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

Interim Report – Survey Findings

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

Victoria University of Wellington
March 2014

Acknowledgements

This interim report is the first report with research findings from the research project 'Kiwis Managing their Online Identity Information'. The research is financially sponsored by the Department of Internal Affairs. A final research report will be published later this year. Further information on this research, including electronic copies of the research reports, can be found on the VUW Chair in e-Government website at: www.e-government.vuw.ac.nz

The research is 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, 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: Victoria University of Wellington, Datacom Systems Ltd, Department of Internal Affairs and FX Networks Ltd for their continuing support of independent e-Government research of importance to New Zealand, and the members of the Project Advisory Group for their valuable contributions and support to this research activity.

Table of Contents

KEY FINDINGS[1]

Using the Internet

- The large majority of Kiwis uses the Internet on a regular basis and most of them at home; only 5.4 percent had not used the Internet in the last 12 months
- Most people who did not go on to the Internet^ in the last 12 months, belong to the lower income groups^ or do not have a personal income^. These findings suggest that personal income has an impact on Internet use in New Zealand
- People who have completed primary school only and those without any level of educational achievement responded much more often that they don't go on to the Internet, compared to people with a higher level of educational achievement. These findings suggest that educational background has a significant impact on Internet use
- Younger generations have different online channel preferences compared with older generations. All age groups prefer a PC^, laptop^ and mobile phone^ over any other devices to go online. However, older people prefer to use a PC^ over a laptop^ and a mobile phone^, whereas younger people prefer mostly a laptop^ followed by a mobile phone^ and a PC^
- Younger age groups use the Internet on a mobile device^ more frequently than older age groups
- The proportion of people that used a PC^, laptop^ or mobile phone^ to go on to the Internet increases with income. However, people with an income between $1-$10k^ are also frequently using these devices
- The higher the level of educational achievement, the more likely people have used a PC^, laptop^ or mobile phone^ to access the Internet
- Mobile devices^ to go onto the Internet are much more preferred by Māori^ than non-Māori^. However, Asians^ use a mobile device^ most frequently to go online
- NZ Europeans were the highest users of an e-book reader^

Online activities in the last 12 months

- The most popular activities undertaken on the Internet in the last 12 months were searching for information (99% of Internet users), communication (94%), and purchasing a commercial product or service (87%). The least popular online activities were pretending to be someone else (0.5%), hacking into another person's system or device (2.5%), and online dating (4%)
- A declining trend across age groups can be observed for a variety of activities online, including online personal banking^, online government transactions^, online entertainment^, creating online content^ and using a Social Networking Site^. However, exceptions were found for people going online to search for information^ and to communicate online^
- People from varying educational backgrounds demonstrate different behaviours with regard to their online activities in the last 12 months. For example, people with at least 4 years at secondary school^ were more likely to have purchased commercial goods online^ and have been engaged in online government transactions^, compared to people with lower levels of educational achievement^ or no education^
- All NZ Europeans and Asians indicated searching for information online^ in the last 12 months. However, small proportions of the Māori population^ and Pasifika^ didn't go online to search for information
- NZ Europeans and Māori^ were significantly more likely to have purchased commercial goods or services online^, compared with Asians^ or Pasifika^

[1] *significant finding: $p<0.05$; ^: confidence interval ≥10%

- Of all ethnic groups, Asians^ were mostly engaged in the creation of content online^. Pasifika^ were the least engaged in this online activity
- Participation in online entertainment^ was high amongst all income groups^. However, people with no personal income participated significantly more in online entertainment compared to other income groups
- People with higher incomes^ were more involved in conducting their business online^ than people from lower income groups^

Identity information provided in online commercial transactions

- In general, Kiwis are quite private in online commercial transactions, with the large majority restricting the identity information they share online. Name, contact details (e.g. email address, home address, mobile phone number) and credit or debit card details were mostly provided in online commercial service transactions; information provision about friends, health or insurance were the least common
- Younger generations demonstrate different online privacy behaviours in commercial transactions, compared with older generations. For example, the online sharing of a home address^ declined with age
- 14 percent of young people up to 24 years of age^ indicated that they don't know^ why they provide their identity information in online commercial transactions. They provided this particular main reason significantly more than people of 25 years and older^
- People from different ethnic backgrounds demonstrate varying identity information behaviours in online commercial transactions. For instance, Māori^ were significantly more likely than non-Māori to share identity information in online commercial transactions, including name, home address, educational background information^, NZ citizenship information^, employment details^, health information^, Facebook log-in details^, who their friends are^, and their personal opinions^. The most important reasons for providing identity information in these online transactions also varied for people from different ethnic backgrounds^
- People from varying educational backgrounds demonstrate different identity information behaviours in online commercial transactions, including around their home address^, email address^, health information^, things they do^ and who their friends are^. People with no education^ and those with up to 3 years of secondary education^ also indicate different reasons for providing identity information in online commercial transactions^, compared to people with higher levels of educational achievement^
- People with higher personal incomes^ indicated convenience^ more often as an important reason for providing identity information in online commercial transactions, than those belonging to lower income groups^

Identity information provided in transactions with government online

- In general, Kiwis are quite private in online transactions with government, with the large majority restricting the identity information they share online. 68 percent of the population had transacted online with a government agency in the last 12 months. Name, contact details (e.g. email address, home address, mobile phone number) and IRD number were most frequently provided in online government transactions; Information about a person's insurance, their Health services number and things they do were the least common
- Younger generations demonstrate different online privacy behaviours in transactions with government, compared with older generations. People belonging to the younger age groups^ much more often provided their IRD number^, student number^ and educational background information^ in online transactions with government, compared with people

belonging to older generations^. However, people who are 45 years and older^ shared their passport number^ more in online transactions with government, compared with those from younger generations^. The reasons for providing identity information in online transactions with government is also different for varying age groups^

- People from different ethnic backgrounds demonstrate varying identity information behaviours in their online transactions with government^. For instance, Māori^ were significantly more likely than non-Māori^ to share identity information in online government transactions, including educational background information^, employment details^, social welfare number^, community services card number^, health information^, things they do^ and their personal opinions^. The most important reasons for providing identity information in online government transactions also varied for people from different ethnic backgrounds^
- People with no income and those from the lower income groups demonstrate different privacy behaviours in their online transactions with government, compared to those with a higher income
- People from varying educational backgrounds^ demonstrate different identity information behaviours in online transactions with government^. People with no education^ are significantly more likely than other educational groups^ to disclose various types of identity information in online transactions with government

Sharing identity information as part of social networking

- In general, Kiwis are quite private on Social Networking Sites (SNSs), with the large majority restricting the identity information they share online. Name, who their friends are, email address, location details, LinkedIn profile, relationship status, and their photos, were most publicly shared; the most private information were a passport number, password, financial information, information about criminal convictions, health information and NZ citizenship information
- Younger generations are generally less private with their identity information on SNSs, compared with older generations
- There are different reasons for older generations for providing identity information on SNSs, compared with younger generations. People of 65 years and older^ much more often indicated convenience^ as the main reason for providing identity information on SNSs, compared to people of 64 years and younger^. However, younger people until 44 years of age^ indicate the reason to connect with others^ significantly more than people of 45 years and older^
- People from different ethnic backgrounds demonstrate varying identity information behaviours as part of social networking. For instance, Māori^ were significantly more likely than non-Māori to share the things they do^, personal tastes and who their friends are^. The most important reasons for providing identity information on SNSs also varied for people from different ethnic backgrounds
- People from varying income groups demonstrate different privacy behaviours on Social Networking Sites, including around their home address^, mobile phone number^, health information, employment details^, NZ citizenship status^, SNS site account details^, and LinkedIn profile^. A substantial number of people with varying incomes^ indicated that it didn't bother them^ to provide identity information on SNSs
- People from varying educational backgrounds demonstrate different identity information behaviours as part of social networking. In particular, different behaviours could be observed between people with no education^ and people with some form of educational achievement^. People with lower levels of educational achievement^ and those with no education^ also indicate different reasons for sharing identity information on SNSs, compared to people with higher levels of educational achievement^

Trust in organisations to protect identity information

- There is relatively high trust in New Zealand central government agencies around the protection of identity information, also compared with overseas trust in public sector agencies and commercial organisations. Kiwis mostly trusted banks, health institutions and New Zealand central government agencies to protect their identity information. Overseas online dating sites, New Zealand-based online dating sites and the online gaming industry were the least trusted
- Younger generations tend to trust (varying) organisations more to protect their identity information, compared with older generations
- People from varying ethnic backgrounds demonstrate differences in trust of New Zealand central government agencies^ and Social Networking Services^ around the protection of their identity information
- Personal income had an impact on the extent to which people trusted the protection of their identity information by the online gaming industry^, New Zealand-based online dating sites^ and overseas online dating sites^
- People with varying educational backgrounds demonstrate different levels of trust in organisations to protect their identity information. For instance, people with no education^ had higher trust in insurance companies^, overseas-based online commercial sites^ and overseas-based online dating sites^, compared with people with some level of educational achievement^

Privacy statements

- Only 25 percent of the New Zealand population usually read and are able to understand privacy statements provided in varying online relationships, which suggest room for improvement in this area
- Older generations usually read privacy statements^ on the Internet but do not fully understand them, whereas younger generations^ usually do not read privacy statements on the Internet
- Most respondents across all income groups^ usually read privacy statements^ but do not fully understand them. Respondents with a personal income of $150k or more^ are most likely not to read them

Steps taken to protect online identity information

- Younger generations use different tools and strategies to protect their identity information online compared with older generations. For instance, people between 24-35 years of age^ used the protection strategy of changing privacy settings^ not only more frequently than respondents belonging to the youngest age group ^and those respondents between 35 and 44 years of age^ but also much more frequently than older generations^
- A larger proportion of people with a personal income between $50k and $150k^ use security-protected WiFi^, compared with other income groups^. Respondents with a personal income between $10k-$20k^ use security-protected WiFi substantially less than other income groups^.

User experiences with forms of cybercrime or cyber-enabled crime

- Actual experience with forms of cyber-enabled crime is much less common in New Zealand, compared to overseas experience
- Older generations seem to have different personal experiences with forms of cyber-enabled crime, compared with younger generations. For instance, people from 45 years and over^ had more frequently experienced situations in which malware^ was downloaded onto their device, compared to younger generations^. However, personal experiences around misrepresented goods and services bought online^ were far more common amongst respondents between 18 and 34 years of age^, compared with others^. Stolen credit card details^ was a personal experience reported by people of 35-44 years of age^, those of 55-64 years of age, and people of 75 years and older
- People from different ethnic backgrounds have had varying experiences with forms of cyber-enabled crime. For example, significantly more Māori and Pasifika^ reported the personal experience of misrepresented goods or services bought online, compared with Asians^ and NZ Europeans
- People who have completed primary education^ only significantly more often reported an online personal experience with stolen credit card details^, being tricked into giving money^, being tricked into a romantic relationship^, or with misrepresented goods or services bought online^, compared with people from other educational backgrounds^

EXECUTIVE SUMMARY

This Interim Report presents the findings of a quantitative web survey amongst a representative sample of New Zealanders. A copy of the full survey questionnaire is presented in Annex 1 of this report.

Research objectives

The objectives of this research are to get a deeper understanding of the identity information behaviours of New Zealanders in online commercial transactions, online transactions with government, and on Social Networking Sites (SNSs), and people's actual experiences with forms of cybercrime or cyber-enabled crime. In this study, "*identity information*" means "*any personal information that identifies you as an individual*"; by "online" we mean "*any activity or service available on or performed using the Internet*". Other definitions or further explanations of key terms used in this research are presented in Annex 2 of this report.

Survey design

The New Zealand Electoral Roll was used as the sampling frame for the survey. This particular sampling frame offers the opportunity to arrive at a representative sample for the New Zealand population by selecting potential research respondents on the basis of a set of relevant demographic criteria for this research, such as geographic location, age and ethnicity (*i.e*. Māori descent or not). Stratified Random Sampling Without Replacement (SRSWOR) was used to identify the sample members. Māori ethnicity and age were used to define 14 strata (see Table 4, p.38), within which a simple random sample was taken. An initial sample size of 3,171 names and addresses were randomly selected from the New Zealand Electoral Roll dataset. This number was calculated to ensure that a representative sample of the New Zealand population could be achieved with a reasonable margin of error.

Stratified sampling improves the efficiency of the sample design by forming homogeneous groups (strata) with smaller coefficients of variation. It also allows for more efficient estimates within subpopulations. In this survey, for example, Māori at all age levels were oversampled to ensure smaller measurement errors within this subpopulation. To calculate population estimates of proportions (percentages) or means from a stratified sample, weighted combinations of stratum-specific proportions or means are used. The standard errors of these estimates are formed using formulas involving the stratum-specific standard errors and the sampling fraction of each stratum.

Caution *- the chosen sampling frame has the disadvantage that we could not sample for the following subpopulations:*

- *different ethnic subpopulations within the non-Māori population, such as Pasifika, Asians and NZ Europeans;*
- *males and females*
- *people from different income groups, including people with no income; and*
- *people with different educational backgrounds, including people with no education.*

This has led to very small subpopulations for some of the survey findings (e.g. the number of Pasifika and Asians is relatively low for several subpopulations). This then implies that, although the presented findings are significant[2], some of these findings have large confidence intervals and need

[2] $p < 0.050$; significant findings are indicated with *

to be treated with some caution. Wherever we present survey findings involving large confidence intervals, we have indicated this with ^.

Survey questionnaire

A questionnaire was developed on the basis of an extensive literature study. Research participants could complete the survey online or via a paper-based version. Participation in the survey was anonymous and responses are confidential to the researchers. The survey was made available for participants from the beginning of August 2013 until the end of October 2013, and received a total of 467 responses in two 'rounds' of invitations to the survey, which represents an overall response rate of 15%. As explained earlier, these responses ("raw data") have been weighted in order to arrive at representative findings for the New Zealand population.

Summary Analysis of Survey Responses

We first provide a brief overview of the demographic background of our respondents, followed by a general presentation of the main findings under each survey question. We then focus on four categories where we have observed meaningful differences in the survey findings: age, ethnicity, income and education.

Demographic background of the respondents

The distribution of the survey respondents across age groups is presented in Table 2.

Table 2: Age distribution of survey respondents

18–24 years of age	25–34 years of age	34–44 years of age	45–54 years of age	55–64 years of age	65–74 years of age	>75 years of age
11%	14%	17%	18%	22%	15%	2.9%

The survey respondents lived in the following cities or rural areas:

- Auckland: 26%
- Christchurch: 13%
- Wellington: 11%
- Hamilton: 3.2%
- Dunedin: 4.4%
- Tauranga: 3.9%
- Other cities: 19%
- Rural areas: 19%

38 percent of the respondents were male and 62 percent were female.

The distribution of Māori and non-Māori respondents across the age groups is presented in Table 4.

Table 4: Age and Māori v non-Māori

	18-24	25-34	35-44	45-54	55-64	65-74	75+
Māori	17%	19%	19%	18%	18%	8.9%	1.4%
non-Māori	10%	14%	17%	18%	23%	16%	3.2%

The large majority of the respondents had achieved a higher level of education: 84 percent of the respondents had at least completed 4 years of secondary education, with 64 percent of the respondents having had some form of tertiary education. Few respondents had completed primary education only (3.6%), or had no education at all (1.6%).

Further demographic background details of the respondents can be found in the full report from page 37.

Survey findings

Using the Internet

The large majority of Kiwis uses the Internet on a regular basis and most of them at home; only 5.4 percent had not used the Internet in the last 12 months

95 percent of the New Zealand population had used the Internet in the last 12 months.

Most people used a PC to access the Internet (78%), followed by a laptop or notebook (68%), and mobile phone (55%). There was no significant difference in device use between males and females, except for a disproportionately higher number of males using gaming devices (15%) compared to females (4.7%).

5.4 percent of the respondents had not used the Internet in the last 12 months, reporting the following reasons:

- I do not have a computer;
- Not interested / do not want to;
- Do not know how to use the Internet;
- Happy to leave to other members of the family

Internet users were asked where they access the Internet and how often (see Figure 2, p.41). 82 percent use the Internet at home on a daily basis and 96 percent do so at least once a week. Only 1.1 percent of internet users never use the Internet at home. The second and third most popular location for using the Internet frequently are at work (54%) and on a mobile device (43%). Hardly anybody uses a public library or an Internet cafe to access the Internet.

