanding what is happening with their online identity information.

> “*I am probably going to provide my details anyway but sometime you wonder if the information you provide is going to be used against you. Particularly later in life*.” FG3 female

> “*I want to know whether the information I provide is confidential or not*.” FG3 female

Social Networking Sites ‘owning’ your information

Several participants indicated that they posted less information now on Facebook than previously. One participant also had uninstalled the Facebook app from his smart phone because he had heard from a friend that Facebook used a clause that they could get all contact information from your phone.

> “*When I learnt that whatever photos you uploaded to Facebook then belonged to Facebook – I took issue with that, and I’ve only just come back to Facebook after a long time away. I’m more cautious now especially around the children and what I post of them*.” FG7 female

> “*A lot of sites would ask you if you have a Gmail or Facebook account, and I used to click, Yes, until I realised that all the information I have on Facebook then goes to this company.”* FG7 female

Another participant recounted how a friend’s photo posted on Facebook was subsequently used by Facebook for advertising for online dating:

> “*But that’s the reality when you put photos on Facebook – you’re signing those rights over to them*.” FG7 female

Permanency of information

Most participants were aware that their information, once published, continued to be available online. Some also had received confirmation by trying this out.

> “*I typed my name in to Google, and oh my gosh, all my details came up. That was really spooky. You just put a photo in there once and you think you’ve deleted it, but it’s still stuck in there! I’m rather new to the internet*.” FG8 female

Several of them had adjusted their information behaviours and were not so worried therefore about the implications of this permanency of information for them personally. However, some were concerned about the information behaviours of their children and the possible implications for them later on in life.

> “*Employers might look at your Facebook, but they’re not going to spend three hours trawling through old photos or looking at some of your comments… If you’re careful with just the initial [obvious] stuff you’ve got out there.*” FG4 female

> “*It’s really handy if I’m thinking of hiring a staff member. Facebook – bang the name in there… It’s too easy to find information about people. It’s great when I’m employing a person, but at the same time it’s my information too.*” FG4 male

> “*We try and counsel the kids that it might seem fun now but that it stays there*.” FG4 female
>
> “*I don’t think the kids have enough restraint. They’ll stick anything on there. I think kids should be taught more. Stuff just goes viral and they stick all sorts of rubbish on it. And when they get to party age and getting drunk and doing stupid stuff with their mates, like my son, they stick it on. I say what if you’re going to an employer and have an interview and they’re going to look on Facebook. And it’s blasted all over there – you being a drunk idiot*.” FG9 female

Multi-channel behaviours in online transactions

Many participants talked about their multi-channel behaviours in online transactions. Most would look up information online, before deciding to enter into a transaction.

For some, online wasn’t always quick enough or provided them with the service they were looking for.

> “*I’d rather ring [StudyLink] up and get stuff done through them rather than going online. It’s ring them up and get it sorted rather than waiting a week for them to reply to something*.” FG8 female
>
> “*StudyLink. They’re useless. Heaps of emails and then you end up calling them*.” FG3 female
>
> “*I’ve tried doing passport renewal. It looks pretty good. I sat with a consultant from Immigration. What was frustrating was uploading the photos…. But other government websites like for tax returns – it’ll take you from one page to another then another and by the end of it all – ring! It’s frustrating*.” FG5 female

Several participants indicated that, after they had looked up the information online, they would do the actual payment over the counter or via telephone.

> “*It’s just an information thing. I switch the money about but I don’t do any actual banking online*.” FG1 female
>
> “*I quite often check up on the Internet for something. If it’s in New Zealand I’ll phone them and order it and give my credit card details over the phone*.” FG4 female
>
> “*I used Internet banking to check my balance… I wasn’t going to use it to transfer money or anything. I could push the wrong button and send it to the wrong place. I’m a bit paranoid about that. I’d rather do it over the phone*.” FG8 male

Online privacy

Without an exception, privacy was of importance to all participants, including young people:

> **“***On Facebook, if you like things then ads will come up for it. So I just stopped liking things*.” FG3 female

Most of the older participants were very careful in sharing their identity information online and preferred to keep it to a minimum:

> “*The only site I have ever put my details on is RealMe. I needed to do that to get the information I wanted for family research*.” FG1 female

Financial information is often considered highly sensitive information

Many participants and in particular Asian people indicated they consider financial information as highly sensitive information.

> “*I try to avoid paying anything online… I’d rather give them cash. I’m not keen to do online shopping*.” FG6 female

> "*As long as it [government site] doesn't ask me for bank details I'm all good*". FG8 female

For some, this was a reason not to buy anything online.

> "*I won't buy anything online because I won't put my credit card details online. You read in the papers and hear on the news about all these scams going on … so I don't buy anything because I don't want to put my credit card details online*." FG1 female

Or to do their tax return online.

> "*Talking to them [IRD] is safer*." FG6 female

Other types of private information

Several participants however considered other types of identity information, such as their children's names, phone number or home address, as even more private.

> *"With your bank information you could go in to the bank and change it, but your private information – like your kids – you can't really change that*." FG2 female

For many participants, sharing photos was mostly restricted to family or friends.

> "*Photos for me: I only want my close friends to see my photos*." FG3 male

A few participants talked about a bad experience with online photos from family members or friends. One story was about a friend who had posted his photo on Facebook. This photo was picked up by Facebook and used for advertising on Facebook for online dating. The other story was about a participant's niece who had been photographed at Kapa Haka for a newspaper. Then Destiny Church picked up the image off the paper website, and the photo was also picked up by a cruise-ship travel agent.

> "*She's 22 now, but was six at the time. And to be a face of Destiny Church or an international cruise line, is shocking to me. I feel so gutted about her privacy at the time. It's yuk*." FG7 female

Other types of identity information that were not shared online include the following:

> "*You don't tell anybody your passwords*." FG3 female

> "*I wouldn't share my liabilities between banks*." FG9 male

> "*We wouldn't share details about our suppliers online because often we would have special arrangements with them that someone else could cotton on to*." FG9 male

Trading off privacy against public safety

Similar to trading off their privacy for convenience, several participants indicated they are willing to trade off their privacy for enhanced public safety.

> "*My general feeling is that if somebody wants to hack in to my personal information, as long as they can't get hold of any payment information, I don't give a damn. That risk is the cost of convenience of using something like the Internet. The same with the GCSB – they can look at my metadata as many times as they want because I'm not doing anything wrong. In fact the more people are looking at, the less attention they're likely to pay to me. And if they catch one or two people doing things they're not supposed to – great outcome.* " FG9 male

> "*I think if they can watch people like potential Isis members, then that's good for all of us*." FG9 male

> *"The GCSB thing in the election was quite interesting, because people were talking about that fifteen years ago. That if you sent an email to the United States and mentioned 'bomb' and 'terrorist' or a few other things, you were going to get screened. So we all used to send those messages! I don't think anyone was particularly surprised that security services were on the lookout for people doing that stuff. The media obviously thought it was a big deal*." FG9 male

Preference for privacy-friendly sites or apps

Several participants indicated that, as much as possible, they prefer to use more privacy-friendly sites or apps. For example, Asian participants prefer the more privacy-friendly social networking site WeChat over Facebook.

> "*We all use it [WeChat]. We like it because you are more in control.*" FG6 female

> "*On Facebook, if I become a friend of a friend, then I can see all of her friends' posts, and all her friends can see my posts. I don't like that. There is a lot of junk postings and I have no choice [with Facebook].*" FG6 female

Online security

Security concerns over Internet use

Although participants used the Internet frequently, they were not unconcerned about the security of their online identity information, with the exception of some of the younger 'digital native' participants.

> "*I went to a bank and they encouraged everybody. Practice what you preach. And it's actually much more convenient for me to do online banking… But I still find that scary. They say it's secure but I've not changed my username or password since I started and that's nearly 20 years. And I hear these horror stories of hackers and they can calculate the key strokes or whatever. And that's scary. I haven't had any problems yet but, you know, one day*." FG5 female

> "*You want to enjoy the convenience of the new technology, but if you are going to think about the many, many risks… you stop using it. I don't know, where's the balance?*" FG6 female

> "*I've purchased things on the Internet and I've used my credit card and I have never had any problem. I do have a concern [about security] but I always make sure that the lock is on for security. I always check that. What else can you do? Otherwise it's not much use, is it*?" FG1 male

> "*I'm just getting used to the idea of online banking. I'm not that happy with my information being online – statements and stuff… I'm just a bit wary of that*." FG2 female

> "*It's down to you to feel safe. You can avoid all that danger by not going on the site in the first place*." FG2 male

> *"I worry that when I click on a site a virus is going to come in to my computer. I never used to be big on anti-virus but now I actually spend money for Norton….. I used to just get the free one, then another free one, then another free one. But I found the computer was going slower and stuff was popping up all over the place."* FG5 female

Security awareness

Several participants demonstrated that they knew where to look in order to feel safe online.

> “*That’s the thing with purchasing you have to put your credit card on and then some of the sites are asking for those three digit security numbers. I’m not sure about this one. Isn’t it meant to be with me – with my credit card? Because once you give them out, if anyone wants to clone your credit card, they’ve also got your security number off the back. But a lot of reputable places ask for that, so they must have a reason for it*.” FG4 male

> “*I’ve purchased things on the Internet and I’ve used my credit card and I have never had any problem. I do have a concern [about security] but I always make sure that the lock is on for security. I always check that. What else can you do? Otherwise it’s not much use, is it*?” FG1 male

> “*I usually leave everything logged in on my phone, but now I have put a pin on it so they can’t get in*.” FG8 female

Several participants were also familiar with credit card companies ‘x-ing out’ parts of their credit card numbers during and after transactions for security reasons.

Young people particularly were not only strongly aware of security issues online but also demonstrated relevant expertise to assess online situations.

> “*My parents say ‘never real name; never do blah, blah blah. They are like security, security! I just dismiss it because I think ‘you don’t know anything about Facebook*’. FG3 female

> “*I figure everything is potentially discoverable’ If you want to find out something about someone, it is not that hard. The password you have on Facebook is not going to change that*.” FG3 female

> “*If someone wants to find out about you then they are going to find out. I know security is not that strict so on Facebook, I just don’t put something up if I don’t want someone to find out about it*.” FG3 female

Lack of understanding of online security

A few participants, particularly those with low education or limited Internet experience, demonstrated a low understanding of online security issues.

> “*I’m a bit iffy about [lottery winning emails] because they could be a scam.”* FG2 female

Some managed this lack of understanding by an attitude of ‘*nothing to hide, nothing to fear*’.

> *“Anyone who wants to hack into my email would go to sleep with boredom.”* FG1 female

> *“My life is an open book … I’ve got my family tree on there. Anyone is welcome to go on there and add stuff to it. They just can’t take stuff off.”* FG1 female

Experiences with cyber(-enabled) crime

Actual experiences

Participants reported the following actual experiences with cyber(-enabled) crime.

Several participants had bad experiences through online shopping:

> “*I’ve gone to this site and thinking it was the business for NZ Rugby and I wanted to go to the All Blacks site. And I went there and it said official All Black site but I didn’t realise it wasn’t really the official All Blacks site because … it’s just some outfit in Denmark… and I’ve got myself stuck because I wanted to purchase live rugby. I purchased something. I purchased live international sport so now I’ve got soccer and hockey from the northern hemisphere. It’s not what I wanted*.” FG5 female

> "*We bought some graphic images off a company once. Three months following that they billed us again for another set, and three months after that for another set. So we contacted the credit card company and apparently it was happening worldwide. So it does pay to be wary*." FG7 female
>
> "*I think our laptop had a virus or something that takes information. We bought something online – and I'll never buy anything online again – but someone managed to get that number and bought something for 150 bucks. I saw it as a purchase that got done in America. But the bank was good because they refunded the money*." FG9 male
>
> "*I was doing online buying as well and we had a little scare where people were hacking into our credit card numbers so I just stopped it altogether. I prefer the face-to-face thing when it comes to something like [banking]*." FG8 female
>
> "*I bought something over in the USA, then I had about eighty bucks go to some corporation that I don't remember spending with. Couldn't get the money back. I had to show proof that I hadn't used my card and the last time I purchased anything overseas. And still haven't heard anything back from the bank but that didn't stop me from using Internet banking - I just swopped banks*." FG8 female

A few participants had experiences with their credit card being hacked, sometimes also whilst traveling overseas:

> "*I've had my credit card hacked. Someone booked a flight in Italy. When I was in Hawaii I got declined, and I rung up the bank. And they said 'someone's using your card overseas', and I said 'I am overseas!' Apparently it's good to let them know [if you are overseas].*" FG7 male

A few had a bad experience whilst trading online:

> "*I bought something from someone on TradeMe and the goods never turned up. She had sold them to about ten people*." FG4 female

Several participants described a bad experience through using Social Networking Sites:

> "*I had people hacking in to my Facebook account. I went in to Facebook one day on my laptop and someone was trying to get in from [location] with a mobile phone. So that was a bit of a hassle. And that's been done to me three times. That's why I was changing the passwords all the time. I've got nothing crucial in there, but still, it's spooky*." FG8 female
>
> "*My friend got hacked on Facebook. She got a message saying change your password. Then she got another saying her password had been changed even though she hadn't done anything. She had data on her phone so she called Facebook and they sorted it out in a few minutes, but if she had not seen it and time had passed who knows what might have happened*." FG3 female
>
> "F*riends who are already my friend asking to accept their new Facebook profile… I don't accept 'cause I know someone stole her ID on Facebook*."FG5 female

One participant was suspicious about her Facebook account being hacked and took action:

> "*I just posted up that someone else was trying to be me – don't accept them. A lot of them already knew. They were saying I was asking for money. But they knew that I wouldn't ask*

> *them. They were private messaging me saying 'are you okay'. That's how I found out*." FG5 female

Many participants had received spam or phishing emails, but only a couple of participants had actually responded to those emails. Most participants had deleted these emails:

> "*Almost every week I receive multiple emails or text messages saying 'you've won the lotto', or 'one million pounds', I simply ignore all of them because there's no such thing*." FG6 male
>
> "*I don't worry about the rubbish… $10 million from Nigeria, $20 million from the lottery! I don't waste much time with those*." FG1 female
>
> "*I was really waiting for my money. But the bank told me they were just trying to get my bank details. Because you had to get some sort of code [for banks] outside of NZ, and when I rung up for the code they told me to be really wary. But I still did it…. I was only having fifty cents missing every now and then, but if they're hacking fifty cents from about 50,000 people – that's a lot of money… I really believed I was a millionaire and I told everyone*!" FG8 female

For example, one participant clicked on a link presented in a bogus bank email, which led to an attack on her bank account numbers:

> "*It was inconvenient at the time to have all my accounts inaccessible. It was a quite scary moment for me. I had to change all of my accounts, my online codes… At least I've got that security now*." FG7 female

One participant got sucked into a Nigerian scam:

> "*I said 'ring me'… next minute they were ringing me hard out! So I had to change my phone number as well. Because I'm a bit gullible – but not anymore!*" FG7 female

Some participants had a bad experience as a result of using online games:

> "*My son and my husband, when they're on the playstation, they're forever having to update, because even though it's on the playstation it can still get hacked. So every now and then the game gets corrupted… But my son doesn't know what to do, so when a [virus] comes through he just carries on, and then it stuffs up. And once that stuffs up everything tends to… It seems to stuff up our internet… They put in their location. That scares me. If my son is on there by himself, someone could be hacking in to something, or they'll know where we are. That's something I don't know how to control either*." FG8 female
>
> "*Can get caught with in-game purchases with free games you can download from iTunes. They use your credit card number… and suddenly you've got all these expensive purchases for in-game things like three green crystals*." FG4 male

A few participants made the mistake of leaving their credit card details on their children's online devices after purchasing an app or particular items for an online game, which created a situation where their children were able to make purchases on their behalf but without their knowledge:

> "*We bought something online and accidently left the credit card details up there. She [daughter] went online and started buying all these things. So we got a bill for over $700…Checked with bank who said we've had quite a few transactions in a very short time. We traced it all back and it was my daughter*." FG2 male

Another participant thought he had downloaded malware as a result of using an online gaming site:

> "*I don't know if this was a virus, but all of a sudden this voice came on telling me how to make money. It was difficult to get rid of because it was just the audio, nothing to X off. I just pressed mute and carried on with what I was doing. Don't know where that came from. And other pop-ups. In the end there were three or four of them and I was going around in circles. It got to the stage it was becoming unusable. Then my neighbour said he could get rid of them*." FG8 male

A few participants were more casual about their bad experiences:

> "*I was hacked [by the recent Adobe hack]. I was one of a hundred and fifty million. But what does that mean? I've lost my credit card for a while now and I keep forgetting to report it. I keep checking it – no-one's tapped in to it yet*." FG7 male

A few participants described how they had used technology in order to manage a crime situation:

> "*We got broken in to when the family was out of the house. They stole iPhones, iPads, computers. A day or so later the people started turning them on and they were pinging up where they were. There'll come a time when there'll be a location device in the crockery! And people will stop stealing stuff*." FG9 male

Another participant related how a friend's stolen car had been recovered as a result of a Facebook post:

> *She posted out as her status 'has anybody seen this car, it was stolen'. She said the number plate and what it looked like. She has lots of friends on Facebook and got a lot of likes for the post and people saying they would keep an eye out for it. And then on another page, there are all these pages where you can trade swap and sell things, and some guy posted on that page, 'I just got a new car and I need this, this and this for it'. It turns out that she recognised this as her stolen car. Some random girl saw both those posts, so she informed my friend that this guy was looking for parts for what looked like her car. So we Facebook stalked him to find out where he lives. She went to the cops and they were saying 'sorry we can't really do anything about it, you don't have enough evidence'. So then she went and made a fake Facebook account and she asked him to be a friend. And he is an idiot because he accepted her. Then she chatted with him to try and find out where he lived. In the end she gathered enough information that she went back to the cops and showed them what she had and the screen shots and everything. There was just so much information out there that helped to locate him."* FG3 female

Not all illegal activities are considered to be bad

For young people, hacking could be a way of teasing others.

> *"It is definitely like that on the Internet. You have someone and its funny and it's all good like writing about someone being pregnant and their mother getting worried. Maybe that is a little bit too far."* FG3 female

It was generally agreed among the younger participants that this kind of behaviour was limited to people you knew could take the joke.

> *"We only do it to people that can take the joke. We only did it to him because he is a funny guy, and his parents are funny. He could say to them it's a joke and his parents laughed. Another friend left her laptop open and her friends said 'we should do something on her Facebook' and then we said 'no', because she isn't really that kind of person [who would appreciate the joke]. That is the final say on how far you take a joke: if you are friends and you know how they will take it, but I wouldn't hack the Facebook of someone that I didn't know."* FG3 female

Or checking on your partner.