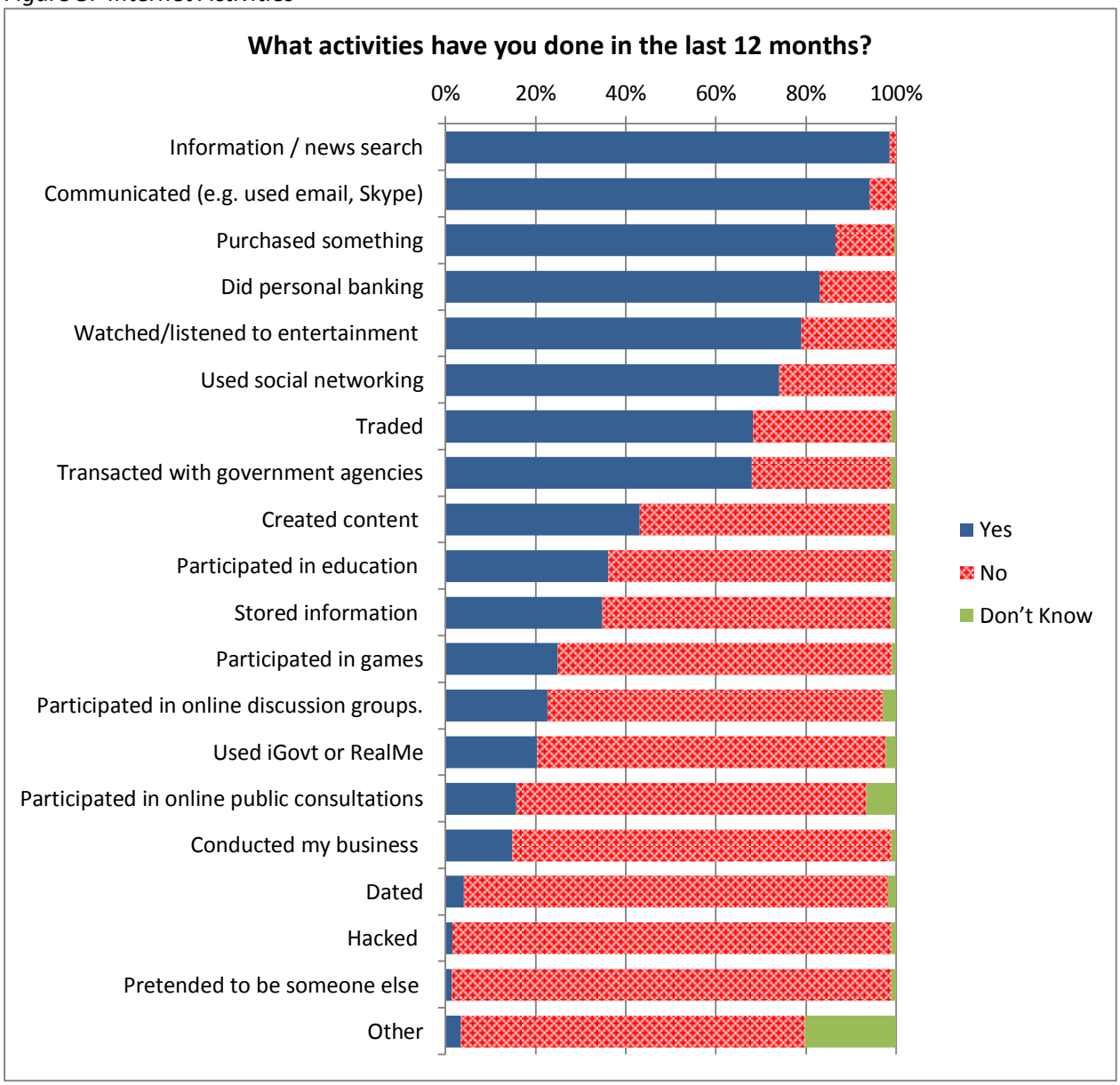
Online activities in the last 12 months

The most popular activities undertaken on the Internet in the last 12 months were searching for information (99% of Internet users), communication (94%), and purchasing a commercial product

or service (87%). The least popular online activities were pretending to be someone else (0.5%), hacking into another person's system or device (2.5%), and online dating (4%)

Figure 3 below provides an overview of people's activities on the Internet in the last 12 months, from most popular to least popular:

Figure 3: Internet Activities



Identity information provided when purchasing goods or services online

In general, Kiwis are quite private in online commercial transactions, with the large majority restricting the identity information they share online. Name, contact details (e.g. email address, home address, mobile phone number) and credit or debit card details were mostly provided in online commercial service transactions; information provision about friends, health or insurance were the least common

Bearing in mind that 87 percent of the respondents had purchased something over the Internet in the last 12 months, participants were also asked what types of personal information they had provided during this process. Name (97%), contact details, such as email address, home address and mobile phone number, and credit or debit card details (93%) were mostly provided in online commercial service transactions (see Figure 4, p.43). Provision of information about friends (8%), health (5.2%), or insurance (3.5%), were the least common. 14 percent of the population provided their Facebook login-in details during this process, which indicates an increasing use of social networking identity information for the purpose of online commercial transactions in New Zealand.

Why identity information is provided in online commercial transactions

The three main reasons for Kiwis to provide identity information in online commercial transactions were:

1. To get the product or service (88%);
2. To complete the transaction (58%); and
3. Convenience (31%)

4 percent of the respondents were not bothered by what personal information they provided in online commercial transactions.

Identity information provided in transactions with government online

In general, Kiwis are quite private in online transactions with government, with the large majority restricting the identity information they share online. 68 percent of the population had transacted online with a government agency in the last 12 months. Name, contact details (e.g. email address, home address, mobile phone number) and IRD number were most frequently provided in online government transactions; Information about a person's insurance, their Health services number and things they do were the least common

68 percent of the population had transacted online with a government agency in the last 12 months, for example to submit a tax form, apply for a benefit, register a vehicle or manage a student loan. Participants were asked what identity information had been provided as part of these online transactions with government (see Figure 5, p.44). Name (93%) and other contact details (e.g. email address, home address, mobile phone number) were the most frequently provided types of personal information in online government transactions. IRD number (73%) and financial information (58%) were also frequently shared with government online. Information about a person's insurance (5.4%), their Health services number (3.9%) and things they do (3.7%) were the least common.

Why identity information is provided in online government transactions

Participants were asked for the three most important reasons why they provided personal information in online transactions with New Zealand government agencies. The most frequently mentioned reasons were the following:

1. To get the service wanted/needed (80%);
2. I was asked to provide the information (46%); and
3. To pay (or receive) tax, ACC levies, fines (35%)

Sharing identity information as part of social networking

In general, Kiwis are quite private on Social Networking Sites, with the large majority restricting the identity information they share online. Name, who their friends are, email address, location details, LinkedIn profile, relationship status, and their photos, were most publicly shared; the most private information were a passport number, password, financial information, information about criminal convictions, health information and NZ citizenship information

Participants were asked to identify personal information they have provided over the last 12 months as part of their usage of a Social Networking Site (SNS) and to whom they have provided it. Respondents were asked to identify whether they have provided a particular type of identity information to no one, friends only, friends of friends, or the public. The identity information most frequently shared was a person's name (34%). Next most publicly shared information, although significantly less so, were who your friends are (9.4%), email address (8.7%), location details (8.6%), Linkedin profile (8.6%), information about your relationship status (8.1%) and photos of you (7.9%).

The most private information, that is, identity information that participants were most likely not to share with any one, was a passport number (100%), password (99%), financial information, such as credit card and bank details (98%), information about criminal convictions (98%), health information (98%), and information about NZ citizenship, residence or visa status (96%). When those who had shared this information only with close friends are taken into account, then passport number is still the most private, i.e. nobody would share this information with close friends, followed by financial information (0.8% share with close friends).

A mean score can be calculated for the degree of 'privacy' of identity information shared on SNSs, where 0 is shared with no-one and 3 is always shared with the public. Figure 6 (p.46) shows the mean 'privacy' scores for all types of identity information.

Why identity information is provided on Social Networking Sites

Participants were asked for the three most important reasons why they provided identity information on SNSs or other sharing sites. The most frequently mentioned reasons were the following, with two reasons equally mentioned as the most important reason for providing identity information:

1. To access the social networking site (54%); to connect with people (54%);
2. To get information (e.g. news, updates from friends, product information) (50%); and
3. To share information with people (35%).

Trust in organisations to protect identity information

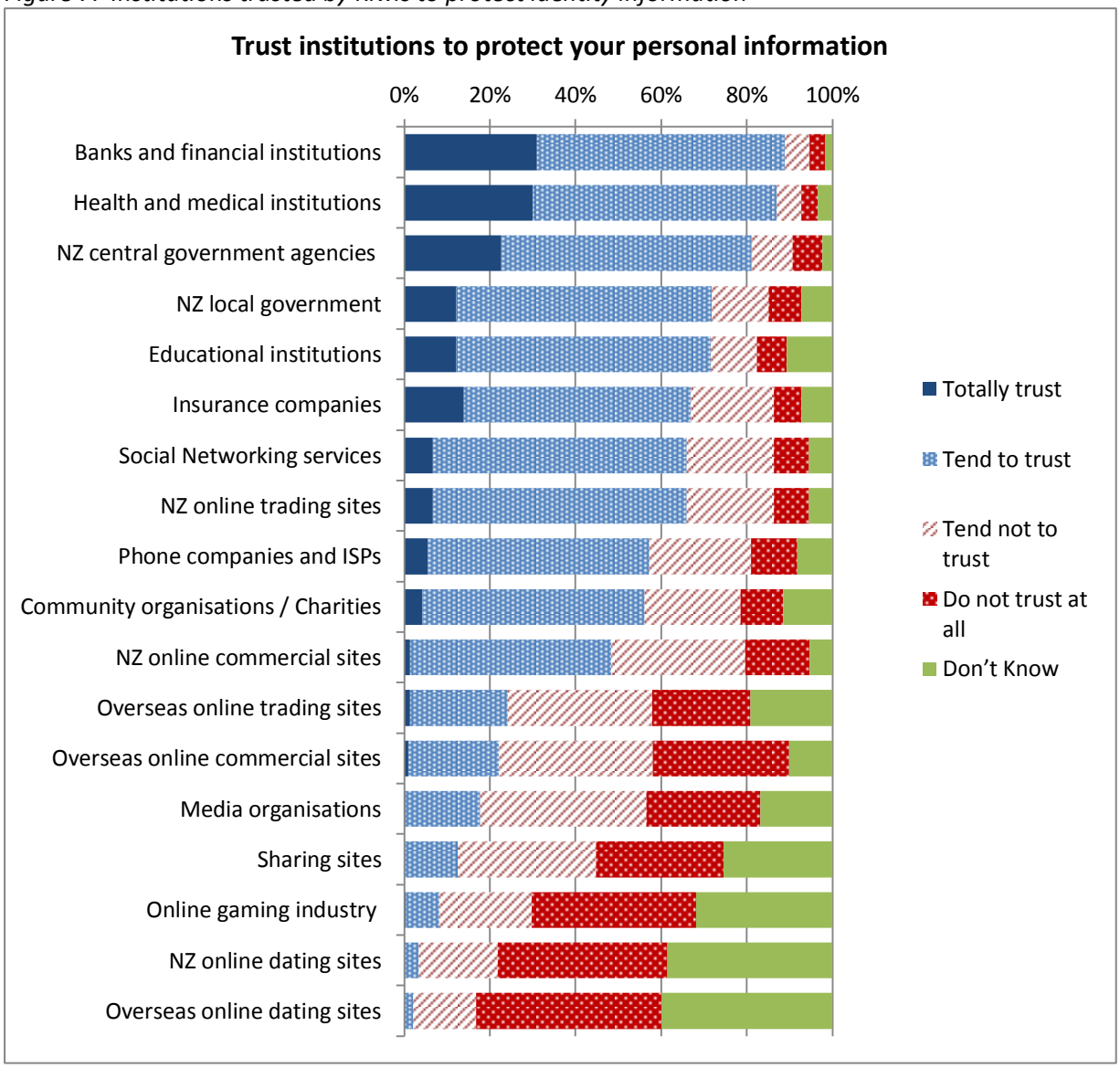
There is relatively high trust in New Zealand central government agencies around the protection of identity information, also compared with overseas trust in public sector agencies and commercial organisations. Kiwis mostly trusted banks, health institutions and New Zealand central government agencies to protect their identity information. Overseas online dating sites, New Zealand-based online dating sites and the online gaming industry were the least trusted

Kiwis mostly trusted banks (89%), health institutions (87%) and New Zealand central government agencies (80%) to protect their identity information (see Figure 7, below). Overseas online dating

sites (2%), New Zealand-based online dating sites (3.4%) and the online gaming industry (8.2%) were the least trusted.

Compared to recent survey findings from the EU (European Commission 2011), where 76 percent of the Europeans responded to fear that their personal data is not safe in the hands of private companies, and 64 percent indicated fearing that their personal data is not safe in the hands of public authorities, we may conclude that Kiwis particularly differ in having a relatively high trust in New Zealand central government agencies around the protection of their identity information.

Figure 7: Institutions trusted by Kiwis to protect identity information



Privacy statements

Only 25 percent of the New Zealand population usually read and are able to understand privacy statements provided in varying online relationships, which suggest room for improvement in this area

38 percent of the population usually do not read privacy statements provided online, 25 percent usually read them but don't understand them, and 25 percent usually read them and understand them. 5.9 percent of the population ignores online privacy statements and 3.3 percent don't know where to find them.

Steps taken to protect online identity information

Participants were asked what they do to protect their identity information when they are on the Internet (see Figure 8, p.50). The five most common protection means reported were the use of antivirus software (94%); limiting the personal information provided online (87%); using tools to limit unsolicited emails such as spam (82%); using a firewall (78%); and using security-protected WiFi (77%). The five least used methods are changing your SNS profile (14%), using a dummy email account (13%), using proxies (8%), using a password generator (5%), and using a personal information vault (2.1%). Another interesting finding is that the number of 'don't know' responses to questions around tools and strategies to protect identity information online is quite high (up to 15% for some questions), which suggest room for more education around available online privacy protection means.

One of the few instances where we can see significant behavioural differences in terms of gender is when it comes to individuals protecting their identity information online. Whereas men and women use most of the online protection tools and strategies, men tend to be more cautious, or aware, about not leaving any traces behind while conducting online activities (see Figure 9, p.50). For instance, men are significantly more likely to delete cookies (77%, compared to 67% for women); use a dummy email account (19%, compared to 11% for women); use a pseudonym (30%, compared to 18% for women); and delete their online search history (68%, compared to 50% for women).

With 87 percent of all respondents indicating that they disclose minimal information about themselves online as a strategy for privacy protection, we may conclude, again, that Kiwis are quite private about their identity information in online relationships, also if we compare this to identity information behaviours demonstrated by people from overseas jurisdictions. For instance, findings from a recent European survey demonstrate that only 34 percent of the European population do not reveal personal information on websites (European Commission 2011). However, with regard to the use of other online identity information protection tools and strategies, Kiwis demonstrate more or less similar behaviours to the Europeans.

User experiences with forms of cybercrime or cyber-enabled crime

Actual experience with forms of cyber-enabled crime is much less common in New Zealand, compared to overseas experience

The most commonly mentioned personal experiences with forms of cybercrime or cyber-enabled crime in New Zealand in the last 12 months, are someone else uploading photos of the person into an online public space without their permission (15%); malware downloaded onto their device (14%); goods or services they bought online were misrepresented (12%); and someone else asking for their bank details (11%) (for a full overview of actual experiences: see Figure 10, p.53). Participants had the least online experience with someone else tricking them into a romantic relationship (0.5%); someone else tricking them into giving money (0.9%); and stolen credit card details (1.0%).

In general, these actual experiences are much less common compared to overseas experiences. For example, in 2012, 38 percent of Internet users across the EU had received emails fraudulently asking for money or personal details; 13 percent had not been able to access online services because of

cyber-attacks; 12 percent had experienced online fraud where goods purchased were not delivered, counterfeit, or not as advertised; and 8 percent had experienced identity theft, such as somebody stealing their personal information and impersonating them online (e.g. in online shopping activities) (European Commission 2012, p.46).

One possible explanation is that Kiwis are more careful with their identity information online compared to people from other countries, and therefore forms of cyber-crime or cyber-enabled crime do not happen that often in New Zealand. Another possible explanation is that Kiwis are less targeted by online thieves or criminals.

Age

Using the Internet

Younger generations have different online channel preferences compared with older generations

All age groups prefer a PC^, laptop^ and mobile phone^ over any other devices to go online. However, older people prefer to use a PC^ over a laptop^ and a mobile phone^, whereas younger people prefer mostly a laptop^ followed by a mobile phone^ and a PC^

Younger age groups use the Internet on a mobile device^ more frequently than older age groups

Online activities in the last 12 months

A declining trend across age groups can be observed for a variety of activities online, including online personal banking^, online government transactions^, online entertainment^, creating online content^ and using a Social Networking Site^. However, exceptions were found for people going online to search for information^ and to communicate online^

Figure 13 (p.56) shows a declining trend across age groups for varying online activities. However, exceptions can be observed for going online to search for information^ and, to a lesser extent, people communicating online^.

Identity information provided in online commercial transactions

Younger generations demonstrate different online privacy behaviours in commercial transactions, compared with older generations. For example, the online sharing of a home address^ declined with age

The sharing of a home address^ in online commercial activities declined with age, with almost 100 percent of respondents between 18 and-34 years of age^ indicating that they had provided their home address^ in online commercial transactions, compared with only 76 percent of the age group of 75 years and older^ doing so (see Figure 14, p.57).

Respondents between 35 and 74 years of age^ provided identity information on their insurance^[3] in online commercial transactions. This development slightly increased for people of 55 and 64 years^ of age and then again for people between 65 and 74 years of age^.

A small proportion of respondents between 35 and 64 years of age^ provided personal information on whether or not they have any criminal convictions^ in online commercial activities[4].

Why identity information is provided in online commercial transactions

14 percent of young people up to 24 years of age^ indicated that they don't know^[5] why they provide their identity information in online commercial transactions. They provided this particular main reason significantly more than people of 25 years and older^

Identity information provided in transactions with government online

Younger generations demonstrate different online privacy behaviours in transactions with government, compared with older generations

People belonging to the younger age groups^ much more often provided their IRD number^, student number^[6] and educational background information^ in online transactions with government, compared with people belonging to older generations^

However, people who are 45 years and older^ shared their passport number^ more in online transactions with government, compared with those from younger generations^

Figure 15, p.59 provides a full overview of the significant findings for the types of identity information that people across age groups share with government online.

A possible explanation for these different online privacy behaviours across generations might be that younger generations prefer online channels over offline channels in their interactions with government, whereas older generations seem to prefer the opposite in government transactions.

Why identity information is provided in online government transactions

The reasons for providing identity information in online transactions with government is different for varying age groups^

Participants of 35 years and older^ more frequently indicated convenience^ as one of the main reasons to provide identity information in online government transactions, compared with people under 35 years of age^.

Respondents between 55 and 74 years of age^ mentioned receiving a price reduction^[7] as one of the most important reasons to provide their personal information in online transactions with government.

[3] 25-34 years: no data
[4] 25-34 years: no data; 65-74 years: no data; 75+ years: no data
[5] 45-54 years: no data
[6] 75+ years: no data

Participants from the younger age groups^ in particular, but also people between 55 and 64 years of age^ (4%), indicated as one of the main reasons to provide identity information in online government transactions that it doesn't bother them^[8].

Sharing identity information as part of social networking

Younger generations are generally less private with their identity information on Social Networking Sites (SNSs) compared with older generations

Younger generations are less private with their identity information on SNSs compared to older generations, as demonstrated by a declining trend for most types of identity information provided on SNSs across different age groups (see Figure 16, p.60).

However, a different pattern is visible for providing SNS account details^ and identity information about websites they visit on SNSs^, with respondents from the youngest and oldest age groups being more private about this identity information than others.

Also, health information is less shared on SNSs by people from younger generations compared to others, with the exception of respondents of 75 years and over.

Why identity information is provided on Social Networking Sites

There is a different value proposition for providing identity information on SNSs for older generations, compared with younger generations.

People of 65 years and older^ much more often indicated convenience^ as the main reason for providing identity information on SNSs, compared to people of 64 years and younger^.

However, younger people until 44 years of age^ indicate the reason to connect with others^ significantly more than people of 45 years and older^.

A small proportion of the respondents of 75 years and older^ (8.4%) indicated getting a discount^[9] as an important reason for providing personal information on SNSs.

Trust in organisations to protect identity information

Younger generations tend to trust (varying) organisations more to protect their identity information, compared with older generations

Trust patterns around what different organisations do to protect personal information are similar across age groups (see Figure 17, p.62). In general, younger generations tend to trust organisations more to protect their identity information than older generations.

[7] 18-24yrs: no data; 25-34 years: no data 35-44 years: no data; 45-54 years: no data; 75+ years: no data
[8] 35-44 years: no data; 45-54 years: no data; 65-74 years: no data; 75+ years: no data
[9] 18-24yrs: no data; 25-34 years: no data; 35-44 years: no data; 55-64 years: no data; 65-74 years: no data

Steps taken to protect online identity information

Younger generations use different tools and strategies to protect their identity information online compared with older generations. For instance, people between 24-35 years of age^ used the protection strategy of changing privacy settings^ not only more frequently than respondents belonging to the youngest age group ^and those respondents between 35 and 44 years of age^ but also much more frequently than older generations^

In general, younger generations use different tools and strategies to protect their identity information online compared with older generations (see Figure 18, p.63). An example is the use of RealMe (formerly iGovt)^ by 48 percent of the youngest age group^ compared to 8.8 percent of the 65-74 years old^, which makes the youngest age group the most active users of RealMe.

People between 24-35 years of age^ used the protection strategy of changing privacy settings^ not only more frequently (90%) than respondents belonging to the youngest age group^ (75%) and those respondents between 35 and 44 years of age^ (70%), but also much more frequently than older generations^.

Similarly, in the case of using tools and strategies to limit unsolicited emails^, people from the age group of 24-35^ are the most active users (93%), followed by respondents belonging to the youngest age group^ (83%) and those between 35 and 44 years of age^ (72%).

A significantly larger proportion of people from the age groups of 45 years of age and over^ do not provide any identity information via online channels^, compared with people of 44 years of age and younger^.

Older generations usually read privacy statements^ on the Internet but do not fully understand them, whereas younger generations^ usually do not read privacy statements on the Internet at all

User experiences with forms of cybercrime or cyber-enabled crime

Older generations seem to have different personal experiences with forms of cyber-enabled crime, compared with younger generations

People from 45 years and over^ had more frequently experienced situations in which malware^ was downloaded onto their device, compared to younger generations^

However, personal experiences around misrepresented goods and services bought online^ were far more common amongst respondents between 18 and 34 years of age^, compared with others^

Stolen credit card details^[10] was a personal experience reported by people of 35-44 years of age^, those of 55-64 years of age, and people of 75 years and older

[10] *18-24yrs: no data; 25-34 years: no data; 45-54 years: no data; 65-74 years: no data*

Ethnicity

Using the Internet

Mobile devices^ to go onto the Internet are much more preferred by Māori^ than non-Māori^. However, Asians^ use a mobile device^ most frequently to go online

NZ Europeans were the highest users of an e-book reader^

9.3 percent of NZ Europeans used an e-book reader^ to go online, which made them the highest users amongst different ethnic groups. Māori hardly used an e-book reader to go onto the Internet and Pasifika^ didn't use an e-book reader at all.

Online activities in the last 12 months

All NZ Europeans and Asians indicated to have searched for information online^ in the last 12 months. However, small proportions of the Māori population^ and Pasifika^ didn't go online to search for information.

NZ Europeans and Māori^ were significantly more likely to have purchased commercial goods or services online^, compared with Asians^ or Pasifika^

Of all ethnic groups, Asians^ were mostly engaged in the creation of content online^. Pasifika^ were the least engaged in this online activity

Identity information provided in online commercial transactions

People from different ethnic backgrounds demonstrate varying identity information behaviours in online commercial transactions. For instance, Māori^ were significantly more likely than non-Māori to share identity information in online commercial transactions, including name, home address, educational background information^, NZ citizenship information^, employment details^, health information^, Facebook log-in details^, who their friends are^, and their personal opinions^

Māori^ were significantly more likely than non-Māori to share the following types of identity information in online commercial transactions:

- Name*: 100%, compared to 97% for non-Māori;
- Home address*: 98%, compared to 92% for non-Māori;
- Billing address*: 97%, compared to 86% for non-Māori;
- Information about their educational background*^: 31%^, compared to 11% for non-Māori;
- Information about their New Zealand citizenship, residence or visa status*^: 27%^, compared to 13% for non-Māori;
- Employment details*^: 30%^, compared to 13% for non-Māori;
- Health information*^: 11%^, compared to 4.3% for non-Māori.
- Facebook log-in details*^: 28%^, compared to 11% for non-Māori;
- Who their friends are*^: 19%^, compared to 6.3% for non-Māori; and
- Personal opinions and tastes*^: 28%^, compared to 16% for non-Māori.

Across ethnic groups, the following differences in identity information behaviours could be observed (see Figure 21, p.67):

- Name*^: 100% of the Māori population provided their name in online commercial transactions, followed by 98% of the NZ Europeans and 91% of Asians^. However, only 77% of Pasifika^ (77%) did so;
- Educational background information*^: Māori^ were significantly more likely in online commercial transactions to provide information about their educational background (31%), than Pasifika^ (16%), Asians^ (16%) or NZ Europeans (11%);
- Facebook log-on details*^: Pasifika^ were significantly more likely to provide their Facebook log-on details (41%) in online commercial transactions, compared to Māori^ (28%), Asians^ (18%) or NZ Europeans (9.7%); and
- Who your friends are*^[11]: Māori^ were significantly more likely to provide information about who their friends are (19%) in online commercial transactions than Pasifika^ (8.2%) or NZ Europeans (6.7%).

Why identity information is provided in online commercial transactions

The most important reasons for providing identity information in online commercial transactions varied for people from different ethnic backgrounds

Non-Māori more frequently indicated getting a financial discount as an important reason for disclosing their identity information in online commercial transactions (10%), compared with Māori (0.1%).

Pasifika^ more frequently provide their identity information in online commercial relationships in order to connect with others^[12] (28%), compared to people from other ethnic backgrounds^.

Identity information provided in transactions with government online

People from different ethnic backgrounds demonstrate varying identity information behaviours in their online transactions with government. For instance, Māori^ were significantly more likely than non-Māori^ to share identity information in online government transactions, including educational background information^, employment details^, social welfare number^, community services card number^, health information^, things they do^ and their personal opinions^

Māori are significantly more likely than non-Māori to share the following types of identity information when transacting with government agencies online:

- Educational background information*^: 46%^, compared to 20% for non-Māori;
- Employment details*^: 61%^, compared to 40% for non-Māori^;
- Social welfare number*^: 34%^, compared to 7.6% for non-Māori;
- Community services card number*^: 34%^, compared to 4.5% for non-Māori;
- Health information*^: 24%^, compared to 7% for non-Māori;
- Things they do*^: 9.4%^, compared to 2.9% for non-Māori; and
- Personal opinions*^: 19%^, compared to 7.8% for non-Māori.

[11] Asians: no data
[12] Asians: no data

Across ethnic groups, the following differences in identity information behaviours could be observed (see Figure 22, p.69):

- Educational background information*^: Māori^ (46%) were the most likely to disclose educational background information in online transactions with government, followed by Pasifika^ (26%) and Asians^ (26%). NZ Europeans^ (19%) were the least likely to do so;
- Social welfare number*^[13]: Māori^ (34%) were significantly more likely than NZ Europeans (8%) or Asians^ (4.7%) to disclose their social welfare number in online government transactions;
- Community service card number*^[14]: Māori^ (34%) were far more likely than Asians^ (8.7%) or NZ Europeans (4.2%) to disclose their community service card number in online government transactions;
- Health information*^: Māori^ (24%) and Pasifika^ (23%) were more likely than Asians^ (11%) to provide health information in online transactional relationships with government. However, NZ Europeans were the least likely to do so (6.2%);
- Things you do*^: Pasifika^ were more likely to disclose the things they do in online government transactions (12%), than Asians^ (9.9%) or Māori^ (9.4%). However, NZ Europeans were significantly less likely to do so (1.9%);
- Personal opinions*^: 50% of the Pasifika^ population provided their personal opinions in online government transactions, compared to 19% of Māori^ and 9.9% of the Asian people^. NZ Europeans were the least likely to do so (6.3%).

Why identity information is provided in online government transactions

The most important reasons for providing identity information in online transactions with government varied for people from different ethnic backgrounds^

Māori^ (14%) were significantly more likely than non-Māori (2.8%) to share information with government agencies online in order to get a service adapted to their personal needs^.

Māori^ were also more likely to do so in order to ask a question^ (8.6%) compared with non-Māori (2.8%). However, non-Māori^ were more likely to indicate compliance with the law^ as one of their most important reasons to share their identity information with government agencies in online transactions (29%), than Māori^ (16%).

Across ethnic groups, the following differences around the most important reasons to disclose identity information in online government transactions could be observed (see Table 12, p.70).

Asians^ and Pasifika^ were more likely to disclose identity information in online government transactions for the reason of being a good New Zealander^. However, only few Māori and NZ Europeans indicated this particular reason.

Pasifika^ and Māori^ were more likely to provide identity information to government online in order to get a service adapted to their personal needs^, than Asians^ or NZ Europeans.

Pasifika^ were much more likely to provide their identity information in order to engage with government^, compared with other ethnic groups^.

[13] Pasifika: no data
[14] Pasifika: no data

Sharing identity information as part of social networking

People from different ethnic backgrounds demonstrate varying identity information behaviours as part of social networking. For instance, Māori^ were significantly more likely than non-Māori to share the things they do^, personal tastes and who their friends are^

Māori^ are significantly more likely than non-Māori to share on SNSs the things they do^, personal tastes and opinions, and who their friends are^.

Across ethnic groups, the following differences in identity information behaviours could be observed (see Figure 24, p.72):

- Home address*^: NZ Europeans were the most private about their home address on SNSs, followed by Asians, Māori and Pasifika^;
- Mobile number*^: NZ Europeans were the most private about their mobile number on SNSs, followed by Pasifika^, Māori^ and Asians^;
- Who your friends are*^: NZ Europeans were the most private on SNSs about who their friends are, compared with other ethnic groups^;
- Details about your location*^: NZ Europeans were more private about their location details than other ethnic groups^;
- Financial information*: Pasifika were the most private about their financial information on SNSs and did not disclose this information at all. NZ Europeans, Māori and Asians were slightly less private about their financial information on SNSs;
- Health information*: Pasifika and Asians were the most private on SNSs about their health information and did not disclose this information at all. NZ Europeans and Māori were slightly less private about their health information on SNSs; and
- Information about any criminal convictions*: Pasifika and Asians were the most private on SNSs with information about any criminal convictions and did not share this information at all. NZ Europeans and Māori were slightly less private about such information.

Why identity information is provided on social networking sites

The most important reasons for providing identity information on Social Networking Sites varied for people from different ethnic backgrounds

Non-Māori were significantly more likely to share identity information on SNSs for fun (15%), compared with Māori (4.8%). Within this subpopulation of non-Māori, NZ Europeans share their identity information on SNSs for fun^[15] significantly more often (17%) than other ethnic groups^.

However, Māori were significantly more likely to share their information in order to get a discount (1.3%) compared with non-Māori (0.1%).

[15] Pasifika: no data

Trust in organisations to protect identity information

People from varying ethnic backgrounds demonstrate differences in trust of New Zealand central government agencies^ and Social Networking Services^ around the protection of their identity information

Asians and Pasifika^ had higher trust in New Zealand central government agencies^ to protect their identity information, compared with NZ Europeans and Māori (see Figure 25, p.73).

Māori^ tended to trust Social Networking Services^ more than non-Māori. However, Pasifika^ had the highest trust in Social Networking Services^ to protect their identity information (see Figure 25, p.73).

User experiences with forms of cybercrime or cyber-enabled crime

People from different ethnic backgrounds have had varying experiences with forms of cyber-enabled crime. For example, significantly more Māori respondents^ (32%) and Pasifika^ (23%) reported the personal experience of misrepresented goods or services bought online, compared with Asians^ (13%) and NZ Europeans (8.8%)

People from different ethnic backgrounds reported the following experiences with forms of cyber-enabled crime (see also Figure 26, p.74):

- Credit card details stolen*^[16]: A larger proportion of Pasifika^ reported to have had the personal experience of stolen credit card details (10%), compared with other ethnic groups^;
- Someone else hacked into your online device*^: Significantly more Asian respondents^ (20%) and Pasifika^ (14%) reported the personal experience of someone else hacking into their online device, compared with Māori^ (4.7%) and NZ Europeans (3.2%);
- Goods or services bought online were misrepresented*^: Significantly more Māori respondents^ (32%) and Pasifika^ (23%) reported the personal experience of misrepresented goods or services bought online, compared with Asians^ (13%) and NZ Europeans (8.8%);
- Someone else tricked you into a romantic relationship*: Slightly more Māori respondents reported to have had the personal experience of being tricked into a romantic relationship (2.3%), compared with non-Māori participants; and
- Someone else tricked you into giving them money*^[17]: Substantially more Asian respondents^ (8.3%) reported the personal experience of someone else tricking them into giving money, compared with Māori (1.4%) and NZ European respondents (0.4%).

Income

Using the Internet

The proportion of people that used a PC^, laptop^ or mobile phone^ to go on to the Internet increases with income. However, people with an income between $1-$10k^ are also frequently using these devices

[16] Asians: no data
[17] Pasifika: no data

The proportion of people that used a PC^, laptop^ or mobile phone^ to go on to the Internet increases with income, with the exception of people with an income between $1-$10k^ (see Figure 27, p.75). A possible explanation for higher use of these devices by this income group is that it involves a relatively large number of individuals from the younger generations (e.g. students).

People with the highest personal incomes used the Internet slightly more at home compared to others. People with the highest personal incomes^ also used the Internet almost every day at work, whilst respondents belonging to income groups of $70k and less^ used the Internet at work less frequently.

Respondents with no personal income^ or an income of up to $10k^ made more frequent use of the Internet at school^ compared to others^.

People hardly used the Internet at a public library^; those with a personal income of up to $10k^ used the Internet at a public library slightly more than others^.

Most people who did not go on to the Internet^ in the last 12 months, belong to the lower income groups^ or do not have a personal income^. These findings suggest that personal income has an impact on Internet use in New Zealand

The large majority of Kiwis who did not go on to the Internet^[18] in the last 12 months, belong to the lower income groups^ or do not have any personal income^ (see Figure 27, p.75). A possible explanation could be that the costs of Internet use in New Zealand have an impact on the decision to use the Internet.

Online activities in the last 12 months

Participation in online entertainment^ was high amongst all income groups^. However, people with no personal income participated significantly more in online entertainment compared to other income groups

Participation in online entertainment^ was high amongst all income groups^ (see Figure 29 , p.77). However, respondents with no personal income participated significantly more (100%) in online entertainment compared to other income groups^, with people earning a personal income between $10k and $20k^ participating the least (68%).

People with higher incomes^ were more involved in conducting their business online^ than people from lower income groups

Respondents with a personal income of more than $150k^ were mostly involved in conducting their business online^[19] in the last 12 months (47%), followed by people belonging to personal income groups of $100k-$150k^ (24%) and $70k-$100k^ (22%) (see Figure 29. p.77).

[18] $100k-$150k: no data; $150k+: no data
[19] $0: no data; $10k-$20k: no data

Identity information provided in online commercial transactions

A significantly larger proportion of people earning a personal income between $20k-$30k^ (34%), an income between $100k-$150k^ (28%), or an income between $30k-$50k^ (17%), shared information about their New Zealand citizenship, residency or visa status^ in online commercial activities in the last 12 months.