> “*They’ve got these programmes, like keystroke. You can send an email and if you click in to it it will put a programme on your computer or tablet. I did that for my partner, ‘cause he was hiding stuff. Got it [his password] – got in to his Facebook, and he doesn’t change his password ever. So I’m constantly logging in, checking his stuff…. Basically keeps a log of everything he writes on his tab…. Well it’s not hacking if you’re just keeping an eye on your partner*.” FG8 female

A few participants described how family members are used to free downloading of movies or music from illegal sites. One participant also admitted that he had downloaded movies from an illegal site.

> “*Students and kids have no ethics for copyright*. *I asked my sister shall I get them vouchers for iTunes, and she said they’ll just say why did you waste your money? There’s no concept of why it wouldn’t be free… They say, ‘this is the way it is now – you don’t pay for music, for DVDs.”* FG4 female
>
> “*My nephew is a cop. He has a library of 450 [illegally downloaded] movies. He hasn’t paid for a single one. And he’s a policeman!”* FG4 male

Protecting online identity information

All participants were privacy and security aware and had developed ways through which they protected their online identity information. The following ways and means of protecting online identity information came up in the Focus Group discussions.

Using a safe or protected location

Several participants deliberately used a particular location they considered safe for doing online transactions.

> *“I only use [WiFi] at home to pay the bills. I do it through online banking where you pay by direct payment directly into their account. Otherwise you have to use a credit card. And sometimes a local trader does something for you and you pay them [by credit card] because you know where they are, and you feel safe. Other than that I would never give those details to [websites].”* FG6 male

Using anti-virus software

Many participants used anti-virus software to protect themselves. All those participants involved in the Computers in Homes (CiH) programme had anti-virus software set up on their computer. For some, it was the only online security strategy they used.

> “*When I had a PC it was just keeping up to date with the Norton’s notifications or whatever they sent through. That’s about the extent of it for me.”* FG7 female

A few participants found the more expensive pro-versions of anti-virus software not that user-friendly and preferred the free software therefore. One participant described a situation of a family member who had purchased anti-virus software that requireed so many upgrades and system checks that they wished they hadn’t got it:

> “*They can’t get it off. So it can be good and it can be inconvenient. And the free stuff has been very good.”* FG7 female

One participant had another reason to prefer the free anti-virus software:

> “*You download the [virus protection] free software then go on YouTube and find the keys for the pro version, and then put those in...”* FG7 male

Using a safe device

Several participants used what they considered a safe device to go online. For Asian people, a mobile device was often seen as more safe. Other participants also considered Apple devices safer than other devices.

> *"I don't use other people's computer for banking or credit card details. I always use my home computer or work computer. It's quite obvious. There's no free food!"* FG6 female

> *"First I choose a safe device – like iPad is safe – and I use my mobile phone since I've got anti-virus. For internet banking I only do it on my work PC because I work for a bank! It's very secure. And I try not to do too many transactions."* FG6 female

> *"My strategy is to use a Mac."* FG7 female

> *"I went in to the shop to get [anti-virus] for the iPad, and they said I didn't need it. Apple has got really top notch security built in. So you don't have to buy add-ons. I didn't know that! You see I don't know. It might be happening but I don't know. All I know is I don't get those clean up cookies, and little malware things happening."* FG5 female

Using privacy settings

Most participants actively used the privacy settings on Social Networking Sites like Facebook. One younger participant also used them for search engines.

> *"I use a lot of privacy settings.... If I post something on Facebook (which I very rarely do), I check to see which of my friends can see it. I think you can limit which search engines can look you up, so I'd use that as well."* FG4 female

> *"I'll change the [Facebook privacy settings] to who can see them [photos]… You've just got to play around with privacy settings. That's how I figured it all out… I change all my settings to just 'me' and 'private'."* FG8 female

> *"There are some people even within the family that I don't want to have the photos I have, because then they blast it all over Facebook... And if there's photos that only I want to see, I customise it to myself."* FG8 female

Friends' policy on Social Networking Sites

Several participants described how they have developed a policy for accepting and managing friends and other connections on Social Networking Sites.

> *"I have a policy that I won't accept any friend requests from people unless I actually know them."* FG9 male

> *"With things like Facebook and LinkedIn so common now, I do think twice before I put stuff on, thinking who might see this and read it. Like letting them know you're away on holiday and the house is empty. It's also who you accept as a friend to see your posts and how much you want them to know what you're up to – if it's an employer or an employee for example!"* FG9 male

> *"I have photos up there but nothing like pole dancing!! But I only have close friends and family that are on my page anyway. And if anyone sends a friend request and I don't know them, I don't accept them."* FG5 female

> *"I have about 150 friends, and fifty of them are close friends. I don't see information from the other one hundred because I don't want to see what they had for lunch."* FG10 male

> “*I’ve got less than 30 people as friends on Facebook. My privacy settings are the highest that I know of. Anyone who isn’t a friend can’t see anything including any pictures I post, which is very rare. Also I never say if I’m going on holiday even if only people I know are my friends on Facebook. I might post pictures when I get back, but for my own security reasons I never do because I don’t want people to know my house is unoccupied*.“ FG10 female

One participant described how he tried to maintain some control over managing online relationships with friends.

> “*I haven’t accepted a friend request in over 3 years. I’ve got a folder with over 140 of them in there. I keep them in case I want to get in contact with you – not you contacting me*.“ FG4 male

Using minimal information

Many participants used minimal information as a way to protect themselves in online relationships.

> “*Unless I was buying something, I wouldn’t put much [information] on. I’d put my name. My age only if it’s necessary… and definitely not location or anything like that*.” FG4 female

> “*[I provide] as little [information] as possible*.” FG10 male

> “*The standard stuff only they ask you for*.” FG10 female

> “*I don’t give out too much information. I’m wary about people stealing information and using it for themselves*.” FG5 female

> “*You just limit the amount of information you give. At that time, you just tick the boxes or give the information that you want to*.” FG8 female

Using real vs fake information

Participants discussed to what extent they use real information in online relationships. Several participants, in particular young people and Asian people, were very careful with sharing their real information with others online.

> *“I usually don’t give all my correct details when I sign up for things. I’ll change my date of birth or my address or just use an initial.”* FG7 female

> *“I must admit I’ve put in false information, mostly for online calculators, because I don’t want them coming back finding it’s me that’s seeking this information… So where it’s just for informational purposes.”* FG2 male

> *“I put false information in sometimes. Like birth dates – I don’t feel comfortable putting them in, and people put them on Facebook.”* FG9 female

> “*I think what would someone need to hack my life – it would be name, address and date of birth. So I just try and bury one of those things.”* FG7 female

Asian people only used their real names with close friends and relatives.

> “*We only use real names with our close friends and relatives. Then we feel safe*.” FG6 male

Young people more often obscured their real identity by using false information.

> “*I use fake names. Sometimes funny ones, sometimes more serious*.” FG3 female

However, older participants would never think of using false information and always used their real identity information when they shared information online.

> “*I always thought it was illegal to give out false information*.” FG2 female.

Several participants explained that it really depended on the situation and who was asking for the information. In some situations, particularly in relationships with government, people indicated that they felt they needed to provide real information in order to access a service.

> *"[Using fake information] depends on the website. If you're applying for an email address you don't have to give a real name, but with e-government, want to apply for a passport or something, you have to give a real number of your credit card."* FG6 male.
>
> "*Sometimes when I go to Work and Income it comes up wrong. And I need to keep entering it over and over. And I get trouble with the emails getting through to them. It's very important that those job applications go through to them*." FG2 female
>
> "*You don't get a choice with Studylink [to use fake information]. They want to know everything about you and if you lie you get fined a lot of money so you don't lie to them*." FG3 female
>
> *"I wouldn't use fake information with TradeMe either because if you want something you have to give them your real details."* FG3 female

Using pseudonyms

Several participants indicated that they used a pseudonym instead of their real name on Social Networking Sites.

> "*I registered under another name. Only the people who I know, know who I am*." FG6 female
>
> "*Often when I sign up to a site I have a pseudonym that I would tend to use*." FG4 female
>
> "*I write reviews on TripAdvisor, but I don't use my real name for that – partly because it's really easy to track someone's travel when you write a review for every hotel you've visited. And if I comment in forums I don't use my name, because I've got an unusual name and it's really easy to find my digital profile. So I try and separate out some things*." FG7 female
>
> *"I did it [used different name] on Tinder so I could see all the people in my area who were on Tinder."* FG8 female

A few participants explained why they sometimes use an 'alter ego' online:

> *"If I don't want anyone to see it's me, I'll use my maiden name."* FG8 female

Using multiple email addresses

Many participants used their real name in their personal email addresses, which made some hesitate about the circumstances in which they provide it.

> *"I always hesitate when someone asks me for my email address about whether to use my real one. If I use a real one it's quick and easy to answer all the questions because it's real. If I use a fake one then maybe years later I won't remember which one… A bit hard to decide but I always use a real one when I apply."* FG6 female

Several participants used multiple alternative email addresses and often one that did not contain their real name.

> *"I have one email address that's only for when I sign up for things that really, I only want to win prizes! So I have a Hotmail address for that. I have another Gmail account that my friend and I share for our work. So I sort my emails with that. So it's a lot of monitoring but, okay."* FG7 female
>
> *"I have a dumping email. So that if I sign up to anything I just use that."* FG4 female

Using passwords

Many participants described how they used multiple passwords for a variety of online relationships. Most struggled with managing them.

> "*It is a bit of a pain trying to remember this password and that password*." FG7 male

> "*I've had one of my passwords for twenty-two years now… Still does me well*." FG7 male

> "*I have about 15 passwords and I get in to a lot of trouble if any of them are required to change. I've got an account that needs to be changed every three months, and it's a disaster when you start running out of the 'suite' of passwords and have to start adding a new one to it.*" FG9 male

However, several participants admitted having only one password.

> *"I am really bad. Like I might have a different user name but it's because it's not my choice but I can't remember a different password for every different website that I am in. So unless I have to have a capital letter or numbers, which some make you do, I usually use the same one."* FG3 female

> *"I use the same password for absolutely everything. And my stepson said, for goodness sake, we know it, everyone knows it."* FG4 female

Many participants had developed strategies for using multiple passwords.

> *"I've got multiple passwords, but some very difficult passwords for a range of work things*." FG4 male

> *"[I use password] ones that are easy to remember, like birthdays*." FG8 female

> *"I have five separate passwords that I have rotated around my life. It's always been like that. So if I can remember it I just go through the five until I get the right one. I have different passwords for university, my banking. My social networks are all the same one*." FG3 female

> "*I have a different one for my Internet banking, but other than that they are all the same."* FG3 female

> "*One is for work and one's for home*." FG5 female

> *"I just have two sets: one for my professional kind of stuff, jobs and university and the like: and one for the junk webs sites and shopping. Username and password sets…. The junk sites user name is a pseudonym."* FG3 male

> *"I forget. And then I have to go in and reset everything. So my one for my bank is one that I've had for years and it hasn't changed. But elsewhere I'll have a capital letter and change one letter to a number. So same password but with different capital letters…. because I go on Facebook so often, I remember that one. It's all the other ones that I don't always use [that are hard to remember]."* FG8 female

> "*I use the kids' birth-dates but I switch them around*." FG2 female

Some participants used strategies to protect their passwords.

> *"I change my passwords all the time. I find it safer."* FG8 female

> "*I'm a bit dubious about writing them down in case you get burgled – there's all your details right there... We've recently opened this Drive account, where you can store your details in the cloud and hide it. 'Cause we've been assured that it's quite a safe, secure site. I have started putting serial numbers in it, and I will start doing passwords because I can't remember any of them – there's so many of them."* FG2 male

A few participants used a password app that saved all their passwords with one master one.

> *"There's an online app you can get to put all your passwords in. You just need the front password to that."* FG4 female

Some participants, in particular Asian people, thought they had too many passwords, creating a recall problem.

> *"But [I use] too many [passwords] now. So I have to write a note to remind myself. My note might be 'first letter of my mother-in-law's surname capital'"* FG6 female

Particularly older participants had difficulty remembering their password(s), but also others.

> *"It says here she remembers her passwords in a system that only makes sense to her. When you get to our age you can't remember any of that*!" FG1 female

> *"It's trying to remember them [multiple passwords] all."* FG9 male

> *"I find it really hard to remember a lot of passwords."* FG2 female.

> "*Honestly there's too many to remember. Because they say not to use the same password for different things*." FG2 female

Forgetting passwords was a hassle for a number of participants.

> *"With Telecom I'm constantly ringing them up saying 'give me a new one'."* FG2 female.

> "*The more you change them the worse it is*!" FG1 female

Several participants, including older people used a notebook to write down all their passwords.

> *"If I write my passwords down I put them in a little book that I can take with me, in case your house gets burgled."* ["So you don't worry about losing that book?"] *"Yes! That's why I keep it with me all the time.*" FG2 female

> "*When I was working we needed four different passwords, and the IT department would then say we needed new ones. I wrote them all down in a notebook, in a row. I've still got that notebook and I write down any password in there. When you open this notebook it looks like a foreign language*." FG1 female

> *"I can't remember all my passwords for different things. I've got a little page folded up for usernames and passwords. Even if I've put my name backwards (I don't use that one anymore) but someone out there has my name backwards as a username."* FG5 female

For some, logging on with their Facebook login details solved the problem of remembering all their passwords.

> "*It's easier because then I don't have to create an account and remember the passwords, 'cause there's heaps to remember. So I just always look for the 'Log in with Facebook' button."* FG8 female

Using protected WiFi

Several participants were aware of the higher security of using protected WiFi compared to public WiFi, and preferred using protected WiFi for that reason.

> *"I rarely use public WiFi."* FG9 male

> "*Where we live we have our own [password protected] router and that's secure enough for us."* FG6 female

A few participants described further strategies to protect themselves when using WiFi.

> *"Heard of some families who change their router to be a name. I don't do that because then people will know it's yours [and might start guessing their password]. Because you can drive anywhere and see the name, and go 'oh that must be that family around here'."* FG5 female

> *"When I'm doing banking I'm careful. I certainly wouldn't go into a cafe and do banking. If I knew the wifi provider I might. I'm loathe to do it on cellular even, I do it on hardline."* FG9 male

For some, the security risks were a reason for not using WiFi.

> *"My husband won't let me use wifi. He hates all internet stuff and he's very security conscious."* FG9 female

Logging out

Several participants mentioned they always made sure they logged out of sites.

> *"I think once you log in always log out."* FG5 female

> *"That's what they offer on lots of sites – to keep you logged in and save your password for this site. oh never!"* FG5 female

Deleting email when you don't know the sender

Several participants indicated they deleted email when they don't know the sender.

> *"If we don't know the sender we just delete it."* FG7 female

> *"If people I don't know send me an email, I delete it straight away. I don't even open it up."* FG6 female

Checking the use of language in a suspicious email

Some also checked the use of language in a suspicious email to confirm that it was a scam.

> *"I get ones [from friends who've had their accounts hacked] that say 'I'm stranded in another country and can you send me money'… But I usually look for the language that they use, like they'll use 'Dear Sir' or something quite formal… Once your email is out there in someone's profile or contact list, it's so easy for it to be hacked."* FG7 female

Using a credit or debit card with a limited amount of money

A few participants used a credit or debit card with only a limited amount of money in order to protect themselves when they are shopping online.

> *"I did invest in a Visa debit card rather than a credit card and I use that online. There's not much money in there."* FG7 female

Deleting credit card details

Some also pointed out that they always deleted their credit card details after using them in online transactions.

> *"I do a lot [online]. Now I'm addicted to GrabOne… At first I didn't realise my credit card details were actually saved with the website so every time I logged on [the details] would just pop in. So once I found this… I would delete the details each time. I would rather trouble myself, take some time and enter all those details again."* FG6 female

> *"Some accounts ask you to save your account information or save your credit card for the next transaction – uh no, delete it out. I try to remember to untick that box."* FG7 female

Not providing location details

Most participants kept their location details turned off on their mobile phone.

> *"I don't turn [my location] on at all."* FG8 female

A few people also described how they never provided location information online when they were away from home.

> *"Also I never say if I'm going on holiday even if only people I know are my friends on Facebook. I might post pictures when I get back, but for my own security reasons I never do because I don't want people to know my house is unoccupied. "* FG10 female

Not giving permission to use contact information

Some participants indicated they didn't want to use certain apps on their phone because of the condition that these apps would have access to their contact details.

> *"So I go – no! There'd be some [apps] I'd use but I wouldn't allow [them] to have access to everything on my phone*." FG9 female

For this reason, a few participants had uninstalled apps from their phone.

Not sharing information online

For privacy and security reasons, several participants did not share any of their identity information online.

> *"I don't give any information out. Zero. So I've got nothing to worry about."* FG8 male

> *"It's extremely annoying that people can take photographs of you and then put it online. There's times when someone says 'all sit together, I'll take a photo', and I step away 'cause I know they're going to put it on their Facebook page… Even though I don't go on myself, I end up on there."* FG8 male

> *"I don't fill in any of the things that say I'm married or single, or anything like that. I think I've said I'm in Wellington. I only like really general stuff on my wall – like Happy Birthday. I prefer people personal message me for anything else."* FG10 female

> *"No personal information. I find it annoying that advertisers are advertising on it. I'm thinking I'll go off Facebook because I don't want to be advertised to by Z Energy or whatever. That's starting to creep in now."* FG10 male

> *"Anyone is just as likely to sell my details to someone else so that I end up getting a whole lot of rubbish in my inbox. So I won't put my details on."* FG9 male

Not using online

A few participants protected their online identity information by not using the Internet.

> *"Not going on [the Internet]…. I just use it for contacting friends [not using Skype*]." FG8 female

Other security strategies

A few participants mentioned other security strategies they used in order to stay safe online:

> *"I check my credit card bills – not often, but I do scan through to see if there's anything suspicious."* FG6 female

> *"I've used PayPal for a number of years and I like it because they say they will never send you emails asking you to verify your account. So if you get them you know it's spam or phishing.*

> *It feels like an extra level of security. I've never had any problem with my PayPal Visa or anything."* FG10 female

Monitoring other people's online behaviour

Some participants indicated they monitored their children's or grandchildren's online behaviours to make sure that their security was protected.

> "*Security for [my children]. They don't really know who they're talking to on the sites…My youngest is learning to spell. Ads pop up and he can't read it properly so he clicks on it*." FG2 female

> "*I'm afraid of the internet in one sense, for what could happen to the grandchildren so I monitor the kids a lot*." FG8 female

> "*I've got a 13-year-old, a 12-year-old, an 8-year-old and a 3 year-old. All of us are on the Internet every day. My 13-year-old and my husband use the Playstation with the Internet for their game [like Modern Warfare and Call of Duty]. You can actually call up other people and talk and play the game. They've also got the Playstation Vitas, which gets the Internet too. Plus all the other little devices the kids get. The 3-year-old uses it for games but not Internet related games – just in case she taps on something while she's on the Internet and bring up something I don't want her to see. So she's the only one not on the Internet. The others are allowed on the internet but only on certain sites and I block off all the other ones. And they're only allowed on at certain times. But they take [the Vita] into their rooms… They're not allowed on Facebook until they are 16*." FG8 female

> "*If I'm signing my kids up for an online game and we have to create a profile, I put my details in there. So if they get any emails or anything it comes to me*." FG7 female

> "[After an incident where credit card was used for many in-game purchases] *we monitor everything [the kids] do now. It's in the family room, where we can see it if we are just walking past. If there's something they want to look up, we look it up first*." FG2 male

Trust in sharing identity information online

Trust is critically important for sharing information online

Trust in a particular organisation or individual played a critically important role in the decision-making process of individuals on whether or not to share their identity information online.

> "*It's about trust and who you are dealing with*." FG2 female

> *"[I trust information sharing] if it's a professional firm that's doing something for me that I need. If I do something for the kids and it asks me for my address details, I'll think 'you don't need my address details', and I'll carry on and do something else."* FG9 male

For instance, many older participants didn't know who or what to trust in these new online environments, which made them hesitant to share their identity information online.

> "*There seems to be a lot of dishonesty out there, which is another reason why I don't want to get mixed up in it, because you don't know what you're getting mixed up in*." FG1 female

For a few participants, all online sites were the same.

> *"Never thought about that before. Just go straight on. I don't really think about if they [online sites] are trusted or not. They're all the same."* FG5 male

Trust in online banking

The majority of participants trusted online banking and found it both convenient and secure. Some participants trusted online banking even more than online transactions on other sites.

> "*I feel quite secure on bank websites. Whereas I wouldn't trust other websites*." FG9 female

However, some participants, including most of the older participants, did not trust online banking and preferred going into the bank.

> "*There's too much in the press about people hacking these things. I have one account in the bank down the road and I go there to check it out*." FG1 male

> "*I want to go to the bank and see what I'm getting*." FG1 male

> "*I wouldn't do personal banking online. I don't trust it."* FG9 male

Trust in Government

Besides online banking, participants had relatively high trust in online transactions with government.

> "*Government you automatically trust more because you expect they're going to have that extra security. Even though they do have failures, they can't really afford to jeopardise that sort of thing."* FG9 male

> "*Generally government is more trusted than other websites. You know if something goes wrong you can easily hold them responsible for that. But for some private companies it can be hard to chase them."* FG6 male

> "*You assume you can trust the government agencies – falsely or not – and you would tell them more."* FG4 female

> "*I assume if they [government agencies] ask [for information] they must need it."* FG4 female

> "*Maybe a government site [I trust] – it's supposed to be authoritative*." FG1 male

Several participants had heard of RealMe and had signed up for it.

> "*RealMe. I trust that one."* FG1 female

A few participants explained that they have no choice but to trust government sites.

> "*Sometimes you have to trust them. When you renew your car registration and things like that, you have to enter your credit card details. So you don't have a choice."* FG6 female

> "*If you're using health services you just have to accept that you will have personal information on their data systems. I guess you kind of have to believe that it's going to be kept in good hands, and they've got good procedures to stop people from snooping about you*." FG10 female

For a couple of participants it didn't make any difference.

> "*I'd say [I trust government] the same. I don't treat them any differently. They could lose my information or accidentally release it as much as anybody else*." FG10 female

Many participants had relatively high trust in New Zealand government websites. They considered them to be secure and using their identity information appropriately.

> "*I trust government websites in that they wouldn't use it [the information I provide] against me or anything. But I don't know what they do with that information. I don't really care because they are not going to harm me in any way. If anything they are probably going to use it for research. I don't know."* FG3 female

> *"But if you're shopping [online], the shopping sites will know far more about you and your habits than the government will ever know*." FG10 male

> *"The use of information by government agencies and the Police, slightly worries me. I think we live in a country which theoretically our government doesn't do that [misuse your information] but if something were to happen and suddenly there was political unrest ... like in Syria ... and then that information was used against you… Me who goes on Greenpeace website, or posts something on rivers… suddenly all that information is being kept. And these relationships between Google and Governments ... that worries me."* FG4 female

However, a few recent immigrants thought slightly differently.

> *"I don't trust any government to act under the premise of honesty. They will act under what they think is best – at the time. And that's not necessarily being honest or open."* FG4 female

Some participants trusted government sites less than other sites.

> *"I'd probably trust the government sites less. Partly because they're bigger, and they talk about sharing information, so the potential for information to get out there and get lost, just seems bigger to me. Their databases are bigger and probably have a lot more personal information than I would release to a site I'm shopping with*." FG10 female

> *"I would say I trust them less. It's got to do with reputation that we talked about before – you can't swop governments, can you!*" FG10 male

Another participant wouldn't trust government to keep information safe or be transparent because:

> *"That means disclosing information that they don't want to – I still have to use Studylink or pay tax, but I'm not happy about it. They might feed you enough information to make you think they're telling the truth, but you're never going to know*." FG8 female

Untrustworthy sites

Participants described the types of sites they didn't trust.

> *"I think that pretty much any illegal site [like for movie downloads] is an untrustworthy site. You've just got to have good virus protection. You've got to accept there's going to be all sorts of viruses and malware coming from those sites – it's part of the deal*." FG7 male

> *"I would think twice about a site that asked to save your credit card number if you're making a purchase through them."* FG10 male

> *"I don't trust any sites with lots of those adverts to 'lose lots of weight' or 'become really skinny' or 'feeling lonely'."* FG7 female

> *"[Wouldn't feel secure with] sites that have ads that pop up."* FG9 male

> *"Any [site] that I'm not familiar with."* FG9 female

> *"When you're signing up for a site I'm always dubious when they have to know your birthday and things like that. I don't mind them asking what month you were born in, but specific information like birthdays I don't like… I would think twice about joining the website."* FG10 female

Participants also didn't like organisations who sent them emails without their consent.

> *"Green Party – they're annoying. I don't know where they got my email from but they just saturate me. They're fully annoying. Any sort of political party."* FG7 female

A bad experience can lead to distrust

According to participants, a bad experience could create distrust whereas not having had any bad experience could lead to trust in Internet use.

> *"I'm pretty trusting 'cause nothing bad has happened to me."* FG5 female

For example, one participant had tried to use a Hotmail account but had been locked out with a message to contact somewhere in India. They wanted a phone number and charged $200 to help. Consequently, the participant never went back into his Hotmail account:

> *"So I wouldn't trust those Hotmail people."* FG9 male

Prior experience is of critical importance

Having dealt with an organisation over a long period of time and without any issues was a reason for participants to trust them.

> *"I trust Telecom with what they offer because I've dealt with Telecom for a long time."* FG5 male

> *"[I trust TradeMe because I] never had any issues.*" FG2 male

Location matters

Most participants pointed out that location is important for trusting a site.

> *"If it's based in Nigeria..! [he laughs]"* FG4 male

> *"I think I'm more conscious about purchasing locally online rather than overseas. At least [here] you think you can track them down or I can go and see them. Whereas overseas you're a bit more hesitant."* FG7 male

Many of them trusted New Zealand websites more than overseas websites.

> *"I would try a New Zealand website. I tried TradeMe before I went to eBay. I would shop at MightyApe before I went to Amazon. And I'm prepared to pay a little bit more because I know I can call them up if something goes wrong. I've had really good customer service from MightyApe – they even tell you when the thing is in your mailbox! On one occasion when something did go wrong I was able to phone them up. It's just nice being able to call and solve the problem rather than contacting someone overseas."* FG10 female

> *"I find that websites with a .co.nz I automatically trust more than a .com."* FG9 male

> *"I think the nz part of the address means it's governed by our laws, not somebody in Nigeria or the USA or something else. So you've at least got the government behind you."* FG9 male

> *"If it's clearly got some local content – like a local phone number and contact address. Some overseas companies will use a .co.nz address but then you know they're not domiciled here."* FG9 male

> *"Anything that doesn't have .co.nz or .com.au. If it doesn't have that I won't do [shopping online]… I stick to Aussie and New Zealand because I trust [those sites] and I've done it before."* FG8 female

Asian people also trusted NZ websites more than overseas websites.

> "*We trust New Zealand websites more than overseas*." FG6 male

> *"In New Zealand I haven't tried a government website, but with ANZ bank or Westpac, if anything goes wrong with the bank system… they either pay you money or – they're quite*

> *reasonable, put it that way. If your card is hacked during the system crash, they will reimburse your money. It's quite fair. It's why I feel safe actually."* FG6 female

However, one participant pointed out that location is becoming less important in trusting online transactions.

> *"I got a Nigeria letter from Dunedin the other week, so perhaps that's changing*!" FG9 male

Physical presence creates trust

Some participants indicated that the physical presence of an organisation gave them the trust to use their online site.

> *"If it's got a physical presence – a shop that you've been into, or a bank – then I have zero qualms about using that."* FG9 male

Brand recognition enhances trust

Several participants described how their trust in using an online site is enhanced through local or international brand recognition.

> *"If it's got an international brand and website, like Amazon, then you're effectively transferring your brand trust with it."* FG9 male

> *"It has to be a known name, like eBay. Smaller sites I would have to Google it and see what other people have to say about the service and reliability."* FG10 female

However, trust in a particular brand could also go together with a bad experience as one participant found out:

> *"On the NZ Herald site I clicked on something that I thought was a proper article and it went to some infomercial site. I was quite surprised actually, that they were infiltrating some of what you'd think are quite trustworthy sites."* FG7 male

Reputation is critically important

Many participants described how they explored the reputation of an online site. Reviews, feedback and online searches were considered of critical importance in their decision-making process for using a particular site.

> *"I'm fascinated by the idea that although buying online is a really new concept, it's all motivated by the old-fashioned notion of reputation – the reviews. I would always check somebody's reviews before I buy off them, whether it's the second time they've sold something or the thousandth time they've sold something."* FG10 female

> *"I'll research them and read the comments that come up to see if there are bad comments or experiences with it. If there's bad comments then that's it – I don't go on it at all – even if there's just one. Because there's probably something else in there."* FG8 female

> *"I always do a bit of investigation into the site that I'm using. My major shopping site is called AliExpress.com. You may have heard of AliBaba owned by Jack Yan, one of the richest people in the world now I think, where you can buy thousands of pens and things like that. AliExpress is a miniature version where you can just buy ones of things. But it had a good reputation before I did an investigation. They had no security flaws, it was well rated by online security people. And they actually have a really good customer service rating, where they'll follow up on issues. The one time I did [have an issue] they followed up and were really good. That's only cemented my opinion of them."* FG10 male

> *"I look for the feedback on a website*." FG4 female

> *"Also external reviews, not just on the website."* FG4 female

> *"If it's overseas I'll do a bit of a review on the company to see whether it's trustworthy or not."* FG7 male

Trust based on experience of people you know and trust

Participants described how they developed trust on the basis of online experience of people they knew and trusted.

> *"I talk to people about the sites I use, because I use quite a few in America with free shipping - gets me every time! But they do actually get you free shipping. And I will talk to my friends about the experiences they've had. It's so convenient, and if you don't like it you send it back. I do go by word of mouth, by people I trust. Although everything's accessible and easy [online] I'll still go and talk to people about sites."* FG7 female

> *'I bought my wedding dress online [from overseas]. And I was a bit paranoid … but they were just late shipping it, and in the end it arrived. My best friend had ordered our bridesmaid dresses online, so that made it a bit more secure for me, doing a big purchase."* FG7 female

> *"Sometimes I will check with my friends if they have used this website. Is it safe or not?"* FG6 female

Trust can be influenced by media stories

Trust was sometimes influenced by stories participants heard through the media.

> *"I would say government ones [to trust] but kind-of not know after you hear all those things in the news – that they're constantly watching you, watching what you put on[line]."* FG8 female

> *"We always think Norton's Antivirus [are an organisation you can trust] but you hear this stuff, that they're probably the place that puts out the virus to keep themselves in business. You wouldn't put it past them these days. You just don't know."* FG7 male

Knowledge

Lack of knowledge

Quite a few participants demonstrated a lack of knowledge about what happened as a result of their online behaviours, in particular those with low education levels or relatively inexperienced Internet users. This situation made them worried.

> *"I just worry if I'm sending an email, if this is going to be secure. Is anyone else going to be reading this letter that I wrote to ... whoever? Is anyone going to be seeing my photos online?"* FG5 female

> *"Especially family photos. Who could be taking that? Who could be using it for their info?"* FG5 female

> *"The thing I didn't get was with Facebook. Before I had an email address I posted my cell phone up, so I was getting a few random calls from people I didn't even know, but they knew people that I knew were on Facebook but they could still see all my information. Also I do Jet Bingo, and I have all my information up there and I'm not sure if people could hack in to it. My account and details is all up there – you just push a button and they take the money out. So I was a bit iffy with that, and I've taken the account down but I'm still not sure if they've got all that information*." FG2 female

> *"Those pop-ups that come up when you put in your password, asking if you want to save this password… I never ever click on those and save the password … I'm just worried that little thing is something that's going to get in and copy my password."* FG8 female

Most did not know what to do, how to report bad experiences or stop them from happening again.

> *"[My old Facebook profile] is still running. It's still running from the day I set it up. I don't even know what people see when they look at my profile – if they can see everything or..."* FG8 male

> *"I didn't think I put stuff in the cloud. But I have been doing it all the time. I don't know my phone is doing all that stuff – you have to turn it off. And then you get a new phone and suddenly it's got all your stuff – photos from eight years ago."* FG9 male

> *"My son and my husband, when they're on the play-station, they're forever having to update, because even though it's on the play-station it can still get hacked. So every now and then the game gets corrupted… But my son doesn't' know what to do, so when a [virus] comes through he just carries on, and then it stuffs up. And once that stuffs up everything tends to… It seems to stuff up our Internet."* FG8 female

Knowing that they don't know

Many participants were aware that they did not know how things work online, and sometimes took action to compensate for that lack of knowledge.

> *"I worry that when I click on a site a virus is going to come in to my computer. I never used to be big on anti-virus but now I actually spend money on Norton."* FG5 female

> *"I've never realised how easy it is to find out information about yourself... I'm still a baby on the internet working and feel I need to learn a bit more so I can be confident doing it."* FG2 female

Several of them admitted they are relatively new Internet users. For example, one participant tried to 'X' out pop-up windows in the top-right corner, but then more pop-ups appeared.

> *"It would be good as a new learner to know where to get rid of that, or even if you can.*" FG2 female

Knowing what they need to know

Several participants knew enough about using the Internet in order to deal with new or unexpected situations online.

> *"My son's 15 and there's a game called Stick Cricket … and he misspelt it and got Sick Cricket. It came up with some fairly nasty stuff with cricket bats … you can imagine. And he was absolutely… 'oh my god, mum, I didn't mean to ... delete history'. So with the best will in the world you can be going somewhere innocent and … make that sort of mistake and that sort of thing comes up. But you hope as parents, we've given our children enough sense to point it out or go – 'ooh mum!!'"* FG4 female

> *"I guess if there was something I didn't know…[I would ask the kids]. But once you know how to use Facebook or how to work Google, you can usually work stuff out*" FG4 female

Privacy knowledge is critical

Without exception, participants described how they wanted to protect their identity information as much as possible online. Most participants struggled with this and admitted that they didn't have enough knowledge on how to keep their information private.

> *"But you need quite a bit of knowledge [to remove information/keep it private]... The more knowledge you have the more secure you're going to be*." FG4 female

Getting help

Receiving help from others

Participants often received help with Internet use from family, friends, or other expertise available to them.

> *"It's not like I'd rush in to something and say 'oh goody something new'. I'd find out about it first. My sons all work in IT, so I'll ask them, and they might say, 'no, that's a bit dodgy Mum, stay away from it'. Or 'I'll have a look and let you know'*." FG1 female
>
> *"I got my mate to set up my computer. He did something on my computer, a security thing I don't know what it is, and it comes up on my screen now saying 'you've got this, all your things are secure', so I don't have to worry about it…. My computer is free of most glitches. I don't get spam mail*." FG2 male

Self-help

Many of them also tried to help themselves online.

> *"Sometimes you just have to teach yourself to be confident to go online. You will probably end up in China or something, but you get used to it."* FG5 female
>
> [With photos] *"I'll change the [settings] to who can see them. You've just got to play around with [the Facebook privacy settings]. That's how I figured it all out… I change all my settings to just 'me' and 'private'."* FG8 female

Searching for help online

Some participants relied on the Internet for help, especially younger participants.

> "*You Google your problem and you come up with a help source*." FG3 female
>
> "*Looking for help with "Aunty Google*" FG2 female
>
> *"You can check on Internet scams – that's a good one. A few times we've texted if something is a scam. You just put 'scam' and google it and normally put in a name of the company it comes from. And it comes up."* FG4 female

Help for older people

Older participants tried to do activities online themselves but some were scared to do so. They usually relied on their children or other young family members to help them out.

> *"You learn from doing it yourself sometimes… When I get to 'where do I go next?' - that 'next' will be one of my kids. When the one gets angry I get the other one to help me with the next level. That's how I go. Getting my kids to show me."* FG5 female
>
> *"It depends on the ages. Like for the young ones they go from one to the other, and search – all those things. But for us – over that age – we're too scared to so. I'm still learning but we've got no choice but to do it. Looking at the young kids now - even the little babies bloody do that – pressing all the buttons… Shame on me asking her kid to show me how to do it – she's only about 9 – and look at me over 50 I can't do it. I find it really hard…. They were brought up with technology. For us we have to write everything down."* FG5 female
>
> "*I guess if there was something I didn't know…[I would ask the kids]. But once you know how to use Facebook or how to work Google, you can usually work stuff out*" FG4 female
>
> "*If I want something I get my daughter to do it for me because she does it quite a lot*." FG1 female

Young people sharing their knowledge

Young people often found themselves in situations where they were helping others with their online activities.

> *"The more I use the Internet, the more I am teaching people."* FG3 female

Teaching children

Many parents had taught their children about Internet use, security and sharing their information online.