Why identity information is provided in online commercial transactions

People with higher personal incomes^ indicated convenience^ more often as an important reason for providing identity information in online commercial transactions, than those belonging to lower income groups^

Identity information provided in transactions with government online

People with no income and those from the lower income groups demonstrate different privacy behaviours in their online transactions with government, compared to those with a higher income

People with no income and those from the lower income groups demonstrate different privacy behaviours around particular types of identity information in their online transactions with government, compared to those with a higher income (see Figure 32, p.80). In several cases, an exception can be observed for those belonging to the $0 to $10k income group:

- Insurance information*^[20]: People with no personal income^ more frequently shared their insurance information in online transactions with government, compared to people with an income^.
- Educational background information*^: a significantly larger proportion of people with no income^ or an income between $10k and $30k^ shared information about their educational background in online government transactions, compared with other income groups^.
- Information about NZ citizenship, residency or visa status*^: More than half of the people with no income^, or an income between $10k and $30k^, shared information about their NZ citizenship, residency or visa status.
- Social welfare number*^[21]: a significantly larger proportion of people with an income between $10k and $30k^ or no personal income^ shared their social welfare number in online government transactions.
- Community service card number*^[22]: A significantly larger proportion of respondents earning a personal income of $30k or less^, or with no personal income^, shared their community service card number with government online.
- Health services number*^[23]: A significantly larger proportion of respondents earning an income between $20k and $30k^ (22%) shared their health services number with government online.
- Student number*^[24]: The large majority of respondents with no personal income^, but to a lesser extent also those with a personal income between $0 and $30k^, shared their student number with government online.

[20] $1-$10k: no data; $10k-$20k: no data; $70-$100k: no data; $150k+: no data
[21] $70k-$100k: no data; $100k-$150k: no data; $150k+: no data
[22] $70k-$100k: no data; $100k-$150k: no data; $150k+: no data
[23] $0: no data; $10k-$20k: no data; $70k-$100k: no data; $100k-$150k: no data; $150k+: no data
[24] $100k-$150k: no data; $150k+: no data

Sharing identity information as part of social networking

People from varying income groups demonstrate different privacy behaviours on Social Networking Sites, including around their home address^, mobile phone number^, health information, employment details^, NZ citizenship status^, SNS site account details^, and LinkedIn profile^

People from varying income groups demonstrate different privacy behaviours on SNSs around the following types of identity information (see Figure 33, p.81):

- Home address*^: Respondents with a personal income between $10k and $50k^ shared their home address on SNSs slightly more than others and, if they did so, only with close friends.
- Mobile phone number*^: Respondents across all income groups^ and including people with no personal income^ had shared their mobile phone number via SNSs. However, they only shared this with close friends.
- Health information*: Only people with a personal income between $10k and $30k shared their health information on SNSs, and restricted to close friends.
- Employment details*^: Respondents with a personal income between $50k and $150k^, or those with a personal income between $10k-$20k^, shared their employment details on SNSs more than people belonging to other income groups^.
- Information about NZ citizenship, residency or visa status*^: People from all income groups^ shared information about their New Zealand citizenship, residency or visa status on SNSs with close friends only, except for respondents with no personal income, who did not share any information at all.
- Personal SNS site account details*^: People from all income groups^ shared their personal SNS site account details on SNSs with close friends only, except for participants with a personal income of $150k or more, who did not share this information at all.
- LinkedIn profile*^: People with a personal income of $70k or more^ shared their LinkedIn profile on SNSs significantly more than respondents from other income groups.

Why identity information is provided on social networking sites

A substantial number of people with varying incomes^ indicated that it didn't bother them^ to provide identity information on SNSs

Trust in organisations to protect identity information

Personal income had an impact on the extent to which people trusted the protection of their identity information by the online gaming industry^, New Zealand-based online dating sites^ and overseas online dating sites^

The higher the personal income, the more people were distrustful of the protection of their personal information by the online gaming industry^.

Respondents across all personal income groups^ tended not to trust online dating sites^ around the protection of their personal information, or did not trust them at all. The geographical location of these online dating sites^ did not seem to have an influence on the trust levels of respondents.

Privacy statements

Most respondents across all income groups^ usually read privacy statements^ but do not fully understand them. Respondents with a personal income of $150k or more^ are most likely not to read them

Steps taken to protect online identity information

A larger proportion of people with a personal income between $50k and $150k^ use security-protected WiFi^, compared with other income groups^. Respondents with a personal income between $10k-$20k^ use security-protected WiFi substantially less than other income groups^

Education

Using the Internet

The higher the level of educational achievement, the more likely people have used a PC^, laptop^ or mobile phone^ to access the Internet.

The higher the level of educational achievement, the more likely respondents had used a PC^ or a laptop^ to go on to the Internet in the last 12 months (see Figure 37, p.85).

Mobile phone^ use is significantly higher amongst people who have completed at least 5 years of secondary education^ and people with no education^.

People who have completed 5 years at secondary school^ had used a game console^[25] much more than those from other education backgrounds^.

People who have completed at least 5 years at secondary school^ are more likely to have used the Internet at school^, compared to people with lower levels of educational achievement^.

People from different educational backgrounds rarely used the Internet at a public library^.

People with some form of tertiary education and those who have completed primary school^, had used the Internet at work^ much more often and at least on a weekly basis, compared to respondents from other education backgrounds^.

People who have completed at least 5 years at secondary school^ and people without any level of educational achievement^ had used a mobile device^ to go onto the Internet more often than people with other levels of educational achievement^.

[25] No education: no data

People who have completed primary school^ and those without any level of educational achievement^ responded much more often that they don't go on to the Internet^, compared to people with a higher level of educational achievement^. These findings suggest that educational background has a significant impact on Internet use

Respondents who have completed primary school^ (35%) and those without any level of educational achievement^ (28%) substantially more often indicated that they don't go on to the Internet^, compared to people with a higher level of educational achievement^; only 1.4 percent of respondents who have completed some form of tertiary education indicated that they don't go on to the Internet. These findings suggest that educational background has an impact on Internet use.

Online activities in the last 12 months

People from varying educational backgrounds demonstrate different behaviours with regard to their online activities in the last 12 months. For example, people with at least 4 years at secondary school^ were more likely to have purchased commercial goods online^ and been engaged in online government transactions^, compared to people with lower levels of educational achievement^ or no education^

People with at least 4 years at secondary school^ were more likely to have purchased commercial products or services online^ and transacted with government online^, compared to people with lower levels of educational achievement^ or no education^ (see Figure 39, p.87).

People with some form of tertiary education^ and those with no education^ had participated in online public consultations^ substantially more than others.

The large majority of people with no educational background^ had engaged in the creation of content online^ and had stored information online^ in the last 12 months.

People with a primary school background^ were the highest users of online education^, followed by those with no educational background^ and those with a tertiary education background^. Others^ had much less participated in online educational activities.

97 percent of people with only a primary school background^ had engaged in online entertainment^, compared with 56 percent of people with 3 years of secondary schooling^, who were the lowest online entertainment users.

People with a primary school background^ and people with some form of tertiary education^ were also mostly engaged in conducting a business online^[26].

Identity information provided in online commercial transactions

People from varying educational backgrounds demonstrate some differences in identity information behaviour in online commercial transactions, including around their home address^, email address^, health information^, things they do^ and who their friends are^

[26] No education: no data; 3yrs secondary school: no data

The following types of identity information were shared differently by varying educational groups in online commercial transactions (see Figure 40, p.89):

- Home address*^: People with 3 years of secondary schooling^ were the most private in online commercial activities about their home address;
- Email address*^: People with 3 years of secondary schooling^ also did not disclose their email address in online commercial activities as much as other respondents^;
- Health information*^[27]: People with no schooling background^ were more likely to provide their health information in online commercial activities than others^;
- Things you do*^: People who had completed primary school^ or those with no education^ were significantly more likely to provide information about things they do in online commercial transactions than people with higher levels of educational achievement; and
- Who your friends are*^: People with no education^ were significantly more likely to provide information about who their friends are in online commercial transactions than people with some level of educational achievement^.

Why identity information is provided in online commercial transactions

People with no education^ and those with up to 3 years of secondary education^ indicate different reasons for providing identity information in online commercial transactions^, compared to people with higher levels of educational achievement^

People with no education^ were significantly more likely to respond that they had provided identity information in online commercial activities in order to get a personalised service^, or to ask a question^[28], than people with some level of educational achievement^.

People who had completed primary school, but also those who had completed 3 years at secondary school indicated significantly more often to provide identity information in online commercial activities for fun^[29], compared with people with higher educational achievements^.

Identity information provided in transactions with government online

People from varying educational backgrounds^ demonstrate different identity information behaviours in online transactions with government^

People from varying educational backgrounds demonstrate different identity information behaviours in online transactions with government (see Figure 41, p.91). The following differences could be observed:

- Health information*^[30]: People with lower levels of educational achievement had significantly more often provided health information in online transactions with government, than those with some form of tertiary education;

[27] Primary school: no data; 4yrs secondary school: no data
[28] Primary school: no data; 5yrs secondary school: no data
[29] No education: no data; 4yrs secondary school: no data
[30] No education: no data; 4yrs secondary school: no data

- Educational background*^[31]: People with at least 5 years of secondary schooling^ had much more often provided educational background information in online government transactions, compared to people with lower levels of education^;
- Student number*^[32]: People with at least 5 years of secondary had more often provided their student number in online transactions with government.

People with no education^ are significantly more likely than other educational groups to disclose various types of identity information in online transactions with government^

People with no education are significantly more likely than other educational groups to disclose the following types of identity information in online transactions with government (see Figure 41, p.91):

- Social welfare number*^: People with no education^ had far more provided their social welfare number in online government transactions than people with some level of educational achievement^;
- Community service card number*^: People with no education^ had more often provided their community service card number in online government transactions than people with some level of educational achievement^;
- Information about any criminal convictions*^: Particularly people with no education^ but also those with a primary education background^, had provided information about criminal convictions to government online; and
- Personal opinions*^: People with no education but also those with a primary education background^ had provided personal opinions in online transactions with government.

Why identity information is provided in online government transactions

Particularly people with no education^ reported as one of the main reasons for them to provide identity information in online transactions with government is to get a service adapted to their personal needs^[33].

Sharing identity information as part of social networking

People from varying educational backgrounds demonstrate different identity information behaviours as part of social networking. In particular, different behaviours could be observed between people with no education^ and people with some form of educational achievement^

People with no education^ were more private than others^ on SNSs about disclosing their name^, information about the things they do, their personal opinions^, and information about their New Zealand citizenship, residency or visa status (see Figure 42, p.93). However, they were less private than others^ on SNSs about disclosing their SNS account details*^, their LinkedIn profile^, and, together with those who have completed primary education, about their personal health information.

Only people with some form of tertiary education disclosed their passport number* to close friends, if anybody, on SNSs.

[31] No education: no data; 3yrs secondary school: no data
[32] No education: no data; 3yrs secondary school: no data
[33] Primary school: no data; 4yrs secondary school: no data

Why identity information is provided on Social Networking Sites

People with lower levels of educational achievement^ and those with no education^ indicate different reasons for sharing identity information on SNSs, compared to people with higher levels of educational achievement^

People with a primary education background^, but also those with 4 years of secondary education^ or less^, and those with no education^, reported convenience^ as an important reason to provide identity information on SNSs.

People with no education^ and some respondents with a tertiary education background reported getting a discount^[34] as an important reason to provide their identity information on SNSs.

People with no education^, but also those who have completed primary education^, reported an important reason for them to provide identity information to SNSs is to ask a question^.

Trust in organisations to protect identity information

People with varying educational backgrounds demonstrate different levels of trust in organisations to protect their identity information. For instance, people with no education^ had higher trust in insurance companies^, overseas-based online commercial sites^ and overseas-based online dating sites^, compared with people with some level of educational achievement^

People with no education^ had higher trust in insurance companies^, overseas-based online commercial sites^, and overseas online dating sites^ to protect their identity information, compared with people with some level of educational achievement^ (see Figure 43, p.95).

People with 5 years of secondary schooling^ and those with a tertiary education background tended to have more trust in community organisations*^ and educational institutions^ to protect their identity information, than others^.

People with 5 years of secondary schooling^ tended to have more trust in the online gaming industry^ to protect their identity information, compared to others^.

Steps taken to protect online identity information

People who have completed primary education^ (22%) used a personal information vault^[35] to protect their identity information significantly more than others^.

[34] Primary school: no data; 3yrs secondary school: no data; 4yrs secondary school: no data; 5yrs secondary school: no data

[35] No education: no data; 3yrs secondary school: no data; 4yrs secondary school: no data

User experiences with forms of cybercrime or cyber-enabled crime

People who have completed primary education^ significantly more often reported an online personal experience with stolen credit card details^, being tricked into giving money^, being tricked into a romantic relationship^, or with misrepresented goods or services bought online^, compared with people from other educational backgrounds^

People who have completed primary education^ significantly more often reported an online personal experience with stolen credit card details^, being tricked into giving money^, being tricked into a romantic relationship^, or with misrepresented goods or services bought online^ (see Figure 44, p.97):

- Credit card details stolen*^[36]: 15% of respondents with a primary school background^, 3.6% of people with 5 years of secondary education^, 0.4% of people with a tertiary education background, and 0.1% of people with 3 years of secondary education, reported the personal experience of stolen credit card details;
- Someone else tricked you into giving them money*^[37]: 18% of respondents with a primary school background^, 0.7% of respondents with a tertiary education background and 0.1% of respondents with 3 years of secondary education, reported the personal experience online of someone else tricking them into giving money;
- Someone else tricked you into a romantic relationship*^[38]: 8.3% of respondents with a primary school background^, 0.4% of the people with a tertiary education background and 0.1% of people with 3 years of secondary education, reported the personal experience of having been tricked into a romantic relationship online; and
- Goods or services bought online were misrepresented*^: 32% of respondents with no education^, 14% of respondents with a primary education background^, 10% of respondents with 3 years of secondary education^, 22% of respondents with 4 years of secondary education^, 27% of respondents with 5 years of secondary education and 8.5% of respondents with a tertiary education background reported the personal experience of misrepresented goods or services bought online.

[36] No education: no data; 4yrs secondary school: no data
[37] No education: no data; 4yrs secondary school: no data; 5yrs secondary school: no data
[38] No education: no data; 4yrs secondary school: no data; 5yrs secondary school: no data

Introduction

This research explores the actual behaviours of New Zealanders in managing their online identity information in relationships with business, government, and family, friends and colleagues via Social Networking Sites (SNSs). It addresses an important knowledge gap untouched by other existing research initiatives thus far and follows from a 2010 study 'Public Attitudes to the Sharing of Personal Information in the Course of Online Public Service Provision' which focused on the *attitudes* of people towards sharing their identity information online with government agencies: understanding the identity information behaviours of people in varying e-relationships is of critical importance, as research points at a significant discrepancy between people's expressed concerns or attitudes about their privacy in online relationships and their actual online information behaviours (Viseu et al. 2004; Fox 20 00; Nissenbaum 2010).

For example, a survey amongst approximately 2,000 Internet users in the USA showed that, although respondents generally expressed their concern about their privacy online, only a few had experienced any significant breaches of their privacy and the majority was undertaking trusting and intimate activities online (Fox 2000). Moreover, respondents knew little about how their personal information was used or how to protect their information online (Ibid). A few other available studies point out that people's online privacy preferences do not reflect a simple desire to control and withhold identity information, but rather exhibit shifting and finely tuned tendencies to disclose, manage, and control their identity information, depending on context, data recipients, and the sensitivity of the information (Halperin & Backhouse 2008: Olson et al. 2005, in: Nissenbaum 2010).

So far however, there is not much empirical, in-depth knowledge available about the online identity information behaviours of individuals, with no research to date about the online identity information behaviours of New Zealanders. Moreover, with forms of cybercrime and cyber-enabled crime, including identity fraud and theft, on the rise in New Zealand and internationally, it is timely to explore the actual experiences of New Zealanders with varying forms of this phenomenon.

The research started in April 2013 and is led by Professor Miriam Lips, Chair in e-Government in the School of Government at Victoria University of Wellington. Other members of the research project team who have contributed to this research report are Dr Elizabeth Eppel, Dr Karl Löfgren and Lynn Barlow from Victoria University's School of Government, and Dr Dalice Sim who is a statistical consultant at Victoria University.

This interim report presents the findings of a quantitative web survey undertaken as the first research activity in this project. A final research report, including a comprehensive overview of the survey findings as well as findings from the other research activities, will be published after project completion.

Research objectives and design

The overall objectives of this research are to get a deeper understanding of the online identity information behaviours of New Zealanders in varying e-relationships enabled by different online channels or devices, and to identify effective solutions for the New Zealand government in managing risks around online identity information behaviours and people's experiences with cybercrime or cyber-enabled crime.

The research focuses on the following three questions:

1. *What are the identity information behaviours of different members of the New Zealand general public in using varying online channels for a wide range of e-relationships and online activities?*

2. *What are the actual experiences of different members of the New Zealand general public with forms of cybercrime and how did they respond?*

3. *Based on these empirical research findings, what are solutions for the New Zealand government in managing risks around online identity information behaviours and people's experiences with cybercrime or cyber-enabled crime?*

In order to gain a broad and deep understanding of what New Zealanders are actually doing with their identity information in online commercial transactions, transactions with government online and on Social Networking Sites (SNSs), and what people's actual experiences are with, and responses to, forms of cybercrime and cyber-enabled crime, a mixed-method research approach was developed involving the following research methods:

- A quantitative web survey with a representative sample of New Zealanders;
- Qualitative interviews with some participant observation of online identity information behaviours from representatives of different groups of the New Zealand population; and
- Ten focus group meetings with representatives of different groups of the New Zealand population.

The survey findings presented in this Interim Report are aimed at contributing to answers to the first two research questions.

Survey design

Sampling frame and method

The New Zealand Electoral Roll was used as the sampling frame for the survey. This particular sampling frame offers the opportunity to arrive at a representative sample for the New Zealand population by selecting potential research respondents on the basis of a set of relevant demographic criteria for this research, such as geographic location, age and ethnicity (*i.e*. Māori descent or not). Stratified Random Sampling Without Replacement (SRSWOR) was used to identify the sample members. Māori ethnicity and age were used to define 14 strata (see Table 2, p.37), within which a simple random sample was taken. Stratified sampling improves the efficiency of the sample design by forming homogeneous groups (strata) with smaller coefficients of variation. It also allows for more efficient estimates within subpopulations. In this survey, for example, Māori at all age levels were oversampled to ensure smaller measurement errors within this subpopulation.