> *"My daughter, who's nearly 12, there's certain information we don't want her sharing. So there's strict instructions for her use of the Internet. If you're chatting to a friend via Instagram or something like that, don't assume just 'cause they say their name is Johnny and he's eleven, that his name is Johnny and he's eleven! We've sat down and had those chats before she was allowed to sign up for Instagram and things like that… She wouldn't give out her address or phone number or anything like that. Or even the town she lives in. I think it's good to have those talks, especially with kids."* FG4 male

> *"My son has known how to set up the computer and skype his family overseas since he was three years old. I think it's really important to teach a balance. Because when they grow up they are going to have access to the Internet, so it's more about teaching them to use it responsibly."* FG7 male

> *"We don't block our Internet either, but we have that open conversation that if there's something they [2 kids] come across that they don't like or they're not sure about , they should come and talk to us. I think it's getting them to use it responsibly and be aware for themselves."* FG4 female

> *"We do quite a lot of talking about social networks." [*Daughter wrote a speech about why 11-year olds should have a Facebook page, after her Facebook page was deleted by her parents.*] "That led to a really good discussion about what Facebook is and the targeted advertising that comes through. So she still doesn't have a Facebook page, but I want to keep those conversations going for when she does have a Facebook page."* FG7 male

> *"We try and counsel the kids that it might seem fun now but that it stays there."* FG4 female

Changing online behaviour over time

Becoming more private over time

The large majority of participants had become more private over time in using the Internet.

> *"Before as a newer user I would fill in everything. And now you don't need to. You don't need this information to give me what I want. So now I think I'm a smarter user – if I get a funny feeling and think why are they asking that, I'll just stop and leave it. And find another avenue to get what I want."* FG5 female

> *"Nah, I've learnt." [*She shares less information with fewer people now than when she started as a teenager*] "Now it's like, 'you don't need to know that – I'll keep it to myself'."* FG8 female

> *"When I learnt that whatever photos you uploaded to Facebook then belonged to Facebook – I took issue with that, and I've only just come back to Facebook after a long time away. I'm more cautious now especially around the children and what I post of them."* FG7 female

> *"I don't use Facebook anymore. I look over my wife's shoulder if I need to know what people are doing. She's on it all the time. I see enough people and interact with enough people, I don't need the distraction. So that's my privacy setting!"* FG9 male

Becoming less private over time

Only a few participants had become less private over time as a result of experience and becoming more pragmatic with their privacy in certain online service areas.

> *"I used to not enable the location service on anything that came through. But I decided what I was losing in privacy I was gaining in benefits, so I tend to enable those."* FG9 male

> "*My behaviour has changed a little in the time I've been using the internet, in that I'm more casual with it. I used to not even put my email address down for things without checking with mum first… but it's become more casual and more open."* FG4 female

Bad experience usually drives changed online behaviour

A personal bad experience usually had a major impact on online behaviour. For quite a few participants, a bad experience caused them stop doing things online.

> "*I was doing online buying as well and we had a little scare where people were hacking into our credit card numbers so I just stopped it altogether. I prefer the face-to-face thing when it comes to something like [banking]*." FG8 female

> "*Those sites that offer you to get rich at night – I really got sucked in to that. That was when I first got on to the Internet. But all it was doing was putting viruses on my computer*." FG8 female

> "*I think our laptop had a virus or something that take information. We bought something online – and I'll never buy anything online again – but someone managed to get that number and bought something for 150 bucks. I saw it as a purchase that got done in America. But the bank was good because they refunded the money."* FG9 male

> *"I'm wary for a bit when something happens, before I get comfortable again*." FG8 female

For most participants, a bad experience for other relatives or friends also had an impact on their own online behaviour. For example for one woman a faked University site convinced her husband to send passport and schooling information to obtain a position, and then there was no more communication.

> "*I am very concerned about security after what happened to my partner's information when applying online for teaching jobs*." FG2 female

Changed online behaviour as a result of a bad experience could happen to multiple family members simultaneously.

> Recounting of man's daughter (10 years) infatuated with Sims online game which used real money for micro-purchases. "*We bought something online [for Sims] and accidently left the credit card details up there. She went online and started buying all these things. So we got a bill for over $700…Checked with bank who said we've had quite a few transactions in a very short time. We traced it all back and it was my daughter." [* Was behaviour changed?] *"Definitely. We check and re-check. And we had quite a lengthy talk with our daughter about mis-use of a credit card, and that someone has to pay it."* FG2 male

However, a few participants continued their online behaviour even though their close family had a bad experience.

> “*It’s just easier… I’ve used online banking for ages. My husband won’t use online banking but that’s only because he’s had a bad experience with a bank once that the money went out and it wasn’t supposed to… But nothing’s ever happened to me so I’ll keep doing it*.” FG8 female

Positive experiences can outweigh negative experiences

Some participants described how many positive experiences can outweigh the few negative experiences they have had online.

> *“Between my husband and I, we probably buy thousands of things online – for business and everything. And we’ve probably had two bad experiences – one on TradeMe… It’s like being a consumer of anything; sometimes you have a problematic experience.”* FG4 female

> *“It’s the number of positive interactions that you take for granted. Then it’s the negative ones that people talk about.”* FG4 female

However, a few participants have not had any bad experience that has caused a change in their online behaviour.

> “*I haven’t had a bad experience that’s caused a change.”* FG7 female

A positive intervention can negate a bad experience

If participants had a bad experience that was followed up by a quick and helpful intervening response, they usually did not change their online behaviour.

> “*When my [work] credit card had five thousand put on it by somebody overseas, because my employer was so quick to intervene it made me feel quite safe about continuing to use it online. I don’t do anything different with my personal credit cards. So long as it’s got an ‘s’ after the http…”* FG7 female

Changing behaviours through learning from bad stories in the news

Several participants indicated they had changed their online behaviours based on stories about bad online experiences in the media.

> “*Probably learn through the bad experiences of others in the newspapers*.” FG9 male

> *“My change [in online behaviour] would be… the photo thing. Sending a photo by email instead of posting it on a site.”* FG4 female (done after listening to a speaker on ‘digital footprints’)

Making mistakes belongs to the learning

One participant made the mistake of leaving his credit card details on his daughter’s iPad after purchasing an app. Then she was able to purchase several more apps without his knowledge:

> “*That’s just an awareness thing.”* FG4 male

Learning over time

Participants described how, over time, they have learned from experience and become more familiar with online activities, especially Internet banking.

> “*I think it is hard to lose money by banking or other venues. The problem will happen only at this stage with people who are not familiar with the e-banking options. I had my first experience of being hacked 18 years ago when I first had my credit card and I didn’t know how to handle it… [story of being duped into giving out credit card details, but then immediately contacting the bank who chased up the people and got the money back.] “And that was the lesson I learned.”* FG6 male

> *"I've been doing only Facebook and Internet banking for so long, they're probably the only ones I'll stick with."* FG8 female

Changing behaviours through learning from others

Several participants had changed their online behaviours through learning from others, positively or negatively. Many of them had learned from (their) children.

> "*My daughter reads on her phone. I used to think that was too little… but actually I read almost all my books on my phone now*." FG5 female

> "*They [children] are guiding us!"* FG2 male

> "*A few years back an ex-flatmate of mine put a program on my laptop and it showed worldwide thousands of addresses skipping through and it was addresses trying to hack in to my computer right then. He could pinpoint addresses in Australia. It was just my software keeping them out. It was quite frightening."* FG9 male

> "*There's an app called 'Seek'. It's free. It hacks into everyone's personal information. All you have to do is punch in '[name]' and that business, and it hacks straight in to it! I've had that experience because a friend who's an IT person told me – try this, and I tried it. Woah! It was scary stuff. I thought, is somebody watching me?! So I totally deleted it."* FG9 male, became more careful of sharing information as a result.

Privacy behavioural types

Besides the three privacy behavioural types we observed amongst our interview participants (i.e. privacy pragmatist, privacy victim and privacy optimist), we identified a fourth type among our focus group participants: a privacy fatalist. We have illustrated these types below.

Privacy pragmatists

The large majority of our FG participants were so-called 'privacy pragmatists': people who were privacy aware but willing to trade off their identity information for convenience, cost- or time-efficiency, and/or a particular service.

> "*Depends. If I really want what they've got I'll do it [share my identity information online]*." FG8 female

> "*When I want something delivered to me I'll just use my first initial instead of my name. But that doesn't matter because then my email comes up and it is my real name. I don't really think about it. Usually they don't save your information, or you can choose not to have it saved. So I choose not to have it saved so that when I have done the transaction my Debit card information is instantly removed. I don't really mind as long as the parcel gets sent to me really*." FG3 female

> "*I used to not enable the location service on anything that came through. But I decided what I was losing in privacy I was gaining in benefits, so I tend to enable those*." FG9 male

> "*I find it interesting that the ads are related to what you are interested in. A lot of the time the ads aren't interesting at all, but when they are customised to you it can be so useful like information about flights to a place you want to go to*."FG3 female

> "*I'm going to be bombarded with ads anyway, at least [this way] it might be something I'm actually interested in…. [Regarding new Facebook Messaging system] A few years down the track you're not thinking 'damn I shouldn't have ticked in that box', you thinking how convenient it is now*." FG4 male

> "*My general feeling is that if somebody wants to hack in to my personal information, as long as they can't get hold of any payment information, I don't give a damn. That risk is the cost of convenience of using something like the internet*. " FG9 male

Privacy victims

Several participants turned out to be 'privacy victims': people who saw no choice but to hand over their identity information in order to use the online service, inevitably leading to a loss of privacy. Privacy victims stopped using the service when the information demands were too intrusive.

> "*Initially you feel bullied in to it…You've given up a bit of yourself as far as individual choice is concerned. And you do get to the point that you either have to accept that either they have the potential to throw more of your information out there, or I just can't use this app anymore. You still have a choice – use it or don't use it*." FG4 male

> "*I usually go there to play games. If they ask questions I just give up and get off*." FG5 male

> "*Once they start asking those questions I click the off button*." FG2 female

> "*Up to a point you think, oh no I'll resist this, I won't do that. Like if you want to continue messaging in Facebook you have to go to this new messenger app. They are not going to allow you to use Facebook to message. If you want to use it – accept it [to share your identity information online]*." FG4 male

Privacy optimists

A couple of the participants were 'privacy optimists': people who were willing to keep doing what they think could be risky, until something bad happened to confirm it.

> "*I've never had any issues. I'm quite amazed I've just typed in my credit card number and they've got no security… I do that sometimes. I think, 'oh I'll find out if it's going to… The banks will look after you. That's sort of what I trust sometimes*." FG5 female

> "*I'm pretty trusting 'cause nothing bad has happened to me*." FG5 female

> "*Wonder if we are becoming too over-paranoid about security. We've got to use the internet these days. Just got to be a bit sensible about what sites you use and what sites you don't*." FG7 male

> "*It's just easier… I've used online banking for ages. My husband won't use online banking but that's only because he's had a bad experience with a bank once that the money went out and it wasn't supposed to… But nothing's ever happened to me so I'll keep doing it*." FG8 female

Privacy fatalists

A few participants were 'privacy fatalists': people who considered there was an unbridgeable power imbalance and a major breach of their privacy was inevitable and unescapable.

> "*For me there's no privacy anymore. When you asked me about what sort of information I put on the Internet, it's irrelevant because there is open access to every area of your life… The moment you first put in any details about anything, you just open yourself up. I know that ten years ago I opened my life to the Internet, and you can't get that back. The thing I probably limit now is how many photos of myself I put up, or of my children, on the Internet. If people think you've got privacy – you're dreaming*." FG4 female

> *"It's a bit of that 'big brother' knowledge about your life. But if you want to play that's what you sign up for. Maybe we didn't know what we were signing up for ten years ago but we know now… what can you do?"* FG4 female
>
> *"It's convenience versus freedom… How much does it impinge on our freedoms without us even being aware of it?"* FG4 female

Online behaviours of particular groups of participants

In the sections that follow, we present research findings where we have observed unique or different online behaviours between particular groups of FG participants, as well as different privacy and security perceptions. The following groups demonstrated different online behaviours: different age groups, in particular young people and senior citizens, and different ethnic groups, especially Māori, Pasifika and Asian people. We also note how the identified privacy behavioural types manifest in these population groups.

Young people

Critical importance of the Internet

Young people said they could not live without the Internet.

> *"10 out of 10"* FG3 female
>
> *"We are so used to it being around now that I think if we suddenly didn't have Internet everybody would be lost."* FG3 female
>
> *"It's like a little cult- no a big cult."* FG3 male

For them, it was the go-to place.

> *'It is just fast, easy, no mess, worry – just open laptop, Google, shut laptop and continue with whatever else you were doing."* FG3 female
>
> *"You go through all your social media sites: Facebook, Tumblr, SnapChat. Once you have been through all of them, then you can get out of bed and start your day."* FG3 female
>
> *"Everything is just so much more difficult to do without the Internet. If you want to get in touch with your friends, it doesn't matter where they are; you want a book from the Library, instead of having to spend time going there and looking for it, you go online and there it is. I might spend all that time going there to check out what is in the book and what I am looking for might not even be there. You just Google it from home. That is much faster and more efficient."* FG3 female
>
> *"The other day my friend's car was stolen. So she posted out as her status 'has anybody seen this car, it was stolen'. She said the number plate and what it looked like. She has lots of friends on Facebook and got a lot of likes for the post and people saying they would keep an eye out for it. And then on another page, there are all these pages where you can trade swap and sell things, and some guy posted on that page, 'I just got a new car and I need this, this and this for it. It turns out that she recognised this as her stolen car. Some random girl saw both those posts, so she informed my friend that this guy was looking for parts for what looked like her car. So we Facebook stalked him to find out where he lives. She went to the cops and they were saying 'sorry we can't really do anything about it, you don't have enough evidence'. So then she went and made a fake Facebook account and she asked him to be a*

> *friend. And he is an idiot because he accepted her. Then she chatted with him to try and find out where he lived. In the end she gathered enough information that she went back to the cops and showed them what she had and the screen shots and everything. There was just so much information out there that helped to locate him."* FG3 female

Several used the Internet for online dating.

> "*My friend has had boyfriends from Tinder, and they have been lovely."* FG3 female

> "*A friend got attacked by one of the guys she was meant to go on a date with. I asked 'how did the date go' but she didn't want to talk about it. Interestingly enough it didn't scare her away from Tinder."* FG3 female

According to our young participants, if you were not online you missed out on things and got left behind.

> *"People get left behind. My friend didn't have Facebook until this year and he never got invited to anything. He'd get mad about it and I'd tell him to make Facebook. If you don't have it you are going to get left behind."* FG3 male

> *"Like one night you are all working away on your own thing but you are all on Facebook and something happens and everyone is commenting on it. Then you are still talking about it the next day [face-to face] and if you weren't on Facebook then you feel left out."* FG3 female

> *"All my friends who were refusing to be on Facebook are now. I don't know anyone who isn't."* FG3 female

> *"If it was one of the other [social media] you don't have to have it, but Facebook, you have to have it. Even if you don't want to be on it 24X7, just to be on it and check it perhaps once a day to see if somebody is trying to contact you, because that is how people do it now."* FG3 female

> *"If you don't have Facebook at Uni you are getting left behind because our lecturers are on Facebook and they are talking about things that help you pass the course. They will post stuff to Blackboard because that is a mandatory requirement but they will chat more informally and answer questions on Facebook*." FG3 female

They were very tech-savvy.

> *"There are so many flaws in the Internet that the people in charge e.g. at university don't know."* FG3 female

For them, the online world was much more important than the offline world.

> "*I feel like I've kind-of lost touch with people… They say that Facebook is the new social thing but you're not just shutting the laptop door, you're shutting yourself off from life. You could have 700 friends, have good chats with them but you could see them in real life and walk right on by… [using the Internet] it's easier to shut people off. Shut off the drama, the nuisance. Hide stuff if you don't want them to see it. Block people*." FG8 female

But there were also limits for young people: even they sometimes needed a break or preferred meeting people face-to-face.

> *"Sometimes I wish I was not so contactable. Everyone can get your mobile, your email, your Facebook and so on. Sometimes you* need *a break and you want to throw everything away and have it that if people want to see you they have to come over [in person]."* FG3 female

> "*Meeting up with people that you have only met online. No. If you want to meet people, you can't work out if they are a psychopath online. You need to check them out first."* FG3 female

Internet as playground

Young people treated the Internet as a playground. For example, they regularly hacked into their friends' Facebook accounts or their mobile phones.

> *"The Internet is definitely like a young people's playground. In a real playground you might trip your friend up as a joke, but you'd make sure that they didn't get hurt or you could just beat someone up in the playground. There is a spectrum."* FG3 female
>
> "*One of my friends who knows my email address thought it would be real funny if she signed me up for a dating site called Sugar Babies. It was good revenge for things I had done to her. I was at uni, and I just suddenly started getting all these emails from random men, asking me to meet up in Wellington. That was pretty scary and it took me ages to work out how to delete the account too. So there could be people on the street who might recognise my face because she put up a photo, and wrote a funny-as description. So people could just look at me and go 'you are that girl'*. FG3 female
>
> *"A lot of people do take Tinder seriously. My friend has got about 1000 people because we stole her phone one night and said 'yes' to everyone. We just told her we were looking at pictures while she was sitting across from us. She tried deleting her account but it didn't work. So she had to turn off all of her notifications for Tinder because her phone just kept vibrating for a couple of days."* FG3 female
>
> *"My guy friends will go into town and they will get out their Tinder and click 'yes' on absolutely everyone, just to see what happens. Guys usually take the piss out of Tinder quite a bit."* FG3 male

However, they did know when and where to stop their online playground-like behaviour.

> *"It is definitely like that on the Internet. You have someone and its funny and it's all good like writing about someone being pregnant [on their Facebook wall] and their mother getting worried. Maybe that is a little bit too far."* FG3 female
>
> *"We only do it to people that can take the joke. We only did it to him because he is a funny guy, and his parents are funny. He could say to them it's a joke and his parents laughed. Another friend left her laptop open and her friends said 'we should do something on her Facebook' and then we said 'no', because she isn't really that kind of person [who would appreciate the joke]. That is the final say on how far you take a joke: if you are friends and you know how they will take it, but I wouldn't hack the Facebook of someone that I didn't know."* FG3 female
>
> *"Nobody knows my Facebook password. But now, I will never leave my phone in my friend's room because I just can't trust my friend with my phone anymore. It's not money or anything like that, it's Facebook. They will write a funny status. I lock my phone with a pass code, but one of my friends saw me putting it in and I left my phone in her room thinking it would be fine but, nah. But they would never cross the line by going into Internet banking or something like that."* FG3 female
>
> *"There is a clear definition of what you can and can't do [in the name of fun]. Social Networking Sites are fine, everything else is just about off-limits."* FG3 male

Multi-tasking

Young people were used to multi-tasking online. They generally had several communication channels open at the same time, such as Facebook, SnapChat, Twitter, and email.

> *"You can have like a hundred tabs open at the same time…. You have your shopping tabs different, like you are eating and you have got a video from YouTube running and you have*

> *Facebook open and you are chatting with your friends. Skype might be going and you are kind of ignoring your mum."* FG3 female

> "*Or you can be having Facebook chats with multiple people so everyone sees everything at the same time. Whereas with texting you have to send it to each one individually. You can do group texts but then the others can't see the replies other make. Same with email."* FG3 female

Most used at least two devices: a laptop and a tablet or a cell-phone and a laptop.

> "*And you have two devices. So then you can do even more."* FG3 female

They usually expected immediate replies to their messages.

> *"People sometimes message you and they expect a reply within about a half an hour. If you are busy you will find you have a pile of messages saying 'why haven't you replied'?"* FG3 female

> "*If I want an immediate reply I would text someone because I know that everyone has usually got their phone on them. You don't walk around with your laptop open but everyone has the Facebook App on their phone anyway."* FG3 female

> "*If I don't have any credit I might text someone with my last credit and tell them to contact me through Facebook so we can talk more*." FG3 female

Struggle to understand government

Dealing with government online was described as difficult or problematic by many young people.

> "*StudyLink. They're useless. Heaps of emails and then you end up calling them*." FG3 female

Generally they did not know how government worked. They struggled in dealing with government online, particularly when they compared this with other online experiences:

> "*Facebook is just so easy. But when you start thinking about doing Government stuff it's like, I don't know how it works, their websites are so hard to use. They send you to different places and it isn't clear how to get to where you want to go. Like finding out whether you can have an allowance or not. The sort of question every student wants to ask. You Google 'can I get an allowance' and it doesn't say yes or no. It says well there is this factor and that factor, but it doesn't actually tell you the information simply. Regarding those sort of things I would rather not use the Internet and go in person to the Studylink office and have someone tell you the answer straight away. They know all the information because it is their job*." FG3 female

RealMe

Because many of the younger people were studying or had recently studied, they had used RealMe to get StudyLink loans and allowances, but all were unaware of what it was or what else they could do with it.

> "*You try to sign in with Studylink and it just throws you off to another site to register with RealMe."* FG3 male

> *"To register to Vote I had to use RealMe and then it said RealMe isn't working, please try again later."* FG3 female

> *"I'd don't understand what RealMe is. It just their log-in thing so I just type in my name and password."* FG3 female

Online Privacy

Privacy savvy

Young people were not only tech savvy, but also privacy savvy.

> *"I use a lot of privacy settings… If I post something on Facebook (which I very rarely do), I check to see which of my friends can see it. I think you can limit which search engines can look you up, so I'd use that as well."* FG4 female

> **"***On Facebook, if you like things then ads will come up for it. So I just stopped liking things."* FG3 female

> *"I hate cookies, they freak me out … I delete them about once a week. Otherwise they are building a picture of everything you do. Like around ball season, no matter what I was doing, along the side it was all ball dresses."* FG3 female

> "*My profile is really boring to stalkers. Friends can't even see anything really interesting. Some people can post, other people can't. You can't see who I am friends with or photos I am tagged in or things I have posted."* FG3 female

> "*My only location thing is my wall say 'lives in Wellington'. I don't think about using my location, but also I have heard stories about it and I don't want to know. I have turned location off in my settings. I know that GPS used the battery up faster.*" FG3 female

> "*I had my full birthday on Facebook but you can choose what part of your birthday different people can see. Only my friends can see the date, not the year and the public can't see any of it. Where I work: I would share with friends but not the public."* FG3 female

Private information

Certain types of information were more private for young people.

> "*Photos for me: I only want my close friends to see my photos*." FG3 male

> "*You don't tell anybody your passwords*" FG3 female

> "*I wouldn't make a post [with my address in it] public and I definitely wouldn't put may address in the 'About' section."* FG3 female

> "*Even my birthday – I might say the date but I don't say what year I was born in."* FG3 female

> *"You just meet someone casually at a party or something. And they didn't get your number, they would definitely add you on Facebook if they wanted to chat and meet up. Giving out your [telephone] number now is just for friends."* FG3 female

Privacy pragmatists

All of them were privacy pragmatists.

> *"When I want something delivered to me I'll just use my first initial instead of my name. But that doesn't matter because then my email comes up and it is my real name. I don't really think about it. Usually they don't save your information, or you can choose not to have it saved. So I choose not to have it saved so that when I have done the transaction my Debit card information is instantly removed. I don't really mind as long as the parcel gets sent to me really."* FG3 female

> "*I've never really over-thought that sort of thing. I just post my address [for a party] without even thinking about it. I just don't overthink the Internet or think of it as scary. If you would tell someone your details then I would tell them online. You don't think 'this person is going*

> *to get at me' if you know them or have met them before. But obviously with random ads and stuff, you just don't accept them. "* FG3 female

Another example of their privacy pragmatism was the use of their real name on social network sites like Facebook, so that people were able to find them online.

> *"A lot of people don't have their real name on Facebook, but I do. It can make it hard to find people and it's really annoying. [My friend's] mum gave us this big speech last weekend: 'don't put your real name on Facebook', but how is anybody supposed to find you then?"* FG3 female
>
> *"[When you use a nickname or a pseudonym on Facebook] your real name can become a surprise for some people who have been Facebook friends for years."* FG3 female
>
> *"[I use my real name on Facebook*] *but I use a cartoon face as my picture*." FG3 male

Online security

Security savvy

Young people were also security savvy.

> *"My parents say 'never real name; never do blah, blah blah. They are like security, security! I just dismiss it because I think 'you don't know anything about Facebook'*. FG3 female
>
> *"I figure everything is potentially discoverable' If you want to find out something about someone, it is not that hard. The password you have on Facebook is not going to change that."* FG3 female
>
> "*If someone wants to find out about you then they are going to find out. Some I know security is not that strict so on Facebook, I just don't put something up if I don't want someone to find out about it."* FG3 female

Lack of transparency

Although they were both privacy savvy and security savvy, even young people did not understand what was happening to their identity information.

> *"I want to know every single website that knows something about me. Where the information is going and what is happening. Like is Facebook information stored even if I delete it?"* FG3 female
>
> *"I want to know whether the information I provide is confidential or not*." FG3 female
>
> "*I am probably going to provide my details anyway but sometimes you wonder is the information you provide is going to be used against you. Particularly later in life."* FG3 female

Experiences with cyber(-enabled) crime

Young people treated the Internet as a playground, hacking regularly into their friends' accounts for fun as long as they knew that their friends would be able to cope.

> A friend had hacked into a participant's Facebook profile to have her working at a well-known pole dancing/stripper bar - "*I just cracked up [laughing]. Mean [clever]. But I didn't do anything about it. My friends are not going to believe my Facebook profile. I leave my Facebook logged in and go to the bathroom and when I come back my friends will have*

> *written whatever they want to on my page. It's usually funny or kind of horrific and I don't care as long as my parents can't see it*." FG3 female
>
> *"If you are in a room of friends, anyone who gets the chance will do it [play a practical joke on a friend by altering their Facebook profile]. We made it sound like this guy had got his girlfriend pregnant, really real and his mum was ringing him and saying what is going on, are you OK? She thought it was real because older people don't understand it as a joke. Anyone who knew him would immediately know it was a joke."* FG3 female
>
> *"We try to make them sound real. Once I went on Google and got a picture of an ultrasound and I write things like 'can't wait for it to be born' and I tagged a random girl in it. I thought I was so funny. And everyone was congratulating him."* FG3 female

However, some participants did have more serious experiences with hacking into their accounts or other forms of cyber-enabled crime and could easily see and understand the difference to a practical joke.

> *"it's quite easy to distinguish when it's a Facebook hack. I did have an experience of someone putting something that sounded serious on my page and I had all these friends ringing me to ask if I was OK. I didn't even realise it was there because it was on their phone and I couldn't see it. I got really annoyed with that because is wasn't even a funny Frape or Facebook rape as we call it."* FG3 female
>
> "*At school, if you were being bullied you would go and tell the teacher and they would do something about it. But on the Internet… My sister was getting bullied for about three months and I just went on to her account and looked at all the stuff and showed my mum. Up until then she had kept it a secret. You can get bullied so hard on the Internet."* FG3 female

Many of their friends have had bad experiences online and usually knew what to do in those situations.

> *"My friend got hacked on Facebook. She got a message saying change your password. Then she got another saying her password had been changed even though she hadn't done anything. She had data on her phone so she called Facebook and they sorted it out in a few minutes, but if she had not seen it and time had passed who knows what might have happened."* FG3 female

Protecting online identity information

Young people used a variety of methods and behaviours to protect their identity information online.

Using a safe and protected location

Young people were privacy conscious about their location when they wanted to do an online transaction.

> "*Banking or Study link or transactions like that I pretty much stick to doing at home on my laptop or my phone. Basically no one is watching over my shoulder when I am doing is when I am doing it at home."* FG3 male
>
> *"I might do it at Uni if my back is against a wall and I can see where the other people around me are. But if I am in an open mall or the Hub, I wouldn't go online [for banking or other secure transactions*]. FG3 female
>
> "*I do it on my phone, because it's tiny. I do it quickly and no one can see anything*." FG3 female

> *"In our flat we have an open network and so you can see which computers are connected to the wifi. At uni you just make sure everything is set to private so that your computer is not sharing anything. New laptops just do that automatically*." FG3 female

Using privacy settings
All of them used their privacy settings on Social Networking Sites like Facebook.

> *"It used to be the same blanket setting for everything, now every photo and post can have its own settings."* FG3 female

Friends' policy on Social Networking Sites
Young people commonly organised their Facebook friends in separate groups and provided different information to each of these groups.

> *"I have an acquaintances group and I might send something to everyone but acquaintances."*
> *"Or everyone but family."* FG3 female

> *"My mum can think I am working hard on my degree while my friends might be saying 'wow, she drinks too much alcohol'. It's handy that way."* FG3 female

> *"I live in a hall [of residence] and we have a floor group and we are really close like a family. When we go out together we share any embarrassing or funny photos or videos just within the group."* FG3 female

Using minimal information
Most young people tried to minimise the identity information they provided online.

> *"Unless I was buying something, I wouldn't put much [information] on. I'd put my name. My age only if it's necessary... and definitely not location or anything like that."* FG4 female

Using real vs fake information
Young people tried to use fake information as much as possible, both in official relationships and in less serious relationships like on their Facebook page.

> *"I use fake names. Sometimes funny ones, sometimes more serious*." FG3 female

> *"I know so many people who just put a random place where they work. It's almost as a joke."* FG3 female

However, in some official relationships, like in their relationships with government agencies, they didn't feel they had a choice but to provide real information.

> *"You don't get a choice with Studylink. They want to know everything about you and if you lie you get fined a lot of money so you don't lie to them."* FG3 female

Using passwords
Young people used passwords in a similar way to older generations, including using password strategies or having problems with remembering them for some.

> *"I am really bad. Like I might have a different user name but it's because it's not my choice but I can't remember a different password for every different website that I am in. So unless I have to have a capital letter or numbers, which some make you do, I usually use the same one."* FG3 female

> *"I have a different one for my Internet banking, but other than that they are all the same."* FG3 female

> *"I have five separate passwords that I have rotated around my life. It's always been like that. So if I can remember it I just go through the five until I get the right one. I have different passwords for university, my banking. My social networks are all the same one."* FG3 female
>
> *"All social networking the same one; all my banking another one*" FG3 female
>
> *"I just have two sets: one for my professional kind of stuff, jobs and university and the like: and one for the junk webs sites and shopping. Username and password sets…. The junk sites user name is a pseudonym."* FG3 male

Using multiple email addresses

Most of them used multiple email addresses, including one email address for relationships of importance to them and another email address for less important or 'junk' mail.

> *"I have two email addresses: one for real stuff where I want to receive emails and one for just random stuff where you have to have an email, but I just never check that account. The one I don't care about I just use a stupid [fake] username*." FG3 female

Using pop-up blockers

Several of them blocked pop-ups.

> *"I use pop-up blockers, so I never have any of that kind of thing*." FG3 male

Trust in sharing identity information online

Young people usually trusted professionally designed sites more than others. Also, brand recognition and friends with a positive experience of a particular site led to increased trust.

> *"A lot of it is that they look legitimate. Like the layout of the website; if they are a well-known site and you know other people who have used it."* FG3 female
>
> *"For instance I live in a small town and there in'ts much for ball dresses. So I went online and looked on ebay. But my friend went to another site and it looked like the cheapest, crappiest website. I said I don't know if you should do that. She paid $200 and the dress was late. But it turned out that it was all good because the most beautiful dress came. And it had looked like the crappiest website. So you can't tell. You don't know what is fake and what is real anymore."* FG3 female

Online reviews made a difference for some participants, but not for all of them.

> *"I look at the website review and how many reviews a website has. If the reviews are bad then even if it is cheaper, I wouldn't go there."* FG3 male
>
> *"No matter what the reviews are, if it looks really dodgy I wouldn't use it. I'd just find the same thing on a different website. It is so easy to find anything these days."* FG3 female

Location usually didn't influence the trust of young people. Their main interest was finding cost-efficient sites.

> *"The main New Zealand site I use is TradeMe. Most of the other sites are boutiques and they are expensive. The main reason you do the online shopping thing is to find what you want cheaper. So the sites you go to are in Australia, or China. There are no cheap ones in New Zealand."* FG3 female

Young people trusted government websites with their online identity information. However, they didn't think they had a choice and they also didn't know what government agencies did with their information.

> *"I don't think we really have a choice. It's not like they are out to get you*." FG3 female

> "*I trust government websites in that they wouldn't use it [the information I provide] against me or anything. But I don't know what they do with that information. I don't really care because they are not going to harm me in any way. If anything they are probably going to use it for research. I don't know."* FG3 female

Changing online behaviour over time

Growing up in the digital age

Also for young people, using the Internet was a learning experience over time. However, compared to older generations, Internet use was an important part of growing up for them. Most of them not only had become more experienced Internet users over time, but also more private. They were tech savvy, privacy savvy and security savvy.

> *"My profile used to be really public and then I'd just get a lot of random people adding me on Facebook, that I didn't know. I thought this is creepy, so I made it more private and then more private. A lot of people add you on Facebook. Sometimes you know them as just acquaintances so you accept them, but you don't actually know them. So then I went through and deleted a whole bunch of people that it wouldn't be awkward that I had deleted them when I saw them in person. So I had about 1000 and I deleted about 500. That is astonishing that you can delete 500 people that you didn't know really."* FG3 female

> *"When I first had a Facebook account I had so many friends. Like everyone [in my peer group] wanted to have heaps of friends. Like everyone from school added you and you had 800 friends. And if you didn't have heaps of friends everyone looked at you as different. So I had 800 friends at 14 and then I began to think 'this is ridiculous, so I just deleted the entire account.*" FG3 female

> *"I was the opposite. When I first got a Facebook account I was kind of terrified and so behind. And everyone was warning me about my identity and 'don't give away everything, people can find you on the Internet and if you want to get a job later then don't put embarrassing pictures up'. So I decided I needed to know people well. If I had talked to them then I would add them. But now I have become a little bit lenient*." FG3 female

> "*At first I only put people in my Facebook friends if they were in a different country to me. Now I would add them even if they are just next door."* FG3 female

> *"My behaviour has changed a little in the time I've been using the Internet, in that I'm more casual with it. I used to not even put my email address down for things without checking with mum first… but it's become more casual and more open."* FG4 female

Hacking experiences and other online jokes do not change online behaviour

An important part of growing up is teasing your friends and learning where boundaries are. As indicated, young people often did this in online environments, treating the Internet as a playground where you could tease your friends and make fun with them by hacking into each other's account, for example. Young people appreciated online playground situations and knew what was acceptable or not in that respect. Consequently, hacking experiences or other online jokes didn't change their online behaviour.

> "*There is a clear definition of what you can and can't do [in the name of fun]. Social Networking Sites are fine, everything else is just about off-limits*." FG3 male

> *"No, you just crack up laughing, or give them the fingers. Then delete if you want to or just leave it."* FG3 female

> *"That's it: you can delete it. If it's a joke you can go 'ha ha, thanks'. Tag whoever did it so that everyone knows."* FG3 female

Bad experience

Also for young people, a serious bad experience could have a major impact on their online behaviour and usually led them wanting to be more private online.

> *"One thing I am concerned about Facebook is that anybody can save your Facebook picture to their computer. One time a friend messaged me and said he'd been talking to some random dude from China, and he sent me a photo of you. It was like a jokey photo of me trying to be sexy. The guy had labelled the photo 'my dream girl'. That was when I went in and changed all my privileges settings to private. The fact that I am talking about it now … [is an indication of how unsettling this experience was] There are a lot of creepy people out there."* FG3 female

Senior citizens

Internet use as necessity to keep up with changes in society

Many older people considered using the Internet a necessity in order to keep up with changes in society.

> "*It's an essential tool really, to keep up with the times*."FG1 male

> "*That is how the world is going nowadays. You need to be up-to-date*." FG1 male

Several also saw the Internet as critically important in keeping in touch with family.

> *"Helps me keep in close contact with my grandkids, and my nieces and nephews in America. It's like my lifeline – I couldn't imagine being this far away without that."* FG2 female

Offline vs online use

Older people preferred offline interactions and transactions over online transactions, and often found it quite a complex change to use online channels.

> "*For someone of my age, it's quite a hard change to go from someone talking with me and taking me step by step through to the solution to my problem, versus looking at a screen and trying to figure out the jargon on there and going from screen to screen .. I have a hard time doing that*." FG2 female

> "*I signed in to [Facebook]. But I don't have the time to play with it… I can see the potential there for communication with people you otherwise wouldn't see. It isn't possible for people in Auckland to have a cup of tea with you*." FG1 male

Older people also saw offline social interactions as superior compared to online social interactions. They were fearful of a development in society of people having less social interaction as a result of Internet use.

> "[*Social networking is] taking people away from having social interaction. It's much nicer to sit down and have a cup of tea with somebody and have a chat. We had a family occasion last week and I had all my granddaughters there. So I took a bucket out and said put your phones in there – and you're not having them back until you go home. They were all twitchy*." FG1 female

Young people are different compared to older generations

Older people described how young people had a totally different Internet use experience from their own. A few older participants tried to catch up with what young people do online. Some also thought that young people's "continuous engagement" with the online world was "sad" and observed a lack of socialising amongst them.