To calculate population estimates of proportions (percentages) or means from a stratified sample, weighted combinations of stratum-specific proportions or means are used. The standard errors of these estimates are formed using formulas involving the stratum-specific standard errors and the

sampling fraction of each stratum[39]. In the analysis of this survey, IBM SPSS Version 20, analysis option "complex samples", was used.

Caution - the chosen sampling frame has the disadvantage that we could not sample for the following subpopulations:

- *different ethnic subpopulations within the non-Māori population, such as Pasifika, Asians and NZ Europeans;*
- *males and females;*
- *people from different income groups, including people with no income; and*
- *people with different educational backgrounds, including people with no education.*

This has led to very small subpopulations for some of the survey findings (e.g. the number of Pasifika and Asians is relatively low for several subpopulations). This then implies that, although the presented findings are significant[40], some of these findings have large confidence intervals and need to be treated with some caution. Wherever we present survey findings involving large confidence intervals, we have indicated this with ^.

Survey questionnaire

A questionnaire was developed on the basis of an extensive literature study. Besides collecting socio-demographic data from each research participant, the survey explored the device(-s) people used to go on to the Internet; the location and frequency of Internet use; online activities in the last 12 months; the types of identity information people had shared in online commercial activities, online government transactions and on SNSs, respectively, and the main reasons for disclosing identity information in these different online relationships; the trust people had in different public and private organisations around the protection of their identity information; what people do to protect their identity; and people's personal experience with forms of cybercrime and cyber-enabled crime in the last 12 months. A copy of the full survey questionnaire can be found in Appendix 1. A Human Ethics application for conducting the web survey was submitted and approved by the relevant HEC Committee at Victoria University.

The questionnaire was migrated to a survey software environment (Qualtrix) and tested multiple times to make sure that it would meet our accessibility and usability criteria. These criteria included that the web survey needed to be accessible via different devices, including mobile phones, and for participants to be able to complete the questionnaire within approximately 20 minutes. Some issues were discovered during this testing phase, such as restricted access to the web survey via a mobile phone or iPad. In order to accommodate these issues as much as possible, a longer testing period than originally envisioned was needed.

Access to potential survey participants

An initial sample size of 3,171 names and addresses were randomly selected from the New Zealand Electoral Roll dataset. This number was calculated to ensure that a representative sample of the New Zealand population could be achieved with a reasonable margin of error. Letters inviting participation in the web survey were sent to this group, including a password to access the survey online. Participation in the survey was anonymous and responses are confidential to the researchers. Submission of the survey indicated the individual's consent to participate.

[39] Details of these methods are given in, for example, Lohr, S. (2010). Sampling: Design and Analysis, (2nd ed.): Brooks/ Cole.

[40] $p < 0.050$; significant findings are indicated with *

Invitees who preferred to fill in a paper-based copy of the survey were encouraged to contact the research team via email or a 0800-contact number set up as a help desk for this research, so that a paper-based version of the questionnaire could be sent to them. As the web survey was accessible via the e-Government Chair website at Victoria University, visitors of that website who were interested in participating in the survey, were encouraged to contact the research team in order to get a password for accessing the online questionnaire.

The survey was made available for participants from the beginning of August 2013 until the end of October 2013, and received a total of 467 responses, which represents an overall response rate of 15 percent. However, as the initial approach resulted in a low response rate (3.1%)[41], an adjusted participant sample of 3,055 (with returned mail removed) was subsequently sent a reminder invitation. The reminder invitation included the incentive of a prize draw of three $100 grocery vouchers, which could be won by people who returned a completed questionnaire, and a paper-based copy of the questionnaire together with a free postage return envelope. Those participants who wanted to be considered for the prize draw, were encouraged to fill in a separate form, which they could sent back in the return envelope (together with the paper-based version of the questionnaire if they preferred). This second, revised approach led to a substantial increase in survey responses (12% response rate), in particular also responses provided via the paper-based version of the survey questionnaire. An overview of the survey questionnaire responses via online and paper-based methods and after each contact approach is provided in Table 1.

Table 1: Response rates and methods of survey questionnaires

Method	Total	1st Approach	2nd Approach
Online	123	97	26
Paper	344	17	327
Total	467	114	353
Response rate	15.3%	3.6%	11.7%

The analysis of the survey responses below is based on 467 survey response forms which were sufficiently completed; 1 returned questionnaire was not complete and therefore discarded from the research. As explained earlier, the responses ("raw data") have been weighted in order to arrive at representative findings for the New Zealand population.

[41] Please note that the Marlborough region / Wellington earthquakes happened around the time that the web survey was available to research participants. These extraordinary events may have had an impact on research participation rates.

Analysis of Survey Responses

We first provide an overview of the demographic background of our respondents, followed by a general presentation of the main findings under each survey question. We then focus on four categories where we have observed meaningful differences in the survey findings: age, ethnicity, income and education. An initial analysis of gender only provided a few meaningful findings: for this reason, we have integrated findings related to gender in the general discussion under each survey question below.

Demographic background of the respondents

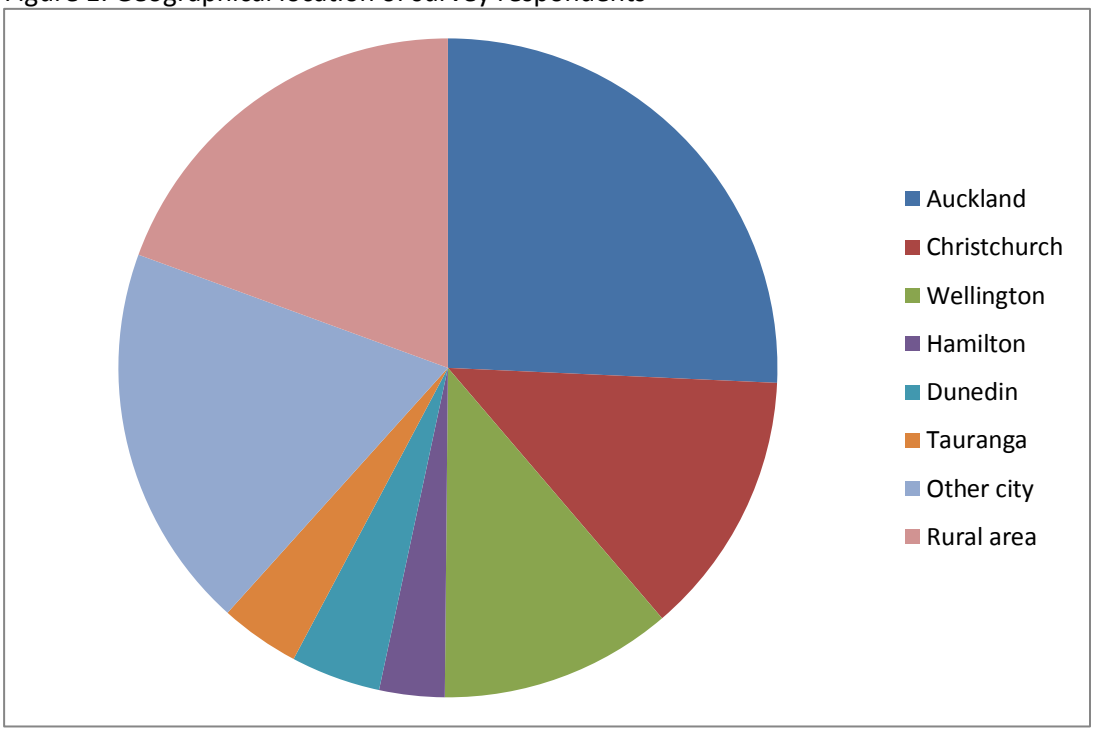
The distribution of the survey respondents across age groups is presented in Table 2.

Table 2: Age distribution of survey respondents

18–24 years of age	25–34 years of age	34–44 years of age	45–54 years of age	55–64 years of age	65–74 years of age	>75 years of age
11%	14%	17%	18%	22%	15%	2.9%

The survey respondents lived in Auckland (26%), Christchurch (13%), Wellington (11%), Dunedin (4.4%), Tauranga (3.9%), Hamilton (3.2%), other cities (19%), and in rural areas (19%) (see Figure 1).

Figure 1: Geographical location of survey respondents



38 percent of the respondents were male and 62 percent were female. The following

Table 3 shows the gender distribution of the respondents for each age group:

Table 3: Age and Gender

	18-24	25-34	35-44	45-54	55-64	65-74	75+
Male	9.7%	14%	15%	19%	22%	16%	3.3%
Female	12%	16%	19%	17%	21%	14%	2.8%

The distribution of Māori and non-Māori respondents across the age groups is presented in Table 4.

Table 4: Age and Māori v non-Māori

	18-24	25-34	35-44	45-54	55-64	65-74	75+
Māori	17%	19%	19%	18%	18%	8.9%	1.4%
non-Māori	10%	14%	17%	18%	23%	16%	3.2%

Within the non-Māori subpopulation, the following distribution of respondents over the different ethnic groups can be observed within each age group (Table 5). Table 5 shows an overrepresentation of NZ Europeans in the age groups of 55-64 years of age and 75 years and over, an overrepresentation of Pasifika in the 35-44 age group, and an overrepresentation of Asians in the 25-34 age group. However, Pasifika were underrepresented in the age groups of 25-34 years of age and those of 55 years and over; Asians were underrepresented in the 55-64 age group and the age group of 75 years and over.

Table 5: Age and Ethnicity for Non-Māori

	18-24	25-34	35-44	45-54	55-64	65-74	75+
NZ European	9.8%	13%	15%	17%	24%	17%	3.6%
Pasifika	15%	8.1%	44%	20%	7.3%	5.4%	
Asians	11%	22%	15%	22%	16%	15%	

The following Table 6 shows the income distributions of respondents within each age group, demonstrating an underrepresentation in this survey of people with no income.

Table 6: Age and Income

	18-24	25-34	35-44	45-54	55-64	65-74	75+
No income	11%	4.8%		4.2%	4.7%		
$1 - $10,000	22%	4.8%	4.7%		5.1%	1.5%	
$10,001 - $20,000	33%	7.7%	9.4%	15%	11%	30%	62%
$20,001 - $30,000	6.7%	15%	7.5%	8.4%	11%	24%	8.7%
$30,001 - $50,000	22%	17%	24%	28%	22%	24%	9.1%
$50,001 - $70,000	4.5%	30%	23%	14%	20%	8.3%	7.8%
$70,001 - $100,000		15%	15%	15%	16%	11%	4.3%
$100,001 - $150,000		4.8%	12%	11%	7.8%	1.5%	3.9%
over $150,000			5.6%	4.9%	3.1%		3.9%

The large majority of the respondents had achieved a higher level of education: 84 percent of the respondents had at least completed 4 years of secondary education, with 64 percent of the respondents having had some form of tertiary education. Few respondents had completed primary education only (3.6%), or had no education at all (1.6%). Table 7 shows the distribution of respondents' educational achievement within each age group.

Table 7: Age and Education

	18-24	25-34	35-44	45-54	55-64	65-74	75+
No education		2.5%	2.8%	1.7%	1.1%	1.4%	
Primary school	1.7%		2.8%	3.6%	3.1%	6.7%	21%
3 yrs secondary	3.5%	4.6%	5.7%	14%	12%	21%	25%
4 yrs secondary	3.5%	9.7%	5.7%	15%	12%	12%	8.5%
5 yrs secondary	43%	11%	4.8%	7.3%	1.8%	6.9%	8.5%
Some tertiary	48%	73%	78%	58%	71%	52%	37%

21 percent of the survey participants of 75 years and over had only primary school or less, compared to only 1.7 percent of the age group of 18 – 24 year olds (see Table 8).

Table 8: Respondents with low education achievement, by age

18-24	25-34	35-44	45-54	55-64	65-74	75+
1.7%	2.5%	5.6%	5.3%	4.2%	8.1%	21%

On average, non-Māori respondents living in urban areas had the highest level of educational achievement (see Table 9). Māori living in urban areas also had on average a higher level of education than Māori living in rural areas.

Table 9: Average mean score of educational achievement for Māori and non-Māori, per geographic location

Mean score of educational achievement (1 = low, 7 = high)

	Urban areas	Rural
non-Māori	5.93	5.83
Māori	5.20	4.52
Significance (p)	0.014	0.026

Survey respondents with a low income or no income at all were likely to have only a primary school background or no education (see Table 10). For instance, 15 percent of those on no income had a primary school education or less, while only 1.1 percent of those earning an income between $70,001 and $100,000 had only a primary school education or less.

Table 10: Respondents with low educational achievement, by income

No income	$1 - $10,000	$10,001 - $20,000	$20,001 - $30,000	$30,001 - $50,000	$50,001 - $70,000	$70,001 - $100,000	$100,001 - $150,000	over $150,000
15%	7.6%	7.6%	4.5%	2.5%	5.2%	1.1%	6.3%	

Survey findings

Using the Internet

95 percent of the research participants had used the Internet in the last 12 months. Respondents were also asked to identify the device they had used in the last 12 months to go on the internet. 95 percent of both female and male respondents had used at least one device to access the Internet.

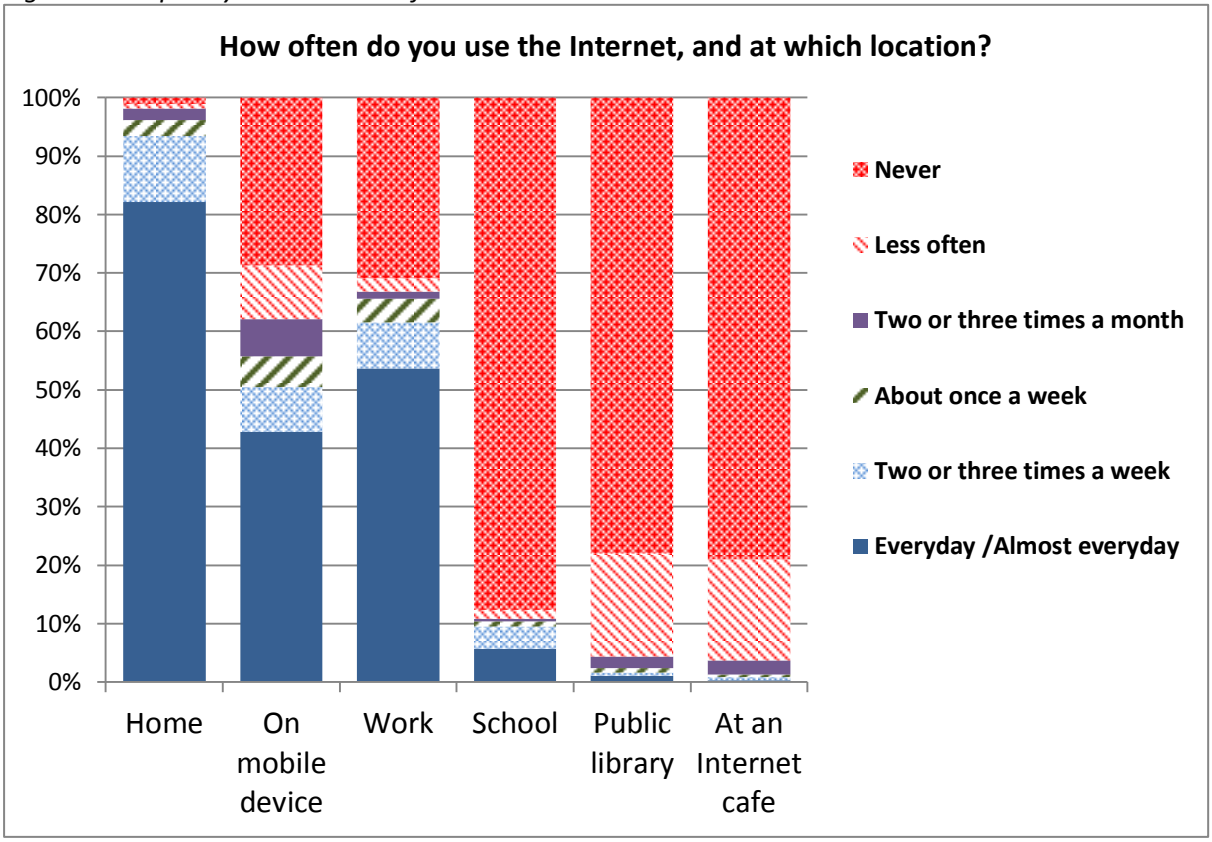
Those respondents who had not used the Internet in the last 12 months (5.4%) were asked about why this was so. The most common reason provided was "*I do not have a computer* ", or similar. Other reasons given included: "*not interested or do not want to*"; "*do not know how to use a computer and/or the Internet*"; and "*happy to leave to other members of the family*". Some gave more than one of these reasons, e.g. "*Do not have a computer. Do not know how to use one. I don't have much interest in computers*". There was the odd anomalous response such as "*I only use it for banking and family photos*". Respondents who did not use the Internet were slightly more likely to be from Hamilton, smaller cities or rural areas.

Of respondents accessing the Internet, 78 percent had done so using a PC or desktop computer, 68 percent used a laptop, notebook or netbook, 55 percent used a mobile phone, 36 percent used a tablet, 8.4 percent used a games console, 7.4 percent used an e-book reader, 5 percent used

Internet-enabled television, and 3.6 percent used a public kiosk (see Figure 2). There was no significant difference in device use by males and females except for a disproportionately higher number of males using gaming devices (15%), compared to females (4.7%).

Internet users were asked where they access the Internet and how often. 82 percent use the Internet at home every day or almost every day, and this rises to 96 percent using the Internet at least once a week. Others do so less frequently and only 1.1 percent of internet users never use the Internet at home. There appears to be no significant difference between males and females, or where people live.