> "*My other grandkids who have gone off to uni, they're continually doing this [face down over phone] and for me, from back in the day, I don't like it. It's like having the TV on when we're sitting down to eat. It's just not on! It's so we can have time. Otherwise I feel as if I'm losing my grandchildren to technology. Where's the help when they're down and feeling depressed? What can [technology] do for them? Whereas people can do for people.*" FG8 female

> "*When you're rearing grandkids that range from going into high school down to a two year old, rather than stress, I hop on and play games… I have a friend in Canada who's a doctor and we communicate quite a bit on health issues, especially concerning my grandchildren. And what is amazing about it is the grandchildren do their homework on [the internet]. It's a big mind-shift for me. I'm finding it difficult to understand what the kids are being taught in school… so the kids then teach me and show me what they do on the computer to complete their work. I don't agree with it, because when I take them away from the computer and ask them 'what's 4 times 9' – they just look at me. But they should have learnt that. It's amazing for discovering things, like when they Google, and show me things they're doing for their projects…*" FG8 female

> *"It [getting help with Internet use] depends on the ages. Like for the young ones they go from one to the other, and search – all those things. But for us – over that age – we're too scared to do so. I'm still learning but we've got no choice but to do it. Looking at the young kids now - even the little babies bloody do that – pressing all the buttons… Shame on me asking her kid to show me how to do it – she's only about 9 – and look at me over 50 I can't do it. I find it really hard…. They were brought up with technology. For us we have to write everything down.*" FG5 female

> *"I think when we get older we are a little more afraid of breaking it. When I look at my grandchildren they just do it. And I'm trying to catch up with what they do."* FG8 female

Online banking

Only about half of the older age group participants transacted with their bank online. The other half did not trust online banking and preferred to deal with cash over the counter.

> "*I want to go to the bank and see what I'm getting*." FG1 male

> "*There's too much in the press about people hacking these things. I have one account in the bank down the road and I go there to check it out."* F1 male

Like other age groups older people would use online banking for ease and convenience, and they considered banks to be secure sites. Banks had also talked to our older participants of Focus Group 1 about using the online banking facility. Most viewed their bank information online, but did actual payments offline. Their bank statements were sent online.

> "*It's just an information thing. I switch the money about but I don't do any actual banking online*." FG1 female

> *"I don't do a car so I'd have to walk a long way to the bank, so I do banking online. I think I'd be lost without it. I've had no problems with it."* FG1 female

Use of Social Networking Sites

Social networking amongst older participants was fairly minimal and focused on communication with family members. Some had tried and then left.

> "*I've got family on Facebook and they put up pictures of the kids. That's what I'm mainly interested in on Facebook. I got bored with Twitter. I don't bother with Twitter anymore*." FG1 female
>
> "*I signed in to [Facebook]. But I don't have the time to play with it… I can see the potential there for communication with people you otherwise wouldn't see. It isn't possible for people in Auckland to have a cup of tea with you*." FG1 male
>
> "*That's where Skype comes in!*" [for communicating with family overseas] FG1 female

Sharing identity information online: privacy victims

Most of the older participants did not know who or what to trust in these new online environments, which made them hesitant to share their identity information online. If older participants shared their information it was always their real information. It was either that for them or not sharing their information at all.

> "*There seems to be a lot of dishonesty out there, which is another reason why I don't want to get mixed up in it, because you don't know what you're getting mixed up in*." FG1 female

Older people believed there was too much information-sharing requested from them.

> "*There's too much of your information out there anyway. I just don't bother [by not providing any more information*]." FG1 male

They gave up when it got too complicated.

> "*Sometimes you can't fill in some of those fields because they don't apply to New Zealand, and then there's a song and a dance at the bottom – 'you haven't filled the field in'. So I just give up*." FG1 male

Older people also gave up when information demands become too intrusive. Most of them were privacy victims.

> "*Blowed if I'm going to give you personal information just so I can know if it's going to rain today*." FG1 female
>
> "*Doesn't happen if you go in to a shop does it*?" FG1 female
>
> "*I keep it as brief as possible and if they ask again I just don't have anything to do with it*. FG1 female

They often felt as not having any choice but to provide their identity information online.

> "*You don't have a lot of choice these days [with the information you put online]. I ordered something from eBay the other day, but if you don't put your name and address how's the thing going to come to you? It duly arrived in a couple of weeks – it was wonderful*." FG1, male

Although they did not like sharing their identity information, a few participants could see some benefits of doing so.

> “*I signed up to became a VIP (with Number One shoes) – very flash. I don’t think it hurts. I skim over them. If you don’t want a pair of shoes you don’t have to open them. They’re informing us, that’s all*.” FG1 male

Online privacy

Most older participants were very careful in sharing their identity information online and preferred to keep it to a minimum.

> “*The only site I have ever put my details on is RealMe. I needed to do that to get the information I wanted for family research*.” FG1 female

> “*If I want something I get my daughter to do it for me because she does it quite a lot*.” FG1 female

They considered credit card numbers as private information. Most of them had strong security concerns about online shopping.

> “*I won’t buy anything online because I won’t put my credit card details online. You read in the papers and hear on the news about all these scams going on … so I don’t buy anything because I don’t want to put my credit card details online*.” FG1 female

Online security

Older people were afraid of hacking, which they saw as ubiquitous in society. However, most of them also had an attitude of nothing to hide, nothing to fear.

> “*Anyone who wants to hack into my email would go to sleep with boredom*.” FG1 female

> “*My life is an open book … I’ve got my family tree on there. Anyone is welcome to go on there and add stuff to it. They just can’t take stuff off*.” FG1 female

Experiences with cyber(-enabled) crime

Older people had experience with spam and phishing emails, and usually deleted them.

> “*I don’t worry about the rubbish… $10 million from Nigeria, $20 million from the lottery! I don’t waste much time with those*.” FG1 female

One participant found a bank-linked site for reporting suspicious emails, which she used. Another rang the Department of Internal Affairs about an email mentioning Teletubbies but linking to porn:

> “*If that’s online – that’s enough to put you off for a lot of stuff*.” FG1 female

One had an experience while on Facebook of receiving odd messages from someone who was not a contact.

Protecting online identity information

Using minimal information

When they shared their identity information online, older participants used minimal information and always their real identity information.

> “*The only site I have ever put my details on is RealMe. I needed to do that to get the information I wanted for family research*.” FG1 female

Using antivirus software

Most older people had free antivirus software installed and knew about its function and purpose. The SeniorNet initiative was an important source of information for FG1 participants on how to protect themselves online.

Using passwords

Older people frequently mentioned difficulty in remembering their password(s).

> "*It says here she remembers her passwords in a system that only makes sense to her. When you get to our age you can't remember any of that*!" FG1 female

Forgetting passwords was a hassle. Most used the same password for all sites, one participant used multiple passwords. Most wrote down passwords to remember them.

> "*The more you change them the worse it is*!" FG1 female

> "*When I was working we needed four different passwords, and the IT department would then say we needed new ones. I wrote them all down in a notebook, in a row. I've still got that notebook and I write down any password in there. When you open this notebook it looks like a foreign language*." FG1 female

Trust in sharing identity information online

Older people had a relatively high trust in government websites.

> "*RealMe. I trust that one*." FG1 female

> "*Maybe a government site – it's is supposed to be authoritative*." FG1 male

Getting help

SeniorNet was, and continued to be, an important source of learning for FG1 participants.

> "*You learn most of it yourself, fiddling around. But when we have queries we have someone more experienced we can ask."* FG1 female

Judging whether to access something or use a service, was mostly down to whether participants really wanted it and if they had people around them who could offer some help, such as family members.

> "*You can find someone who is using it and ask them what their experience is."* FG1 female

> "*It's not like I'd rush in to something and say 'oh goody something new'. I'd find out about it first. My sons all work in IT, so I'll ask them, and they might say, 'no, that's a bit dodgy Mum, stay away from it'. Or I'll have a look and let you know."* FG1 female

Changing online behaviour over time

Bad experience leads to change in online behaviour

For several participants, a bad experience had caused them to stop doing things online. For example, one participant had experience with a link to a porn site:

> "*If that's online – that's enough to put you off for a lot of stuff*." FG1 female

People from different ethnic backgrounds

Māori

Critical importance of the Internet

For Māori, the Internet was an important tool to connect and communicate with the whānau and iwi – wherever they were internationally and adding on to relationships that already existed.

> *"Someone wrote out a history of our meeting house, and we were going to print it all out and post them out – what a hassle!... So last night I just pdf'd it, put the link on Facebook and there it is, have it, it's out there. And now I don't know how many people have accessed it – from all around the world. I've got messages from people all around the country and overseas who've got it.*" FG7 male

The Internet had become another way to stay connected to Māori culture and people.

> *"I love the Māori television site because I get to go back and watch 2013 kapa haka competitions. I see it as an interactive site. I see how much usage is in te reo Māori and can then gauge my proficiency and see if I want to push myself or just be surrounded by the language. I like that there's no ads. That's really the only one I use."* FG7 female

And to learn about mātauranga and tikanga Māori:

> *"YouTube's great…. Then there's other things like learning waiata. A lot of useful information and a lot of not so useful information."* FG7 male

Online vs offline use

The Māori participants were aware of limits to what can be achieved through online connections in cases where little or no relationship existed in the first place. One recounted their experience of work on a school Board of Trustees trying to improve whānau engagement in the school. Their idea was to move away from mass emails and get back to phone calls and other contact with family.

> *"I'm convinced nothing can replace that face-to-face in that environment where you're building relationships with people who perhaps haven't had a great experience with the education system themselves. Getting them through the door isn't going to happen with a text message or Facebook message or an email*." FG7 female

Sharing identity information online

Given how geographically dispersed Māori iwi and hapū are, there was often a trade-off between providing information where it was widely accessible to the whole iwi or hapū irrespective of whether they were already known, or restricting it to a smaller number of already known members.

> *"On our Marae site, it's a bit of a balancing act: do you want to restrict it, or do you want to get it out there?"* FG7 male; in the end, access to the genealogy part of the website was restricted by password.

The same sort of dilemma existed over whether to put their whakapapa online. A few said they would only provide this through private email to nieces and nephews, while others were comfortable with providing this information on a public Facebook page.

> *"My whānau has a Facebook page and people go online and post all their information."* FG6 female
>
> *"I put it up there [on Facebook] otherwise I get multiple requests for it all the time. Plus a lot of people are searching for the information from around the world."* FG7 male

> *"I met some cousins I didn't know through Facebook so I'm writing about that on Ngati Facebook."* FG7 female

There appeared to be evolving practice about what cultural practices and information was shared online. For example, when an Aunty died and family could not get to the tangi, one participant posted an old photo of her and wrote a poroporoakī (farewell) as if on the marae. He also encouraged the sharing of stories on Facebook for that family member.

Another participant had experienced a family member's death being posted on Facebook because a cousin did not have everyone's phone numbers.

> "*I believe she did it to be practical. This really upset many family members. The seven remaining brothers and sisters felt this was disrespectful to their brother. They didn't think it was appropriate. It was really impersonal… It caused tension, and there was no way to retract that…. Even if I wasn't Māori that wouldn't be how I would communicate that*." FG7 female

Such practice was quite common for the whānau of another participant.

> "*It's the way you do it. It's like an obituary notice*." FG7 male

> "*I didn't see [the notice about a close friend's death] until the day before the funeral because it was only on Facebook and I only check it a couple of times a week*." FG7 female

> "*Cheaper than in the papers. That's why we're not going to the papers so much*." FG7 male

Online privacy

Māori found online privacy critically important.

> *"I think we should always be careful about our information and not be blasé. Like that click here to sign on through Facebook – and there's all my information for you. I think that's a bit too complacent."* FG7 female

Photographs were a particular type of identity information considered more private by Māori. For example, one Māori participant described a situation of her niece who had been photographed at Kapa Haka for a newspaper. Then Destiny Church picked up the image off the paper website, and the photo was also picked up by a cruise ship travel agent.

> "*She's 22 now, but was six at the time. And to be a face of Destiny Church or an international cruise line, is shocking to me. I feel so gutted about her privacy at the time. It's yuk*." FG7 female

Māori uploaded fewer photos to Social Networking Sites now than previously because individuals had heard stories about what had happened to others or could happen to them.

> *"When I learnt that whatever photos you uploaded to Facebook then belonged to Facebook – I took issue with that, and I've only just come back to Facebook after a long time away. I'm more cautious now especially around the children and what I post of them."* FG7 female

Privacy pragmatists

Most of our Māori focus group participants were privacy pragmatists: if the reason for providing their identity information online appealed, then a pragmatic decision was made by them to provide it.

> *"I'm pretty [mercenarily] motivated I guess. If there's a reward for me at the end – and there really is a reward – you can pretty much get whatever you want from me. If I don't see the value in signing up or subscribing, I won't. I see it as, if you want something from me, what*

> *are you giving me?... Then it's on me – if I've chosen to subscribe, then I've given you my information."* FG7 female

Privacy victims

However, some Māori believed there was too much information-sharing requested. When it was too intrusive they would just stop and get out of the online transaction.

> *"Those generic questions are alright – like, 'did you find this information useful? Yes or No'. But as soon as they start asking personal information that's a bit much. Though it does depend on who's asking and I'm a bit anti-establishment. I don't want to help big power companies out with their marketing research so that they can target their advertising to us. But if it were a government agency or a charity asking a question, I might be a bit more flexible."* FG7 female

Privacy optimists

A few Māori participants were privacy optimists and indicated that they would continue using identity information online until something bad happens.

> *"I wonder if we are becoming too over-paranoid about security. We've got to use the internet these days. Just got to be a bit sensible about what sites you use and what sites you don't."* FG7 male

> *"I sometimes draw the line at credit card information. I was going to sign up to LightBox for a free trial but before you can continue you need your credit card. Nah, pass. I did one where I signed up for a year's subscription of a British newspaper. But I obviously didn't read the terms and conditions properly and didn't tick a box which said I didn't want to continue this next year so suddenly on my credit card was a bill for another hundred and forty dollars for another year's subscription… It's a cunning move."* FG7 male

> *"I haven't had a bad experience that's caused a change."* FG7 female

Protecting identity information online

Using fake information

Some Māori used fake information in order to be more safe online.

> *"I think what would someone need to hack my life? It would be name, address and date of birth. So I just try and bury one of those things."* FG7 female

Using pseudonyms

One Māori participant used the opportunity of Māori-ifying his name in order to have a pseudonym available for online use.

> *"I used to 'Māori-ify' my name – that was in the old days. I just use my name now."* FG7 male

Trust in sharing identity information online

There was a lot of cynicism amongst Māori participants about whether some sites could be trusted with their identity information.

> *"I don't trust any sites with lots of those adverts to 'lose lots of weight' or 'become really skinny' or 'feeling lonely?'"* FG7 female

One gave an example of searching for some information online and finding a website that had so many ads you could hardly see the article:

> "*I just exited out straight away*." FG7 female

Some even thought those responsible for providing online support might have had a hand in creating the problem.

> *"We always think Norton's Antivirus [are an organisation you can trust] but you hear this stuff, that they're probably the place that puts out the virus to keep themselves in business. You wouldn't put it past them these days. You just don't know."* FG7 male

A trusted brand usually would help with trust of the related site but even then a bad online experience could happen sometimes.

> *"On the NZ Herald site I clicked on something that I thought was a proper article and it went to some infomercial site. I was quite surprised actually, that they were infiltrating some of what you'd think are quite trustworthy sites."* FG7 male

However, for a few Māori participants, online experience and trust seemed to go hand in hand.

> *"I think I've become more trusting. I've signed up to that RealMe. I don't mind giving my correct information. I've got nothing to hide."* FG7 male

Māori participants' views of government organisations were mixed. On the one hand there was general derisive laughter about trusting government. Others expressed more trust.

> *"I don't have any problem with the government. I signed up [to RealMe]."* FG7 male

Two other participants at least also had RealMe accounts, required because of their connection to StudyLink. One who signed up for RealMe:

> "[*I*] *might have used an old address though. I don't trust that John Key.*"FG7 female

Changing online behaviour over time

For Māori, a quick and helpful intervention after a bad experience could lead to continuing behaviour online.

> "*When my [work] credit card had five thousand put on it by somebody overseas, because my employer was so quick to intervene it made me feel quite safe about continuing to use it online. I don't do anything different with my personal credit cards. So long as it's got an 's' after the http…"* FG7 female

Pasifika

Critical importance of the Internet

To Pasifika, the Internet was highly valuable to search for information related to their Island or culture.

> "*I like to look up Island songs and lyrics 'cause you can find a lot of those online*." FG5 female

The Internet also made up for the unavailability of some services on the Islands.

> *"We're looking for the best price and that's the only way to book because there's no administration in the island that we came from."* FG5 female

For Pasifika people, the ease of making contact even when someone might be at home on a Pacific Island was particularly helpful and made it possible to do things that would have once been impossible.

> "*Where we're situated it's quite isolated. And that's our comms to the rest of the world*." FG5 female
>
> "*When Mum left her bag somewhere. I thought I'll text people. Or then I'll email, but I didn't know everyone's email. So I thought I'll put it on Facebook – 'mum's lost her bag with all her pills. It will cost heaps to replace them'. In ten seconds I got a reply saying 'they're here'… It's the fastest way to get out some information*." FG5 female

Particularly in special times like a birth or a death in the family:

> "*On the other hand, they couldn't get hold of me when Dad passed away. I wasn't on the phone or the email. So my sister did a blanket email to our little island – 'anyone on this island who can get my sister to call me urgently'. Oh yeah, I got like 5 calls*." FG5 female

Sharing identity information online

The information Pasifika people provided online depended on the circumstances and what they thought was reasonable to provide. While most had a Facebook account there was wariness about what was provided there.

> *"I find with Facebook it's got all these updates – update your profile. It's got all these little captions things – you're friends with so-and-so. I'm not interested but it's coming at you, prompting you to finish off your profile. 'You're only 72% completed'. I don't. I just go on Facebook to see what's going on. It's starting to get annoying."* FG5 female
>
> *"I don't give out too much information. I'm wary about people stealing information and using it for themselves…. I have photos up there but nothing like pole dancing!! But I only have close friends and family that are on my page anyway. And if anyone sends a friend request and I don't know them, I don't accept them."* FG5 female
>
> *"I can't recall what I typed in to actually sign up for Facebook. Because that profile asks you lots of questions about what school you went to… I haven't filled in much of that stuff. But to actually get the account they ask for your name and a mobile phone number and an email. That's all you needed – those are the basics… But anything other than those three things, especially an email address ... I won't.* FG5 male

This wariness about providing information extended to other sites as well.

> *"Even things in the government website. Sometimes I won't even go there because it asks you lots of questions."* FG5 male

Online privacy

Privacy victims

Several Pasifika were privacy victims: if they did not trust the site or if they thought the information asked for was too personal in the circumstances, they exited the site without providing the information. Information about their children, income and other financial information was considered as private information.

> *"In that last example [live rugby site] it asked you for name and blah blah blah and it didn't ask for any more personal information like how many children do you have, or what's your income. Because I find that quite intrusive. I'll just back right out. But if it's simple purchasing,*

it's just your name, address phone number and card number. Even that I feel scared giving the card number. It says it's the official site but where do you go to check it's the official site? You just have to be trustworthy that that site's okay." FG5 female

"I usually go there to play games. If they ask questions I just give up and get off." FG5 male

Experiences with cyber(-enabled) crime

Most of the Pasifika had some experience that made them feel unsafe on the Internet, such as unwanted popups or redirection to an unwanted site.