Figure 2: Frequency and location of Internet use

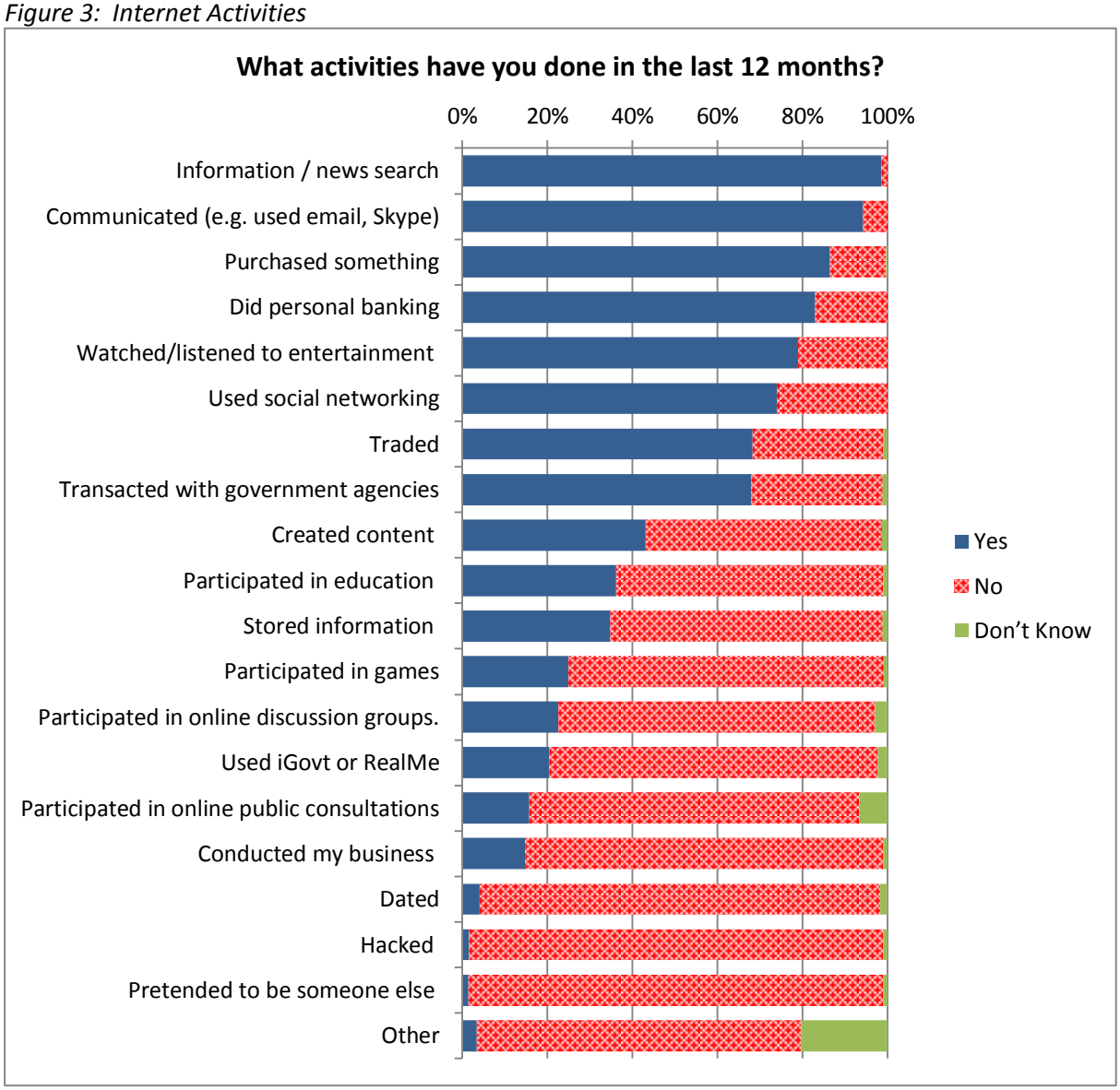


Online activities in the last 12 months

Figure 3 provides an overview of the online activities Kiwis undertook in the last 12 months. The most frequent online activities were searching for information or news (99%), communication using email, Skype, text or similar (94%), purchasing something (87%), personal banking (83%), participating in entertainment, such as watching movies, videos, television on demand listening to music, or reading an e-book (79%), using a Social Networking Site (74%), or trading online (68%). Other activities were much less frequently engaged in by participants: accessing stored information online (35%), participating in online games (25%), participating in online discussion groups (23%), using RealMe (or its predecessor iGovt) to log onto government department services (20%), participating in online consultations from government agencies (16%), conducting a business online (15%), or online dating (4%). Anti-social activities, such as hacking into another person's online system or device, or pretending to be someone else, had an estimated frequency of between 0.5 percent and 2.5 percent when the margin of error is applied.

Using a social networking site is most frequent in the youngest age group at 95 percent, and this then declines with age (55-64yr age group, 55%, and 65–74yr age group, 58%).

Figure 3: Internet Activities



People who used the Internet at home (see also Figure 2) were significantly more likely to undertake the following online activities, and doing so on a daily basis: social networking; the creation of content online; trading; transacting with government; purchasing something; communicating; and participating in entertainment.

People who used the Internet at work (see also Figure 2) were significantly more likely than others to conduct their business online, to participate in education online; store information online; transacting with government online; do personal banking online; to purchase something online; and, to some extent, hack[42] into another person's online system or device.

Survey participants who used the Internet on a mobile device (see also Figure 2) were significantly more likely than others to use RealMe (formerly iGovt); create content online; store information

[42] Hacking was defined towards survey participants as '*attempting to gain unauthorised access to another person or organisation's computer systems*'

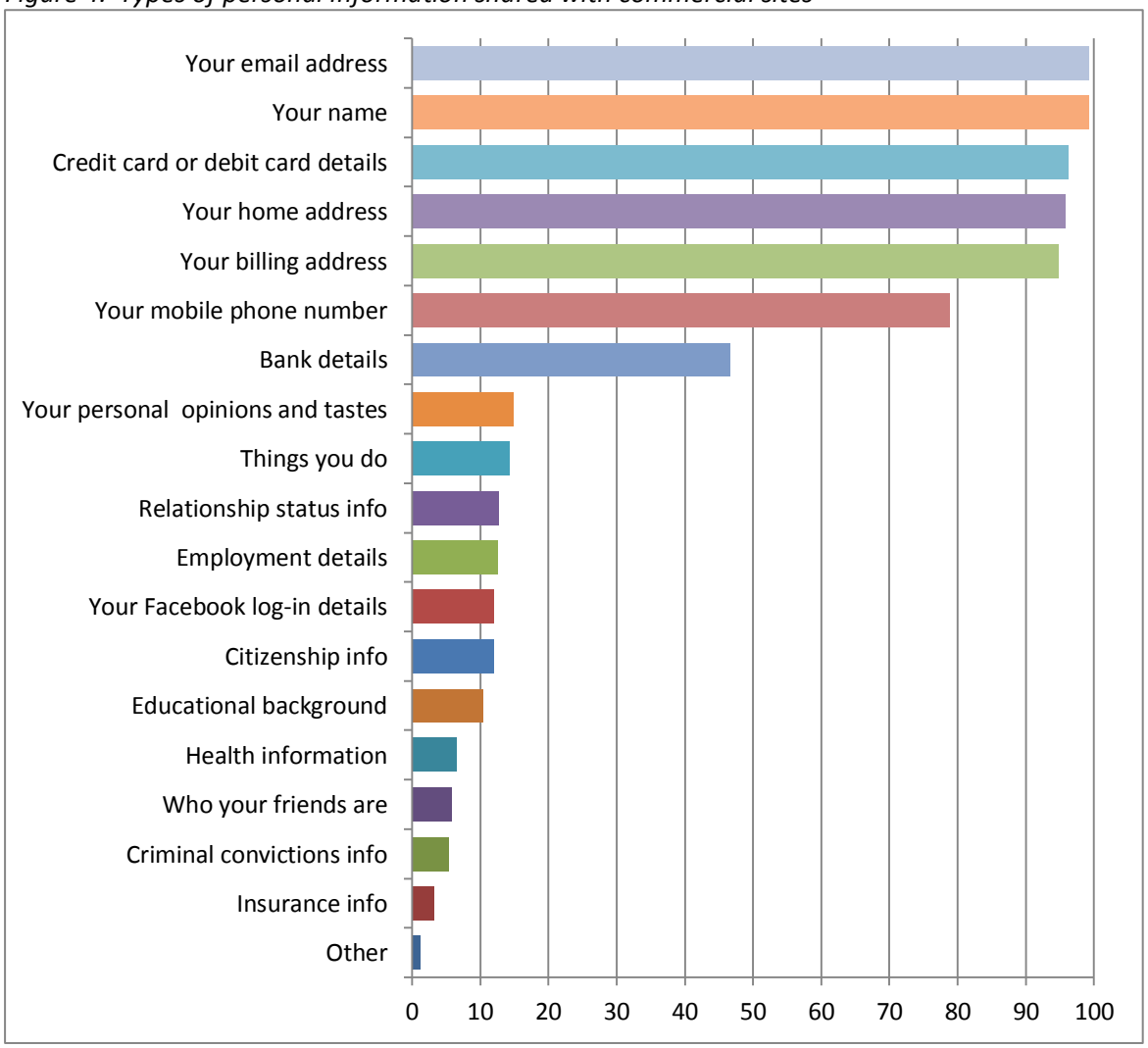
online; participate in online education; use social networking; transact with government agencies online; do personal banking online; and participate in online education.

Identity information provided in online commercial transactions

Bearing in mind that 87 percent of the respondents had purchased something over the Internet in the last 12 months, participants were also asked what types of personal information they had provided in this process. In general, people were quite private in online commercial transactions, with the large majority restricting the identity information they share online.

Name had been provided by 97 percent of the respondents, followed in frequency by email address (95%), home address (92%), credit or debit card details (93%), billing address (87%), and mobile phone number (74%). Bank details were provided about half as often (41%). Other information was provided less frequently: personal tastes and opinions (17%), things you do such as hobbies, sports or place you go (17%), information about NZ citizenship, residency or visa status (15%), employment details (15%), information about educational background (14%), Facebook login-in details (14%), information about relationship status (14%). Provision of information about friends (8%), health (5.2%), or insurance (3.5%) is less common again (see Figure 4).

Figure 4: Types of personal information shared with commercial sites



Why identity information is provided in online commercial transactions

When asked to identify the top three reasons for proving their personal information to commercial organisations online, the most frequently cited reason was to get the product or service (88%). Other popular reasons were to complete the transaction (58%), convenience (31%), to comply with the law (27%), and to access further information about the service (25%). Other reasons, such as to get a financial discount, to ask a question, to get a personalised service, to benefit from personalised commercial offers in the future, to connect with others or have fun, were cited in descending order by between 8.5 percent and 2.1 percent of the population. 4.1 percent responded that they were not bothered by what information they provided.

Identity information provided in transactions with government online

68 percent of the population had transacted online with a government agency in the last 12 months, for example to submit a tax form, apply for a benefit, register a vehicle or manage a student loan. Participants were asked what personal information had been provided as part of these online transactions with government (see Figure 5). In general, people were quite private in online transactions with government, with the large majority restricting the identity information they share online.

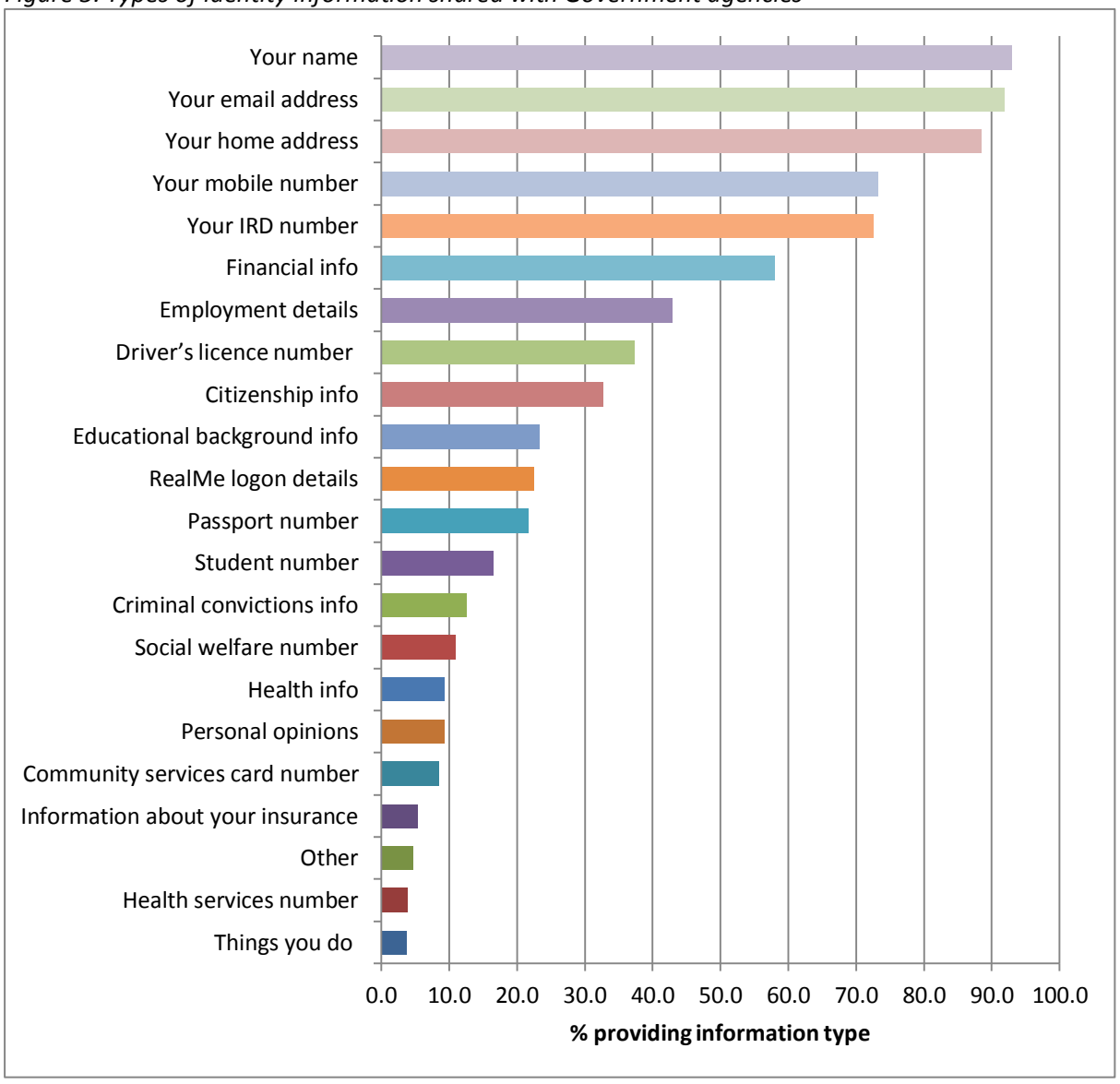
Name (93%), email address (92%), home address (88%), and mobile phone number (73%) were the most frequently provided types of personal information in government online relationships. IRD number (73%) and financial information (58%), such as credit card or bank details, were also frequently shared with government online. Information about a person's insurance (5.4%), their Health services number (3.9%) and things they do (3.7%) were the least common.

People who were using the Internet at home on a daily basis were significantly more likely than others to provide a health services number in online transactions with government. Those who were using the Internet on a mobile device on a weekly basis were more likely than others to provide their social welfare number in online government transactions.

Why identity information is provided in online government transactions

Participants were asked for the three most important reasons why they provided personal information in online transactions with New Zealand government agencies. The most frequent reason by a large margin is to get the service wanted/needed (80%). Other common reasons cited included because the participant was asked to provide the information (46%), to pay (or receive) tax, ACC levies, fines (35%), to access information about the service (32%), for the convenience such as saving time or having 24/7 service access (28%), or to comply with the law (27%). Other reasons such as benefit from personalised service (5.7%), to engage with government (5%), to get service adapted to personal needs (4.4%, to ask a question (3.6%), or organise an appointment (1.4%), were given much less frequently.

Figure 5: Types of identity information shared with Government agencies



Sharing identity information as part of social networking

Participants were asked to identify personal information they have provided over the last 12 months as part of their usage of a Social Networking Site (SNS) and to whom they have provided it: respondents were asked to identify whether they have provided a particular type of identity information to no one, friends only, friends of friends, or the public.

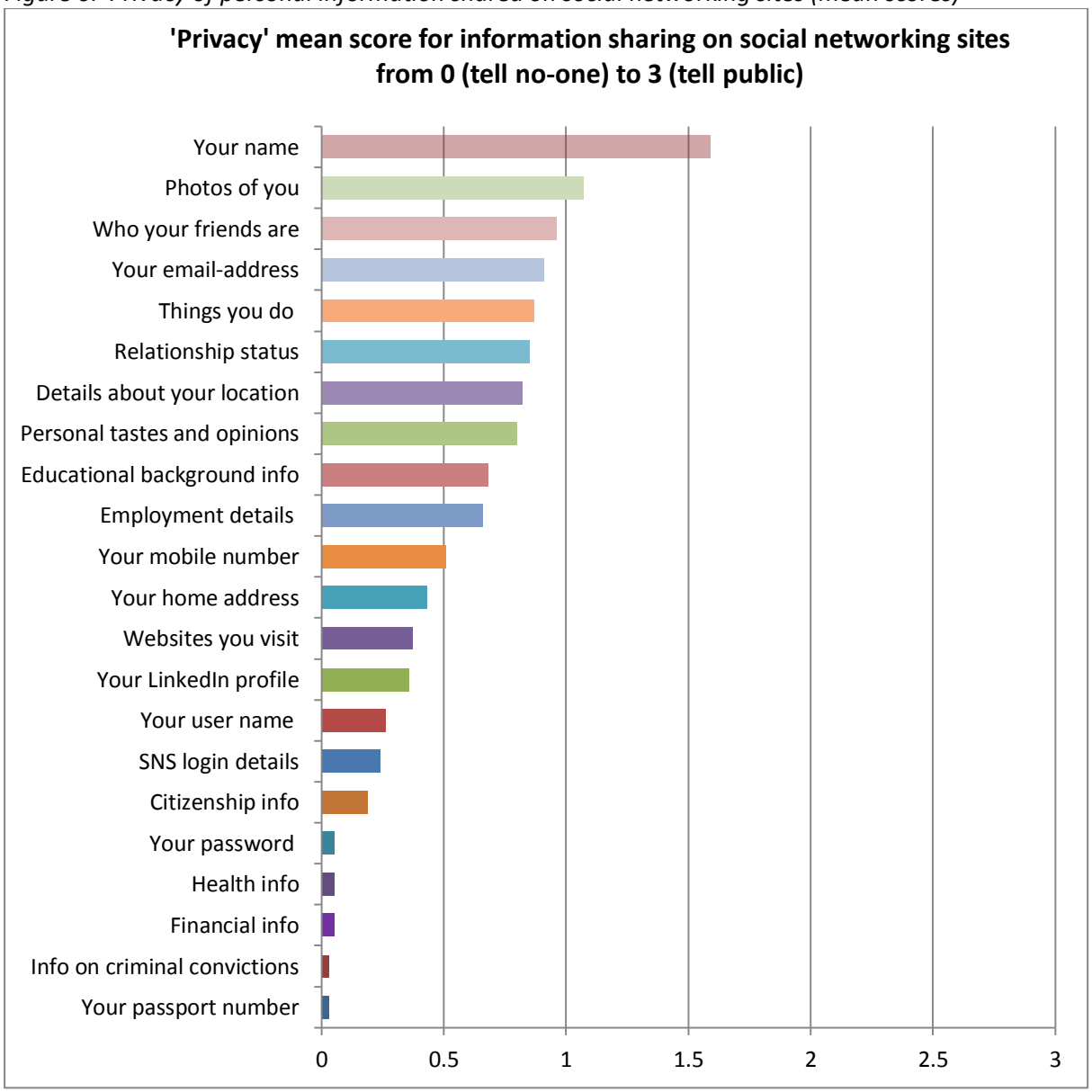
In general, people turned out to be quite private on SNSs, with the large majority restricting the identity information they share online. The identity information most frequently shared with the public was a person's name (34%). Next most publicly shared information, although significantly less so, were who your friends are (9.4%), email address (8.7%), location details (8.6%), Linkedin profile (8.6%), information about your relationship status (8.1%) and photos of you (7.9%).

The most private information, that is, identity information that participants were most likely not to share with any one, was a passport number (100%), password (99%), financial information, such as credit card and bank details (98%), information about criminal convictions (98%), health information

(98%), and information about NZ citizenship, residence or visa status (96%). When those who had shared this information only with close friends are taken into account, then passport number is still the most private, i.e. nobody would share this information with close friends, followed by financial information (0.8% share with close friends).

A mean score can be calculated for the degree of 'privacy' of identity information shared on social networking sites, where 0 is shared with no-one and 3 is always shared with the public. Figure 6 below shows the mean 'privacy' scores for all types of identity information.

Figure 6: Privacy of personal information shared on social networking sites (mean scores)



Why identity information is provided on Social Networking Sites

Participants were asked for the three most important reasons why they provided personal information on social networking sites or other sharing sites. The most frequent reasons were: to access the social networking site (54%), to connect with people (54%) to get information such as news, updates from friends and family or product information (50%), and to share information with

people (35%). Other less frequently cited reasons were: for fun (14%), to get a product or service adapted to personal needs (12%), for the convenience of saving time or having 24/7 access (9.4%), to benefit from personalised commercial offers (1.1%), and to get a discount (0.3%). 9.8 percent of the respondents provided other reasons and for most this was that they did not use social networking sites. Other additional responses provided by individuals included: whanau, iwi and hapu support; or in two instances, to promote a business.

Trust in organisations to protect identity information

Given that different public sector institutions, such as government departments and local authorities, and also private companies and non-government organisations collect and store personal information, participants were asked about the extent to which they trusted a range of these institutions on a five point scale from totally trust, tend to trust, tend not to trust, don't trust at all, or don't know. Figure 7 below provides an overview of the overall responses to this question.

Banks and financial institutions received the highest frequency of responses on the positive side of the trust ledger – totally trusted (31%) and tend to trust (58%); and were closely followed by health and medical institutions – totally trusted (30%) and tend to trust (57%). 23 percent of the population totally trust New Zealand central government agencies to protect their identity information, while 59 percent of the population tend to trust New Zealand central government agencies. Overseas online dating sites (2%), New Zealand-based online dating sites (3.4%) and the online gaming industry (8.2%) were the least trusted to protect identity information.

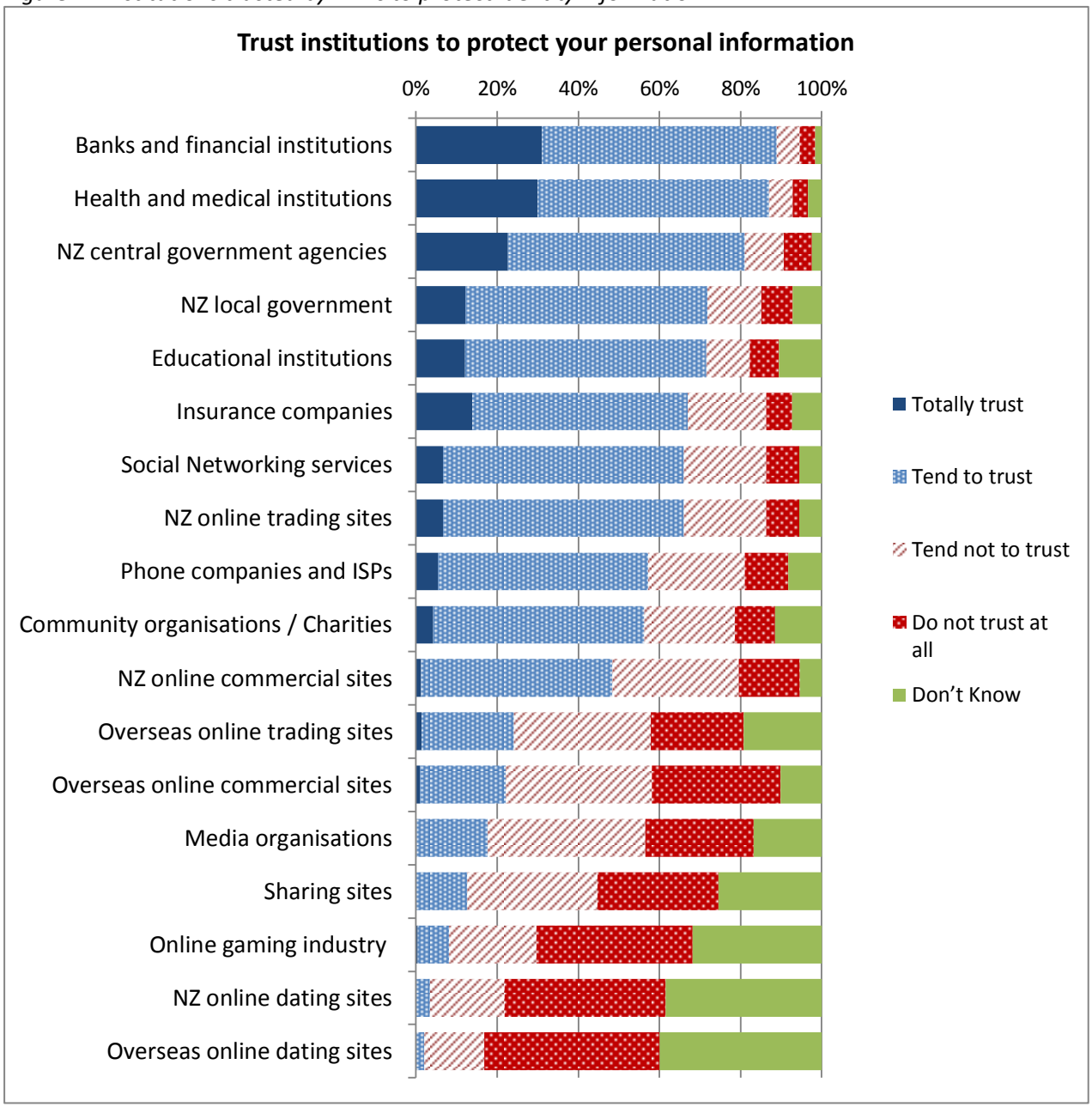
Trust levels in New Zealand central government agencies are relatively high if we compare these findings with responses to similar survey questions in overseas jurisdictions. Compared to recent survey findings from the EU for instance, where 76 percent of the Europeans responded to fear that their personal data is not safe in the hands of private companies, and 64 percent indicated to fear that their personal data is not safe in the hands of public authorities (European Commission 2011), we may conclude that Kiwis particularly differ in having a relatively high trust in New Zealand Central Government agencies around the protection of their personal information.

Privacy statements

Participants were asked to select from a set of statements provided, which of the statements best describes that they usually do or most often do when they encounter privacy statements on the Internet. The total responses show that only 25 percent of the population usually read and are able to understand privacy statements provided in varying online relationships, which suggests room for improvement in this area.

The responses provided by people were *"usually do not read them"* (38%), *"usually read them but don't understand them"* (25%), *"usually read them and understand them"* (25%), *"ignore them"* (5.9%), and *"don't know where to find"* privacy statements (3.3%). Participants were also given the opportunity to specify another response and 2.3% did this. The statement individuals made included: "*usually browse over quickly as privacy statements can be overbearing (and who has time to read the whole statement?*", "*flick through them but don't read closely in detail*", "*sometimes read*", "*depends on the site*", and "*ask my wife*".

Figure 7: Institutions trusted by Kiwis to protect identity information



Steps taken to protect online identity information

Participants were asked what they do to protect their identity information when they are on the Internet (see Figure 8 below). The most common protection reported was the use of antivirus software (94%). Other measures in decreasing frequency of use were: limiting the personal information provided (87%), using tools to limit unsolicited emails such as spam (82%), using a firewall (78%), using security-protected WiFi (77%), checking that a transaction is protected such as using only Paypal for transacting money online (72%) , deleting cookies (61%), changing their privacy settings (60%), using a filter such as an email filter (59%), deleting online search history (54%), using a search engine, such as Bing, Google or Yahoo, to check for personal information online (53%), avoiding giving the same information, such as a password, to different sites (48%), checking that the website has a safety logo or label (41%), checking the privacy policy of the website (40%), not providing any personal information via online channels (37%), asking organisations to delete or

update their personal information (20%), using iGovt or RealMe (20%), using a pseudonym (20%), changing their social networking site profile (14%), using a dummy email account (13%), using proxies such as Tor (8.3%), using a password generator such as Lastpass or PWGen (5%), or using a personal information vault (2.1%).

Another interesting finding is that the number of 'don't know' responses to questions around tools and strategies to protect identity information online is quite high (up to 15% for some questions and not including the 'Other' response category), which suggest room for more education around available online privacy protection means.

With 87 percent of all respondents indicating that they disclose minimal information about themselves online as a strategy for privacy protection, we may conclude, again, that Kiwis are quite private about their identity information in online relationships, also if we compare this to identity information behaviours demonstrated by people from overseas jurisdictions. For instance, findings from a recent European survey demonstrate that only 34 percent of the European population do not reveal personal information on websites (European Commission 2011). However, with regard to the use of other online identity information protection tools and strategies, Kiwis demonstrate more or less similar behaviours to the Europeans. European survey findings (European Commission 2011) show for example that 46 percent of the European population has installed anti-virus software; 40 percent do not open emails from strangers; 32 percent only visit websites they know and trust; 26 percent only use their own computer to go online; 24 percent use different passwords; 17 percent buy fewer goods online; 16 percent change their security settings; and 15 percent use fewer banking services.

One of the few instances where we can see significant behavioural differences in terms of gender is when it comes to individuals protecting their identity information online. Whereas men and women use most of the online protection tools and strategies, men tend to be more cautious, or aware, about not leaving any traces behind while conducting online activities (see Figure 9). For instance, men are significantly more likely to delete cookies (77%: compared to 67% for women); use a dummy email account (19%: compared to 11% for women); use a pseudonym (30%: compared to 18% for women); and delete their online search history (68%: compared to 50% for women).

Figure 8: How individuals protect their privacy when using the Internet

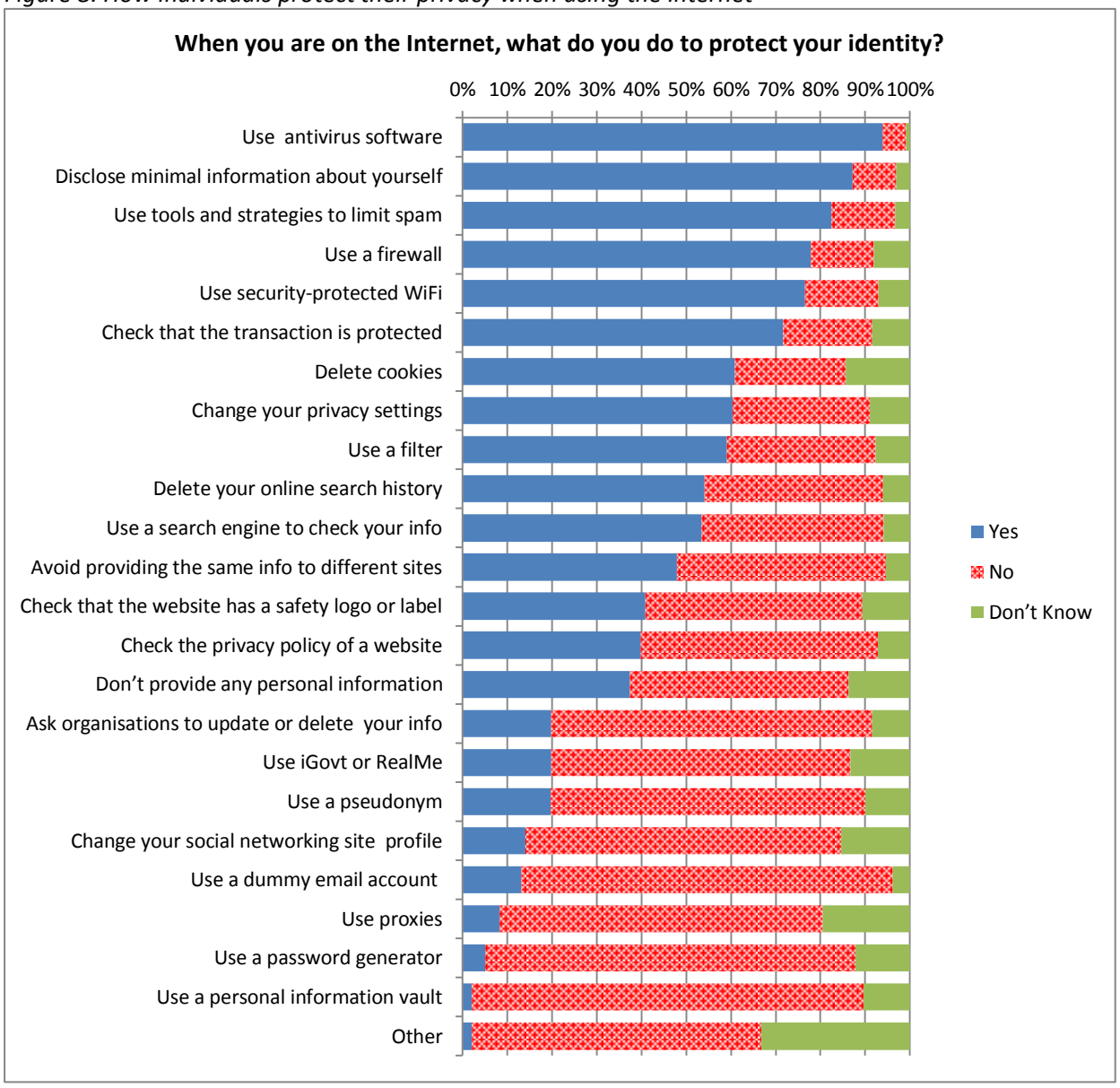
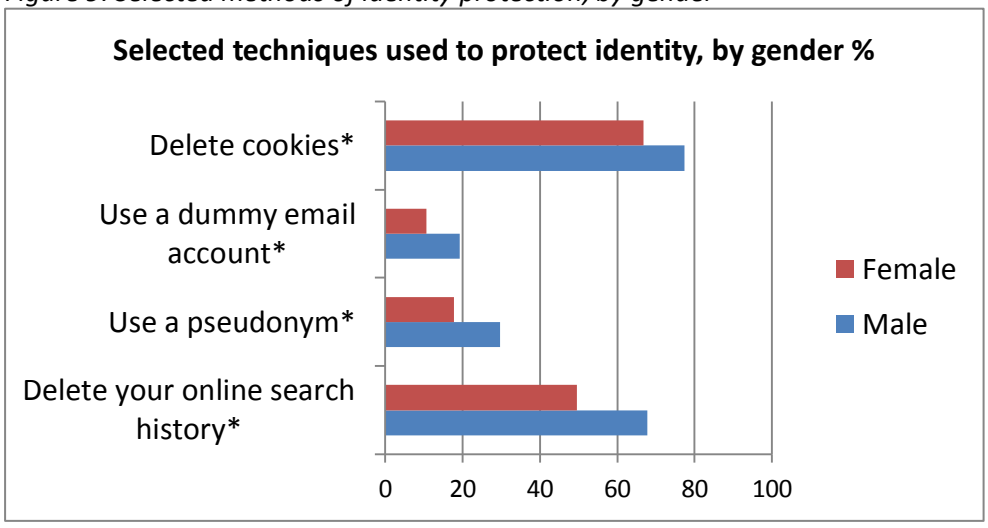


Figure 9: Selected methods of identity protection, by gender



Dummy e-mail account (p=.033), deleted cookies (p=.046), deleted online history (p=.002), use a pseudonym (p=.017).