"Those free movie sites are the worst." FG5 female

"I try and close it but for some reason it keeps coming back up. So I just shut the computer off and then go back and I know not to click that button ever again." FG5 female

"It's also scary. When you're searching and it says listen, and you go to some completely horrible random site like 'Date for Free' or 'Girls'. Like losing weight and it's not losing weight it's a pole dancer or …. or otherwise your computer says 'adjust your cookies' and 'okay, I shouldn't be here'" FG5 female

All Pasifika participants had experienced spam and phishing emails but there was no actual experience of loss of money.

"*Twice – twice I've won six point something billion [in an email]. Well, I'm still here. I knew straight away, they are a waste of my time*." FG5 male

A few had experienced stolen identity information and online requests for money, which were ignored.

*"Had a few of those [requests for money]. And also friends who are already my friend asking to accept their new Facebook profile… I don't accept. 'Cause I know someone stole her ID on Facebook."*FG5 female

"I just posted up that someone else was trying to be me – don't accept them. A lot of them already knew. They were saying I was asking for money. But they knew that I wouldn't ask them. They were private messaging me saying 'are you okay'. That's how I found out." FG5 female

"My sister-in-law is a big Facebook user and she likes taking photos and uploads them. She went to a site because it said Tokelau [her home country] and it had one of her photos. She managed to find the photographer, saying 'this is my photo you're using', and he goes 'no it's on the Internet, it's free.' I said maybe you need to look at some copyright to protect it. She was so upset." FG5 female

Protecting identity information online

Pasifika participants used few strategies for online protection. Most had only one email account and the same password was used for every purpose. Antivirus software was one strategy used, as was remembering to log out after use.

"Adjusting the cookies. Or installing the anti-virus." FG5 female

"I think once you log in always log out." FG female

"That's what they offer on lots of sites – to keep you logged in and save your password for this site ... oh never!" FG5 female

> *"Where we live we have our own router and that's secure enough for us. [it's password protected]"* FG female

Public WiFi was rejected because of speed concerns, not for safety reasons.

Using real vs false information

The use of pseudonyms or the provision of fake information was not common practice among the Pasifika participants.

> *"I've got the right information except my name isn't my full name. But I'm thinking back, maybe I should have changed it 'cause someone could steal my info. Too late. Done."* FG5 female

> *"For freebies. If someone says it's free, just fill this in, and I'll go, 'oh just a name or even letters', then when you get to the end they go 'and a real email address', and I go 'oh' and delete… That's why I think I should set up a fake email address just so I can get that stuff."* FG5 female

Some had not even thought of having a dummy email address with fake information.

> *"I've never tried it."* FG female

> *"Not me. I'd get in trouble."* FG5 male

And some thought it might be something to consider:

> *"I might actually do that when I get home."* FG5 female

Concerns for online security

The absence of sophisticated strategies for online protection did not equate to a lack of concern for security. Inaction was more a question of not knowing what to do or where to go for authoritative help.

> *"I worry that when I click on a site a virus is going to come in to my computer. I never used to be big on anti-virus but now I actually spend money for Norton….. I used to just get the free one, then another free one, then another free one. But I found the computer was going slower and stuff was popping up all over the place."* FG5 female

> *"You don't know if it's dead or your laptop!"* FG5 male

> *"I went in to the shop to get [anti-virus] for the ipad ... and they said it didn't need it. Apple has got really top notch security built in. So you don't have to buy add-ons. I didn't know that! You see I don't know. It might be happening but I don't know. All I know is I don't get those clean up cookies, and little malware things happening."* FG5 female

Trust in sharing identity information online

It was generally accepted that the sites the Pasifika participants visited could be trusted.

> *"Never thought about that before. Just go straight on. I don't really think about if they're trusted or not. They're all the same."* FG5 male

This automatic acceptance of trust in a site did not translate to universal feelings of security about online transactions.

> *"I'm pretty trusting 'cause nothing bad has happened to me."* FG5 female

> *"I trust Telecom with what they offer because I've dealt with Telecom for a long time. So I don't really trust the things that come on TV."* FG5 male

And there was trust by those doing financial transactions online that they would be looked after by their bank.

> *"I've never had any issues. I'm quite amazed I've just typed in my credit card number and they've got no security… I do that sometimes. I think, 'oh I'll find out if it's going to… The banks will look after you. That's sort of what I trust sometimes."* FG5 female

Changing online behaviour over time

Pasifika participants had changed their online behaviour over time because of what they had learned from their own experience and that of others.

> *"Before, as a newer user, I would fill in everything. And now you don't need to. You don't need this information to give me what I want. So now I think I'm a smarter user – if I get a funny feeling and think why are they asking that, I'll just stop and leave it. And find another avenue to get what I want."* FG5 female

Learning about online behaviour

Most admitted to learning what should and should not be done online either by learning-by-doing it themselves, or with the help of young people.

> *"Trial and error."* FG5 female

> *"It depends on the ages. Like for the young ones they go from one to the other, and search – all those things. But for us – over that age – we're too scared to so. I'm still learning but we've got no choice but to do it. Looking at the young kids now - even the little babies bloody do that – pressing all the buttons… Shame on me asking her kid to show me how to do it – she's only about 9 – and look at me over 50 I can't do it. I find it really hard…. They were brought up with technology. For us we have to write everything down."* FG5 female

> *"Sometimes you just have to teach yourself to be confident to go online. You will probably end up in China or something, but you get used to it. You learn from doing it yourself sometimes… When I get to 'where do I go next?' - that 'next' will be one of my kids. When the one gets angry I get the other one to help me with the next level. That's how I go. Getting my kids to show me – and these guys as well…. Even at work it's about helping each other."* FG 5 female

> *"I'm still learning to do that [use the tablets introduced for children in class]. I go along to the teachers myself and learn it."* FG5 female

Asian people

Critical importance of the Internet

Asian people had come to depend heavily on constant Internet access for the way they live their lives.

> *"Can't live without it."* FG6 female

> *"It's addictive."* FG6 female

They particularly appreciated the convenience and efficiency of the Internet.

> *"Convenience for banking or for IRD returns, or even paying for a passport. Online is much faster and easier."* FG6 male

> *"A lot of information you can't find in the library, so you go online."* FG6 female

> *"For me it's just really entertainment and socialising. I haven't really used IRD or Internal Affairs website much."* FG6 female

They particularly found the social media app WeChat essential for facilitating personal communications.

> *"I use WeChat more than Facebook. It's like texting too but you can speak straight to it… My mum doesn't like texting because it's a lot slower."* FG6 female

> "*We have WeChat for talking to people face to face. You can use your data – it's much cheaper, and you can see the people*." FG6 female

Online devices

All the Asian participants had smart phones for accessing the Internet as well as a range of other devices such as tablets, laptops, Internet TV and so on. Smart phones were the main devices used for personal communication, most using the app WeChat.

> *"I only use iPad when I watch a movie, because it's bigger."* FG6 female

> *"I use the iPad when I can't find my phone!"* FG6 female

> *"With WeChat can use the iPad as a phone – to talk through the WiFi."* FG6 female

The Asian participants clarified what they liked about WeChat: it was more privacy-friendly compared to Social Networking Sites like Facebook and they felt more in control of their identity information therefore. For example, on WeChat, people could be put into different groups. A similar 'friend' request needed to be sent and accepted also by the recipient. There was an English language version of WeChat and a NZ mobile phone number could be used to register. Video calling was also available.

> "*We all use it [WeChat]. We like it because you are more in control*." FG6 female

> *"On Facebook if I become a friend of [participant], then I can see all of her friends' posts, and all [her] friends can see my posts … I don't like that. There is a lot of junk postings and I have no choice [with Facebook]."* FG6 female

> "*I do check my Facebook updates, but I'm reluctant to post anything there*." FG6 female

Asian participants liked to feel they had some control over what information they shared with whom.

> *"Facebook is blocked in China. And personally I don't like Facebook… When I first heard of it I thought 'it's a dating one!' Don't use the social media ones. Just use WeChat to keep in touch with people in China. And only people I know. And any photos of me or my family I only make public to the family. We can categorise different people."* FG6 female

Sharing identity information online

What information Asian participants tended to share with others was quite variable and depended on context and circumstances.

> *"Sometimes it's not clear cut what information you want to share or not. Family information, personal information you definitely do not share. But photos with a gathering of friends you share, but sometimes it causes problems if you put it there where another group of friends can see. It can be embarrassing. And some people may not respect other people's privacy…. They don't think if some words should be used or not, and they might give offence."* FG6 male

A few Asian people took the conservative stance that information posted online could be accessible more widely than intended, and matched their information-sharing behaviours accordingly:

> *"If you don't want to share, then you don't post anything."* FG6 female

> *"WeChat is like Facebook, in that you don't share any sensitive information there. It's just socialising."* FG6 female

Online privacy

Most Asian participants said that, over time, they had become more careful with what personal information they provided online, and to whom.

> *"Yes. I only now share passport number or financial details with very close friends – person to person [online]. Not the whole group."* FG6 male

Privacy pragmatists

Asian people predominantly were privacy pragmatists and particularly saw the benefit of convenience by using online transactions.

> *"Convenience for banking or for IRD returns, or even paying for a passport. Online is much faster and easier."* FG6 male

> *"I always hesitate when someone asks me for my email address about whether to use my real one. If I use a real one it's quick and easy to answer all the questions because it's real. If I use a fake one then maybe years later I won't remember which one… A bit hard to decide but I always use a real one when I apply."* FG6 female

Private information

Particularly financial information was considered private information.

> *"We don't share credit card details or passport number [on WeChat]. No way."* FG6 female

> *"I only give financial details if I book the [flight] tickets or pay the bills. Nothing else."* FG6 female

Therefore Asian participants took additional steps to protect themselves around online financial transactions.

> *"I check my credit card bills – not often, but I do scan through to see if there's anything suspicious."* FG6 female

> *"At first I didn't realise my credit card details were actually saved with the website so every time I logged on [the details] would just pop in. So once I found this… I would delete the details each time. I would rather trouble myself, take some time and enter all those details again."* FG6 female

> *"My colleague helped another colleague with online payment. It saved her credit card with her colleague's account, and next time it pays a bill it goes on [friends] account. She's wondering why her credit card is getting charged twice."* FG6 female

Passport number and family information were also considered very private by Asian people. Age and salary were less so and the sharing of health information depended on the circumstances and the benefits to the user.

Online security

Asian participants also made considered choices about which Internet connections and devices were more secure.

> *"First I choose a safe device – like iPad is safe – and I use my mobile phone since I've got anti-virus. For internet banking I only do it on my work PC because I work for a bank! It's very secure. And I try not to do too many transactions."* FG6 female

> *"I only use [WiFi] at home to pay the bills. I do it through online banking where you pay by direct payment into their account. Otherwise you have to use a credit card. And sometimes a local trader does something for you and you pay them [by credit card] because you know where they are, and you feel safe."* FG6 male

> *"I don't use other people's computer for banking or credit card details. I always use my home computer or work computer. It's quite obvious."* FG6 female

> *"I've still got my Chinese bank account. I will go online here and transfer money to other friends. So I will do internet banking with Chinese currency, with a Chinese bank in China."* FG6 female

Experience with cyber(-enabled) crime

All Asian participants were very much aware of various forms of cyber(-enabled) crime, especially forms of identity fraud overseas.

> *"My friend had the experience of phone calls from Hong Kong saying you've won lotto and trying to get your bank account details off you."* FG6 male

> *"There are more frauds than before. Because there are a lot of identity frauds in China we are normally quite on alert for things like that. A lot of people are reluctant to use Internet banking. They prefer phone banking because they're not entering a password."* FG6 female

All had experienced some sort of Internet deception and knew how to deal with these situations.

> *"Almost every week I receive multiple emails or text messages saying 'you've won lotto', or 'one million pounds', I simply ignore all of them because there's no such thing."* FG6 male

> *"If people I don't know send me an email, I delete it straight away. I don't even open it up*." FG6 female

One Asian participant had received a phone call purporting to be IRD with a tax credit, but when they provided a phone number someone else later called them back asking for a payment. Another had a phone call from Hong Kong, followed by another call a couple of days later, saying they had won a large amount of money but had to pay a little bit of money first.

> *"So I think for us we don't trust it."* FG6 female

> *"It's becoming common sense now. When people ask for account details you think, hmm. Because you only pay when you want to buy something not when people come to ask you to give [financial details]."* FG6 female

Protecting online identity information

Using real vs fake information

For Asian people, the decision to use real or fake information in online transactions was both context- and security-driven. Their preference was to use fake information wherever possible, as it shielded their valuable identity information.

> *"[Using fake information] depends on the website. If you're applying for an email address you don't have to give a real name, but with e-government, want to apply for a passport or something, you have to give a real number of your credit card."* FG6 male.

Using pseudonyms

The use of pseudonyms in online transactions and communication was also quite common amongst Asian people. For example, some had registered on WeChat with a nickname, as their phone number is the main identifier for registration purposes.

> *"I registered under another name. Only the people who I know, know who I am."* FG6 female

The decision to use a pseudonym was for some dictated by a judgement about the publicness of the online application:

> *"Depends on how safe you feel…We only use real names with our close friends and relatives. Then we feel safe."* FG6 male

> *"But some people are concerned about their privacy."* FG6 female

For others it was more about being able to adopt another persona for some activities.

> *"When I chose a nickname it was for fun, not for privacy, because I can set the privacy part when I agree [or not] for you to join in."* FG6 female

For example, WeChat is partly just a fun place, for teasing friends, playing jokes on them.

> *"We form a group and then we can tease each other. We can also decide what we are going to do tomorrow … all of that."* FG6 female

> *"Unconnected people won't see what we are talking about. It's like a window for us only."* FG6 female

Trust in sharing identity information online

The decision about what to share was linked to the level of trust Asian participants had in a particular app or site. For Asian people, trust was strongly related to online security, which they sometimes assessed with the help of friends who had used a particular site.

> *"Depends on whether it's a trusted website or not, like booking flights. For overseas websites – I don't know."* FG6 female

> *"Sometimes I will check with my friends if they have used this website. Is it safe or not? And I try to avoid paying anything online… I'd rather give them cash. I'm not keen to do online shopping."* FG6 female

> *"Also depends on how secure the website is, and how secure is your computer – whether you have any protections, firewall or something like that. A friend got his credit cards hacked a few times because there wasn't enough security."* FG6 female

Location was also an important condition for trust in a particular site. New Zealand-based websites were more trusted by Asian people.

> *"Definitely. We trust New Zealand websites more than overseas."* FG6 male

In the commercial and online purchasing sphere, Asian participants agreed that reputation and user feedback ratings were important ingredients of trust for them.

> *"There's a well-known online shopping site in China. I use that as well. I feel quite safe."* FG6 female.

> *"There are a couple of Chinese websites, called AliBaba and Hobo. These are popular ones. And we know they are safe, so we feel safe to buy things from there. But other than that, local small companies aren't safe."* FG6 male

> *"Mostly are known by their reputation… If we don't know them, then we simply don't do anything [trading] with them."* FG6 male

> *"Users rate them."* FG6 female

A respected method of protecting the integrity of the financial part of a transaction also contributed to trust.

> *"I think you hold the money with a third party before you receive the goods. Like eBay."* FG6 female

Trust in government sites

Asian people tended to trust government sites more than other websites, for varying reasons.

> *"Generally."* FG6 female

> *"Generally government is more trusted than other websites. You know if something goes wrong you can easily hold them responsible for that. But for some private companies it can be hard to chase them."* FG6 male

> *"Sometimes you have to trust them. When you renew your car registration and things like that, you have to enter your credit card details. So you don't have a choice."* FG6 female

Although online trust was not universal amongst the Asian participants, e.g. doing a tax return online:

> "*Talking to them [IRD] is safer*." FG6 female

Asian people tended to compare government services with their most trusted private sector sites, such as online banking, as a benchmark.

> *"In New Zealand I haven't tried a government website, but with ANZ bank or Westpac, if anything goes wrong with the bank system… they either pay you money or – they're quite reasonable, put it that way. If your card is hacked during the system crash, they will reimburse your money. It's quite fair. It's why I feel safe actually."* FG6 female

> *"There's like a guarantee – if it's not your fault and you've lost money, then you can get your money back."* FG6 female

Changing online behaviour over time

Most Asian people said that negative experiences did not really change their online behaviour because they always stayed aware of safety and remained suspicious about unexpected approaches.

> *"Anything on WeChat that is asking for money – just dump it."* FG6 female

> *"They steal your photo then create a new profile using that photo. And send something to your friends, and they think it's you."* FG6 female

Because Asian people have a lengthy history of Internet use, sometimes participants' behaviour change was well back in the past.

> *"I think it is hard to lose money by banking or other venues. The problem will happen only at this stage with people who are not familiar with the e-banking options. I had my first experience of being hacked 18 years ago when I first had my credit card and I didn't know how to handle it … [story of being duped into giving out credit card details, but then immediately contacting the bank who chased up the people and got the money back.] And that was the lesson I learned."* FG6 male

Asian people changed the apps they favour if they believed they were at risk of having their identity information stolen.

> *"We have a programme called CueCue, similar to WeChat. But unfortunately a lot of your details were stolen. I've got a home-stay student who said his details were stolen and they actually contacted his parents asking for money."* FG6 female

> *"It's very popular, but it's getting outdated because WeChat is becoming more popular."* FG6 female

> *"WeChat is probably more reliable than CueCue."* FG6 female

Asian people's online risk assessment was subject to ongoing reassessment.

> *"But maybe later on problems will come!"* FG6 female

> *“We think WeChat has got security issues. There are always warnings like ‘don’t disclose your bank account number’.* FG6 female

They took steps to verify who they were dealing with online.

> *“With my family we talk about [money] using WeChat but then we phone. Because when you ring you recognise the voice and you talk about it. So this is one of our techniques [to prevent fake requests for money].”* FG6 female

Learning about online protection

Learning about what to do to protect yourself online could come from learning about experiences from others:

> *“From all the stories.”* FG6 female

> *“Most of us also watch Chinese TV at home. So there are all these scary stories about fraud – unbelievable!”* FG6 female

Some Asian sites also warned their users of potential online risks, which Asian people found reassuring.

> *“If you talk about money WeChat will send you a warning automatically from the system, saying ‘don’t discuss any personal details about money’.”* FG6 female

Project recommendations

The findings from the three research phases have led to a number of recommendations about how New Zealanders might be further supported in their online identity information behaviours, especially also in being safe and protected whilst communicating and transacting in a variety of online relationships. Moreover, as part of the conclusion of each focus group we asked the participants what would help them with using the Internet and feeling safe while they did so. We have drawn on their responses in the recommendations below.

Better access to high quality knowledge

Many people 'don't know what they don't know', and often they were finding this out when they were already in the process of trying to do something. Many, particularly inexperienced Internet users, low income and less well educated participants suggested a recommendation of having an 0800 number or something to call and report a problem or get help on a particular site. While most had become used to looking for help with "Aunty Google", they were wanting more reassurance than this gave them.

Recommendation 1 – An 0800 number to call for help

Two further recommendations were suggested as ways of addressing these knowledge gaps:

1) Set up an online panel of more experienced users willing to answer questions about a site or app and share what they have learned with novices.

   "It would be easier to talk with someone than going on Google." FG2 female.

   "People are too smart nowadays. They can just get your phone hacked and you never can detect. Training for me is not that efficient, but information sharing… or raising awareness to people so that they switch on an alert… something like that." FG6 female

2) Set up an authoritative site where people can find information about (how to manage) online risks and which sites can be trusted or not.

   a. There is relatively high trust in the New Zealand government to provide for such an authoritative site:

      "It would be good for the government to confirm 'yes this is a legitimate site'." FG3 female

   b. Where they can find an authoritative (e.g. government-supported) review or rating system of trusted sites, e.g.:

      "In the States they had a place where you could type in a business name and they had a rating. I know my Mum and Dad only went to businesses that were associated with Better Business. It would be nice to have something like that, that was really accessible – not have to get through 12 pages before you got to this piece of information … if they're reputable enough to sign up with Better Business then they're safe. But accessible to computer learners." FG2 female

   c. An authoritative (e.g. government) site with an overview of all banned sites:

> *"A friend used to send me a link of all the banned websites. If New Zealand government could have that kind of website… and a good education programme."* FG6 female
>
> *"Like a scam-wall chat. And we could go there every couple of days to update. See what are the new tricks!"* FG6 female

d. An authoritative (e.g. government) site where people can find authoritative information about what is risky and what is safe online when sharing their identity information (e.g. how safe it is to use public WiFi compared to protected WiFi).

Some of the Focus Group participants drew comparisons with the drive social, drunk driving and family violence social marketing campaigns and the need for a similar approach to raising the general level of community knowledge about the Internet.

> *"Most users will have some degree of uncertainty and are afraid to use it [the Internet]. I think it should be something on a national level like a TV advertisement, saying 'hey, this is the place to go' or 'use this' or 'look out for this code – those are trusted sites'. You need those sorts of things – a blanket. Even if you put it online before you go to Facebook 'this is really Facebook'… That would make me feel better – going to a trusted site."* FG5 female

Recommendation 2 – Set up an online panel of more experienced users willing to answer questions and share their learning and experience with novices

Recommendation 3 - Set up an authoritative (e.g. government) site where people can find information about (how to manage) online risks and which sites can be trusted or not

Education and training

Many of the older users had relied upon someone else in their family network to help them get started. Such help is not always available in family or neighbourhood networks and might not always provide the best or most up-to-date help available. There appeared to be some knowledge and expertise transfer occurring between younger, digital native users to older participants. One older participant made the following recommendation:

> *"I used my neighbour's daughter to set up my computer when I brought it home from Computers in Homes. She came and sat right beside me and showed me how to do it. Pairing young people with old people in this is a really good idea."* FG2 female

Recommendation 4 – Pair young people with older people to offer online support to older people and share young people's knowledge and expertise

For lower income and older participants, the *Computer in Homes* courses and *SeniorNet* courses were a major source of knowledge, training and peer support. There was strong support from the participants in these initiatives for having more of these Computer in Homes and SeniorNet courses available to them:

> *"We're really blessed that we have a safety net.… We can even bring our big black box in here to get fixed up!"* FG2 female
>
> *"More Computers in Homes!"* FG8 female

> *"There's quite a lot of people here who are older, like me, and at home quite a bit, and no contact. I think email is awesome and that Skype thing. I really enjoyed Computers in Homes because we were all on the same page."* FG8 female

However, although Computer in Homes and SeniorNet courses are very useful introduction courses about using the Internet, they do not offer enough insights and knowledge about how people can (better) protect their identity information online and would require additional, more advanced courses on online information behaviour and how to protect yourself online. For instance, many of the online protection strategies discussed in the Focus Groups made many participants think about alternative online information behaviours. A good example were the older people who had never considered, and were not raised as such, providing fake information (also perceived as "lying") or minimising the information they provided in online relationships.

Recommendation 5 – Offer more Computer in Homes and SeniorNet courses, in particular more advanced courses on online privacy and security, and how people can protect themselves better online

In general, the findings from this research demonstrate the critical importance of having knowledge about online privacy, security and strategies to protect your identity information better. The recommendation is to offer more learning and training opportunities to people from various backgrounds on how to keep themselves private online:

> "*You need quite a bit of knowledge [to remove information/keep it private]… The more knowledge you have the more secure you're going to be*." FG4 female

The research findings also show the importance of tailoring the education and training needs of individuals so that different online privacy perceptions and behaviours of people from different ethnic backgrounds, socio-economic backgrounds and age groups can be taken into account.

Recommendation 6 – Offer tailored education and training programmes to people from various backgrounds on how to keep themselves private online

Increased transparency about online identity information

The research findings clearly demonstrate a lack of transparency about how identity information is collected, processed and used in a variety of online relationships. Participants of all ages and levels of Internet experience did not understand how their identity information is processed and used and demanded more knowledge, leading to a recommendation of promoting increased transparency and transparency reporting on how organisations, websites and/or apps collect, process and use online identity information:

> *"Can get caught with in-game purchases with free games you can download from iTunes. They use your credit card number… and suddenly you've got all these expensive purchases for in-game things like 3 green crystals."* FG4 male

> *"I want to know every single website that knows something about me. Where the information is going and what is happening. Like is Facebook information stored even if I delete it?"* FG3 female

Recommendation 7 – Promote increased transparency and transparency reporting on how organisations, websites and/or apps collect, process and use online identity information

Many, even experienced and well educated participants, said that they needed help to understand the digital footprint they are creating when they use particular applications. The lack of transparency about what information is being stored on sites or via apps and exchanged with third parties is a problem for people understanding their digital footprint and deciding what they might do to manage it. Many thought that the following four things would help them with this problem:

1) A requirement for sites available in New Zealand to make a transparent, plain-language disclosure of the information they collect or pass on to third parties;
2) A frequently updated site which contains description of the types of information various sites collect;
3) Advice on how to increase privacy when using particular sites (e.g. Social Networking Sites); and
4) Training on managing your digital footprint. This is particularly important for inexperienced older Internet users and socially unaware younger users.

Recommendation 8 – Promote increased transparency on people's digital footprint and how to manage it

A lack of transparency also leads to lack of trust in online transactions, especially for people with lower education and income levels. Consequently, the promotion of increased transparency and transparency reporting would contribute to higher levels of trust in online transactions. As people from different backgrounds not only have different perceptions of online privacy but also demonstrated that they have different training and education needs around online privacy and security, it is recommended to introduce so-called 'Transparency Impact Assessments (TIAs)' from these varying user perspectives. TIAs would help organisations in their efforts to increase their transparency to varying user groups who have different ethnic, cultural and socio-economic backgrounds and related differentiated education and training needs.

Recommendation 9 – Introduce user-centred Transparency Impact Assessments (TIAs), taking into account different training and education needs around online privacy and security for users from varying backgrounds

Authorised secure Internet access and online identity verification

Several participants indicated that they would feel more safe online if they could have access to authorised secure sites or public kiosks to interact with government agencies online at all stages of the service transaction.

> *"It would be great for government departments to have secure websites to make life a little bit easier for people. I tried to use IRD to check something. Registered a long time ago, forgot my password, it then says I have to ring IRD to do something. But the whole time is too long so I just left it."* FG6 female
>
> *"I think it would be good to have some kiosk-type thing at departments like IRD, where people know it is safe to use and it's quick and convenient. Self-help but safe and secure."* FG6 female

RealMe was perceived as a good option in that respect, but many participants were not aware of it.

> *"This whole RealMe setup I think needs a lot more promotion and that could make life a lot easier as well, if people knew what that was and how to use it. Have you guys heard of RealMe [directed to other participants]? –* couple of others said no, so then an explanation was given as *"a government identification system that could evolve into something quite good".* FG9 male

The research findings also show that an increased uptake of RealMe could solve the problems most participants had with managing multiple passwords in the government space.

Recommendation 10 – Introduce the option for people to safely interact with government agencies online at all stages of the service transaction

Recommendation 11 – Promote RealMe more extensively as a safe online identity verification and single log-on service

All participants, and especially Asian people, were looking for the use of more sophisticated levels of security to protect their online transactions, such as they already see in some transactions like online banking.

> *"Something like what banks do with authentication. So if you were doing something on IRD's website you get a text, like an alert to say it's actually you doing it."* FG6 female

> *"Getting a text with every transaction on your credit card, so you know it is you doing the transaction."* FG6 female

> *"I think now the IRD will record your voice when you ring up. So next time they will match your voice and know it's you… I think that is very good in terms of government agencies."* FG6 female

> *"I think the government agencies are doing some good things already, like they ask you questions to check who you are."* FG6 female

Recommendation 12 – Promote the use of more sophisticated levels of security in online transactions, such as online authentication and identity verification

Cost of online security

Most lower income participants used publicly available freeware for antivirus and malware protection. Those who could afford it had come to realise that higher levels of protection and more up-to-date protection is available through commercial security software. Those who had purchased additional software had fewer problems with unwanted pop-ups, phishing or scam emails, and as a result, felt more secure online. Several participants recommended to reduce the cost of anti-virus programmes with higher online protection levels. It could be possible for instance to make provision of high quality security software for their clients a requirement for ISPs or alternatively government could have a number of mechanisms open to it for lowering the cost of this software and increasing its use.

> *"I reckon they should make those cheaper too – the anti-virus programmes… If you're spending $250 that's quite expensive… So it would be good if they made [anti-virus] part of the [device] package rather than us figure out which is the best one."* FG5 female

A reduction of costs of anti-virus programmes with higher online protection levels might be arranged through regulation of the provider's fee. Other alternative options are for government to negotiate a whole-of-country low fee price for anti-virus programmes with higher protection, and/or to make these anti-virus programmes part of existing (high-speed) networks (e.g. the Ultra-Fast Broadband Initiative and the Rural Broadband Initiative).

Recommendation 13 – Promote the use of anti-virus programmes with higher online protection levels by reducing the cost

A better alignment of digital service design assumptions with user needs or experience

The research findings demonstrate that there can be substantial gaps between the digital service design assumptions of organisations, such as government agencies, and the end-user service needs or experience. We therefore would like to recommend that digital service design assumptions need to be based on empirical facts about users from various backgrounds, including for instance:

- High levels of technology savviness, privacy savviness and security savviness amongst young people, but low levels of government savviness;
- Not every individual has a mobile phone or a mobile phone with an Internet connection available for authentication purposes; and
- All New Zealanders care deeply about their online privacy but differently, and have different privacy support needs.

We also recommend that more research is needed into the requirements of differentiated online user groups and how privacy-by-design, as part of digital service design, looks from a differentiated user perspective.

Recommendation 14 – Make sure that digital service design assumptions are closely aligned with actual user needs or experience

Recommendation 15 – Undertake more research into the varying online user needs and requirements of different groups of the New Zealand population, including how privacy-by-design in digital service provision could be achieved from a differentiated user perspective

References

Lips, M., Eppel, E., Sim, D., Barlow, L., & Löfgren, K. (2014). Kiwis managing their online identity information: I*nterim report - Survey findings*. Wellington: Victoria Univrsity of Wellington http://www.victoria.ac.nz/sog/researchcentres/egovt/research-projects/research-2011/KOI_Interim_Report_19March2014v2.pdf

Annex 1 - Definitions of terms used

Cookies	Small amount of data generated by a visited website which allows personal preferences and settings for that website to be stored on the user's computer
Cybercrime	Criminal activities specifically requiring computers or the Internet, e.g. spreading virus software, hacking
Cyber-enabled crime	Criminal activities which are enabled by computers or the Internet, e.g. phishing is a cyber-enabled fraud
Firewall	Software that helps screen out hackers, viruses, and destructive programmes that try to reach a device being used, via the Internet
Hacking or hacked	Attempting to gain unauthorised access to another person or organisation's computer systems
Hacker	The person doing the hacking, i.e. obtaining access to a user's device or computer system and files over the Internet without the user's permission
iGovt	see RealMe
Identity information	Any personal information that identifies you as an individual
Malware	Computer viruses, Trojan horse, keylogger or other software which a user is either tricked into downloading on to their device or does so by mistake, and results in corruption, or disruption of the users device or information being gathered from the device without the user's knowledge
Online	Any activity or service available on or performed using the Internet
Personal data vault	A service which stores and protects a user's personal data, loaning it only to Internet companies and advertisers trusted and approved by the user. The service might operate in exchange for discounts or rebates for the user.
Personal information	Information about an individual that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context
Phishing	Attempt to acquire sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money) by masquerading as a trustworthy entity in an online communication
Proxy/proxies	Using a proxy prevents others, especially sites visited on the internet, learning about an individual's online behaviour and location by 'bouncing' communications around other networks.
Pseudonym	A name made up by the user
RealMe (previously iGovt)	A New Zealand Government provided service used as a way of verifying user identity so that the same log-in can be used for communications with several government departments
Spam	Nuisance, irrelevant or unsolicited messages sent over the Internet, typically to large numbers of users, for the purposes of advertising, phishing, spreading malware, etc.

Annex 2 – Individual Interview Guide and Observation Protocol

We would like to understand what people are actually doing in sharing and managing their identity information in online environments and why that is, not just what people's perceptions are towards sharing their personal information online. Also, the researchers are not interested in the content of the personal information but only want to know what *types of personal information* (e.g. name, email address, bank details) are being shared online.

Each participant will meet with the researchers in person and at a location of their convenience (e.g. at home, in a public space, at the university), and show the researchers examples of how they share and manage their personal information online in different relationships and using varying online devices, such as a computer, iPad or mobile phone. This will provide the researchers with the opportunity to triangulate information gained from observing what people are actually doing with what they say they are doing in sharing and managing their identity information online.

During each meeting, the researchers will ask further semi-structured interview questions to the research participant about why they manage their online identity information in the way they do and their actual experience with, and response to, forms of cyber-enabled crime.

As preparation for the observation interview, each research participant is asked to keep a log of their online identity behaviour in the 7 days prior to the interview, and share this log with the researchers during the interview meeting.

Interview questions will include the following:

- Background questions regarding demographic variables (age group, gender, geographic location, ethnic background, personal income band, educational background, Internet access);
- Background questions regarding Internet use (frequency, different locations, bandwidth use at home, personal costs involved), the type of devices they use to go on to the Internet and how they use these devices;

- In general, tell us about the activities you have done online in the last 12 months:
    - What activities have you done?
    - When you *have purchased goods or services online*, which types of personal information have you provided and why? Are there any types of information you deliberately did not provide in those relationships and why was that? Could you please show us an example of how you have shared your personal information online in order to purchase goods or services?
    - When you *transacted with New Zealand government agencies online*, which types of personal information have you provided and why? Are there any types of information you deliberately did not provide in those relationships and why was that? Could you please show us an example of how you have shared your personal information online in order to transact with a government agency?
    - When you *used social networking sites with friends, family or colleagues*, which types of personal information have you provided and why? Are there any types of information you deliberately did not provide in those

relationships and why was that? Could you please show us an example of how you have shared your personal information online on social networking sites?

- When you are on the Internet, what do you do to protect your identity information? Could you please show us an example?
- Could you tell us about how you use privacy statements on the Internet?
- Have you had any personal experience with any of the following events? If so, could you tell us more about that particular experience and how you responded?

Annex 3 – Focus Group Interview Guide and Observation Protocol

Through this research initiative, we would like to understand what people are actually doing in sharing and managing their identity information in various online relationships with the private sector, government and through social networking sites and why that is, not just what people's perceptions are towards sharing their personal information online. Also, the researchers are not interested in the content of the personal information but only want to know what *types of personal information* (e.g. name, email address, bank details) are being shared online.

The focus group meetings are the third research activity in this project, which also involved a quantitative survey (phase 1) and qualitative semi-structured interviews with some participant observation (phase 2).

The Focus Group meetings are aimed to further understand and explain the research findings from the survey and the qualitative interviews. These findings will be presented to the focus group participants during the focus group meeting. A second objective of the Focus Group meetings is to explore possible solutions for the New Zealand government in managing risks around the observed online identity information behaviours and people's experiences with cybercrime.

Ten qualitative focus group meetings with representatives of different groups of the New Zealand population will be organised and conducted across New Zealand, with each focus group involving six to ten participants in an in-depth collective discussion of about two hours based on a set of semi-structured interview questions.

The following topics will be explored in each focus group meeting:

- Why do people with overlapping backgrounds share, or don't share, (types of) identity information in varying online relationships?
- Do they have any actual experience with forms of cybercrime or cyber-enabled crime (e.g. identity fraud or theft)? If so, what is their actual experience and how did they respond? Did they change their online identity information behaviours as a result of this experience?
- How do they protect their online identity information?
- Have their online identity information behaviours changed over time and if so, for what reasons?
- What knowledge and understanding do they have about the processing and use of their identity information in various online relationships?
- What levels of trust do they have in varying institutions around the protection of their identity information?
- What would help people in order to be able to better manage any risks around the sharing of their identity information in various online relationships?

Prior to their participation in the focus group meeting, each participant will be asked to fill out a short, anonymous questionnaire with the following type of questions. These questions are similar to the questions asked in the survey:

- Background questions regarding demographic variables: age group, gender, geographic location, ethnic background, personal income band, educational background, Internet access;
- Background questions regarding Internet use: frequency, different locations, bandwidth use at home, personal costs involved, the type of devices they use to go on to the Internet;

- The type of activities they have done online in the last 12 months

Focus Group Meeting Confidentiality Protocol

- All focus group meetings will have confidentiality ground rules. This implies that although the researchers are able to identify the participants their identity will not be revealed to anyone outside the research team. Also, the research team will ensure that participants' identities cannot be linked to their responses in the future;
- In the reporting of the data, confidentiality will be maintained by using pseudonyms. Moreover, data will be aggregated and, with that, not reported at an individual level;
- Each participant will be presented with a participant information sheet and a participant consent form prior to the meeting. A participant's informed consent will be obtained through a signed consent form;
- All written material from the focus group meeting will be kept in a locked file and all electronic information related to the focus group meeting will be password-protected, with access restricted to the researchers. Any audio recordings will be electronically wiped and all interview notes and questionnaires will be destroyed after 5 years.