Significant findings around the use of online identity information protection methods and trust in organisations

The survey findings demonstrated some significant correlations between the types of organisation people trusted, or distrusted, to protect their identity information, and the protection methods people use to protect their own identity information online. In general, people who had lower levels of trust in organisations to protect their identity information were significantly more likely to use security protected WiFi; use a firewall; delete their online search history; or use a search engine to check online information about themselves.

The following findings were observed for the use of specific protection methods in relationship to the trust people have in a particular organisation:

- Banks and Financial Institutions. Those survey participants who used anti-spam strategies, checked the privacy policy of a website, or didn't provide any personal information online, had significantly higher levels of trust in banks and financial institutions, compared to those who did not use these techniques. However, participants who used search engines to check their information online, had significantly less trust of financial institutions compared with people who did not.

- Health and Medical Institutions. Respondents who changed their privacy settings, used anti-spam strategies, or checked the privacy policy of a website, had significantly higher trust in health and medical institutions, compared with others. However, those participants who used security protected WiFi, deleted their online search history, used a search engine to check online information about themselves, or those who used a firewall, had significantly less trust in health and medical institutions, compared with others.

- NZ Central Government Agencies. Those survey respondents who disclose minimal information about themselves online, use a dummy email account, use a pseudonym, or ask organisations to update or delete information about them, have a significantly higher trust in New Zealand central government agencies, compared with others. However, those participants who use security protected WiFi, use a firewall, check that a site is protected by Paypal, or change their SNS profile, have significantly less trust in New Zealand central government agencies, compared with others.

- NZ Local Government Agencies.. People who changed their privacy settings, used a dummy email account, delete cookies, use anti-spam strategies, disclose minimal information about themselves, use a password generator, or use the RealMe (formerly iGovt) service, had significantly higher trust in New Zealand local government, compared with others. However, people who use security protected WiFi networks, delete their online search history, check the protection of their online transaction, avoid providing the same information to different sites, change their SNS profile, use a search engine to check information about themselves, or those using a proxy, had a significantly lower level of trust in New Zealand local government agencies, compared with others.

- Sharing Sites. People who trusted sharing sites more, were significantly more likely to protect themselves online by using a firewall, disclosing minimal information about themselves, or use the RealMe (formerly iGovt) service, compared with others.

- Online gaming Industry. People who protected themselves online by deleting cookies, use anti-spam strategies, check the privacy policy of a website, or ask an organisation to update or delete their information, have significantly higher trust in online gaming sites, compared with others. However, those who use a password generator, or change their SNS profile, had significantly less trust in the online gaming industry, compared with others.

- NZ online dating sites. People who use antivirus software have significantly higher trust in NZ online dating sites, compared with others. However, those who ask to update or delete their information, have significantly less trust in NZ online dating sites, compared with others.

User experiences with forms of cybercrime or cyber-enabled crime

Participants were asked whether they personally in the last 12 months had experienced any of a list of forms of cybercrime or cyber-enabled crime. The most commonly mentioned experiences were someone else uploading photos of the person into an online public space without their permission (15%), malware downloaded to the participant's device over the Internet (14%), goods or services purchased online were misrepresented (12%), and participant's bank details requested by someone else through an online channel (11%). Less frequent experiences were someone misrepresenting themselves online to the participant (7.1%), goods and service ordered online were not delivered (6.7%), someone else sent emails out in the participant's name without their permission (6.5%), or pretended online to be the participant (4.2%), someone hacking into the participant's online device (4.4%),someone using the participant's name to set up a social media account (2.2%), and the participant being tricked by someone using an online channel into giving money (0.9%). One per cent of the participants reported that the details of the credit card they had used online had been stolen. These results are shown in Figure 10 below.

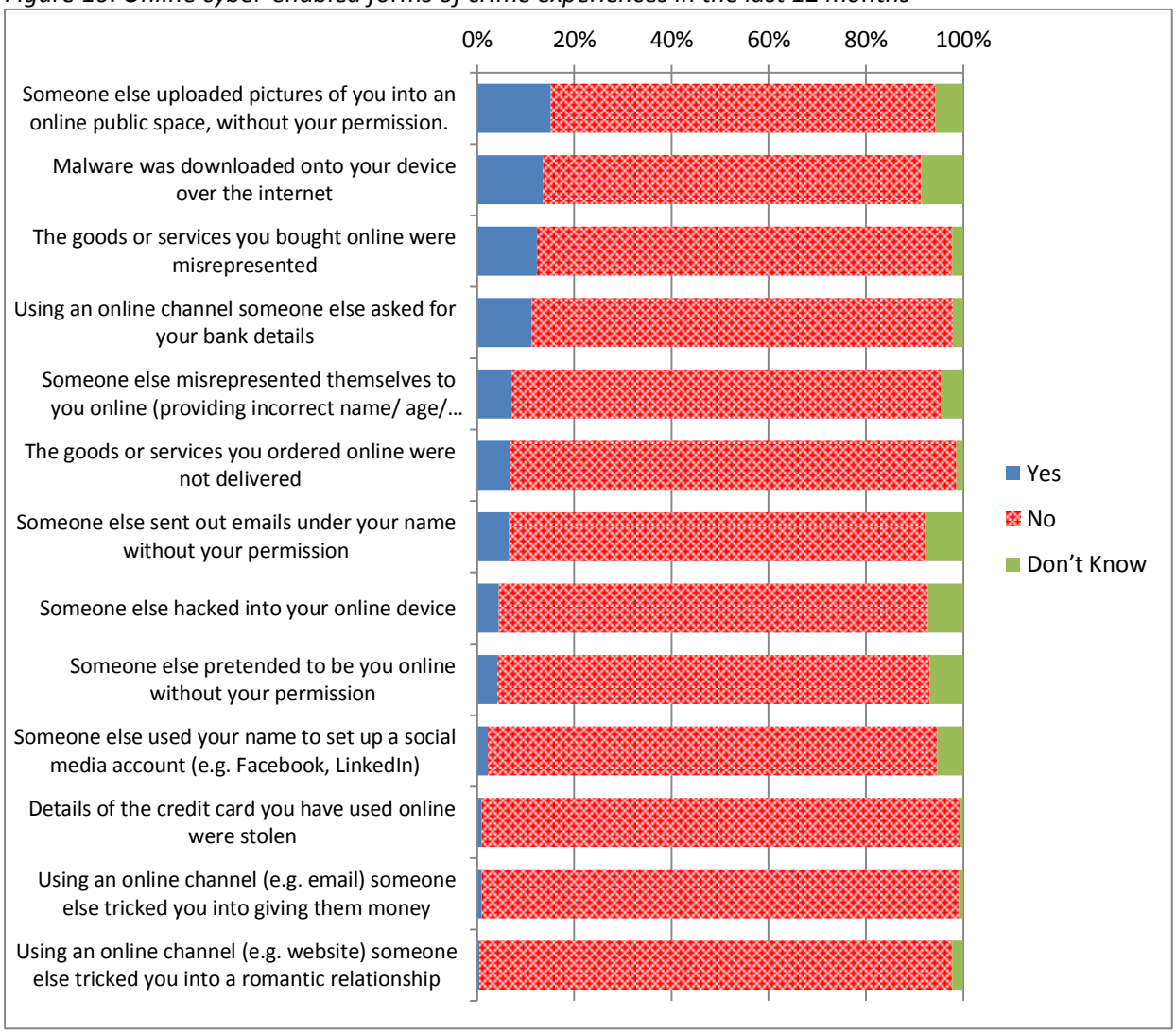
The following different findings for gender could be observed: men were significantly more likely to have malware downloaded on to their device (22%), compared with women (9.5%). Additionally, women were more likely to report that someone else sent out emails under their name (9.4%), compared with men (3.5%).

In general, these actual experiences are much less common compared to overseas experiences. For example, in 2012, 38 percent of Internet users across the EU had received emails fraudulently asking for money or personal details; 13 percent had not been able to access online services because of cyber-attacks; 12 percent had experienced online fraud where goods purchased were not delivered, counterfeit or not as advertised; and 8 percent had experienced identity theft, such as somebody stealing their personal information and impersonating them online (e.g. in online shopping activities (European Commission 2012, p.46).

One possible explanation is that Kiwis are more careful with their personal information online compared to people from other countries, and therefore forms of cyber-crime or cyber-enabled crime do not happen that often in New Zealand. Another possible explanation is that Kiwis are less targeted by online thieves or criminals.

A further observation is that the actual experience of forms of cyber-enabled crime amongst Kiwis is much less common than the media stories tend to make us believe.

Figure 10: Online cyber-enabled forms of crime experiences in the last 12 months

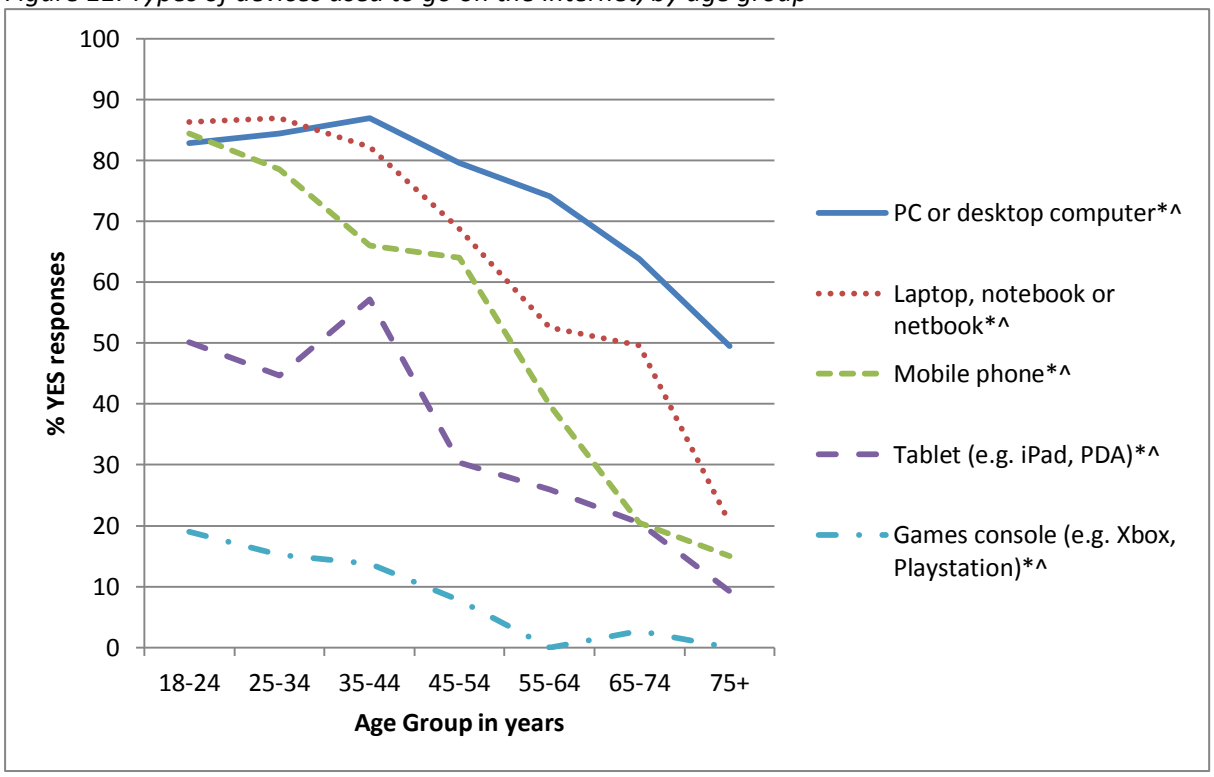


Age

Using the Internet

In general, people's use of a PC^, a laptop^, a mobile phone^, a table^t or a games console^ to go onto the Internet, decreases with age (see Figure 11). A PC, laptop and a mobile phone are the devices respondents used mostly to go onto the Internet in the last 12 months, with some interesting differences in preferred devices between the youngest respondent group of 18-24 years of age^ (laptop^ mostly preferred, followed by mobile phone^ and PC^), the respondent group of 25-34 years of age^ (laptop^ mostly preferred, followed by PC^ and mobile phone^), respondents between 35 and 74 years of age^ (PC^ mostly preferred, followed by laptop^ and mobile phone^), and the oldest respondent group of 75 years and over^ (PC mostly preferred^, followed by a laptop^ and mobile phone^).

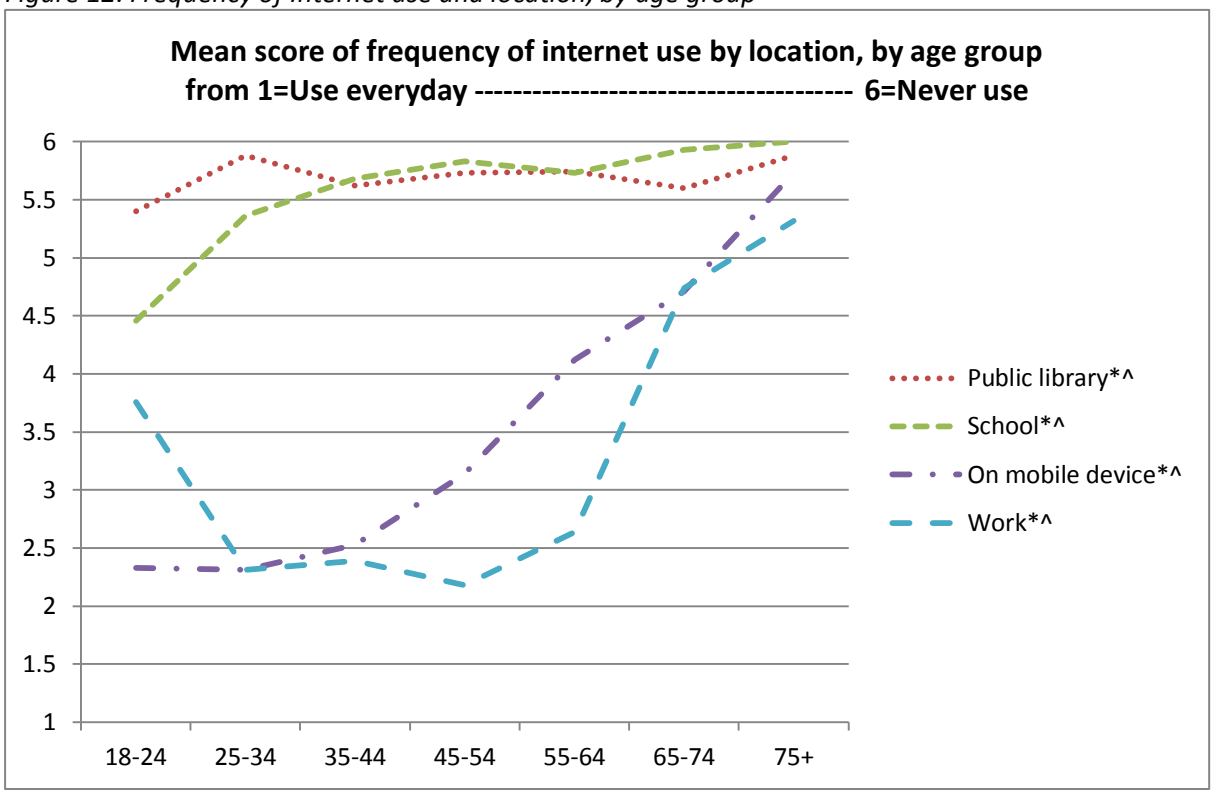
Figure 11: Types of devices used to go on the Internet, by age group



PC (p=.015); laptop (p=.000); mobile phone (p=.000); tablet (p=.000); games console (p=.000)
^Confidence intervals: PC or desktop computer (18-24yrs: 62%-94%; 25-34 years: 70%-93%; 35-44 years: 76%-94%; 45-54 years: 69%-87%; 55-64 years: 64%-82%; 65-74 years: 52%-74%; 75+ years: 34%-65%); laptop etc (18-24yrs: 64%-96%; 25-34 years: 73%-94%; 35-44 years: 70%-90%; 45-54 years: 57%-78%; 55-64 years: 42%-63%; 65-74 years: 39%-61%; 75+ years: 10%-36%); mobile phone (18-24yrs: 73%-92%; 25-34 years: 64%-88%; 35-44 years: 53%-77%; 45-54 years: 53%-74%; 55-64 years: 30%-51%; 65-74 years: 13%-31%; 75+ years: 6.7%-30%); tablet (18-24yrs: 33%-67%; 25-34 years: 32%-58%; 35-44 years: 53%-77%; 45-54 years: 53%-74%; 55-64 years: 30%-51%; 65-74 years: 13%-31%; 75+ years: 6.7%-30%); games console (18-24yrs: 11%-31%; 25-34 years: 7.2%-29%; 35-44 years: 6.7%-26%; 45-54 years: 3.5%-17%; 55-64 years: no data; 75+ years: no data)

Younger age groups use the Internet on a mobile device^ more frequently than older age groups: this development declines with age (see Figure 12). Also, younger age groups more frequently use the Internet at school^ compared to older age groups.

Figure 12: Frequency of Internet use and location, by age group

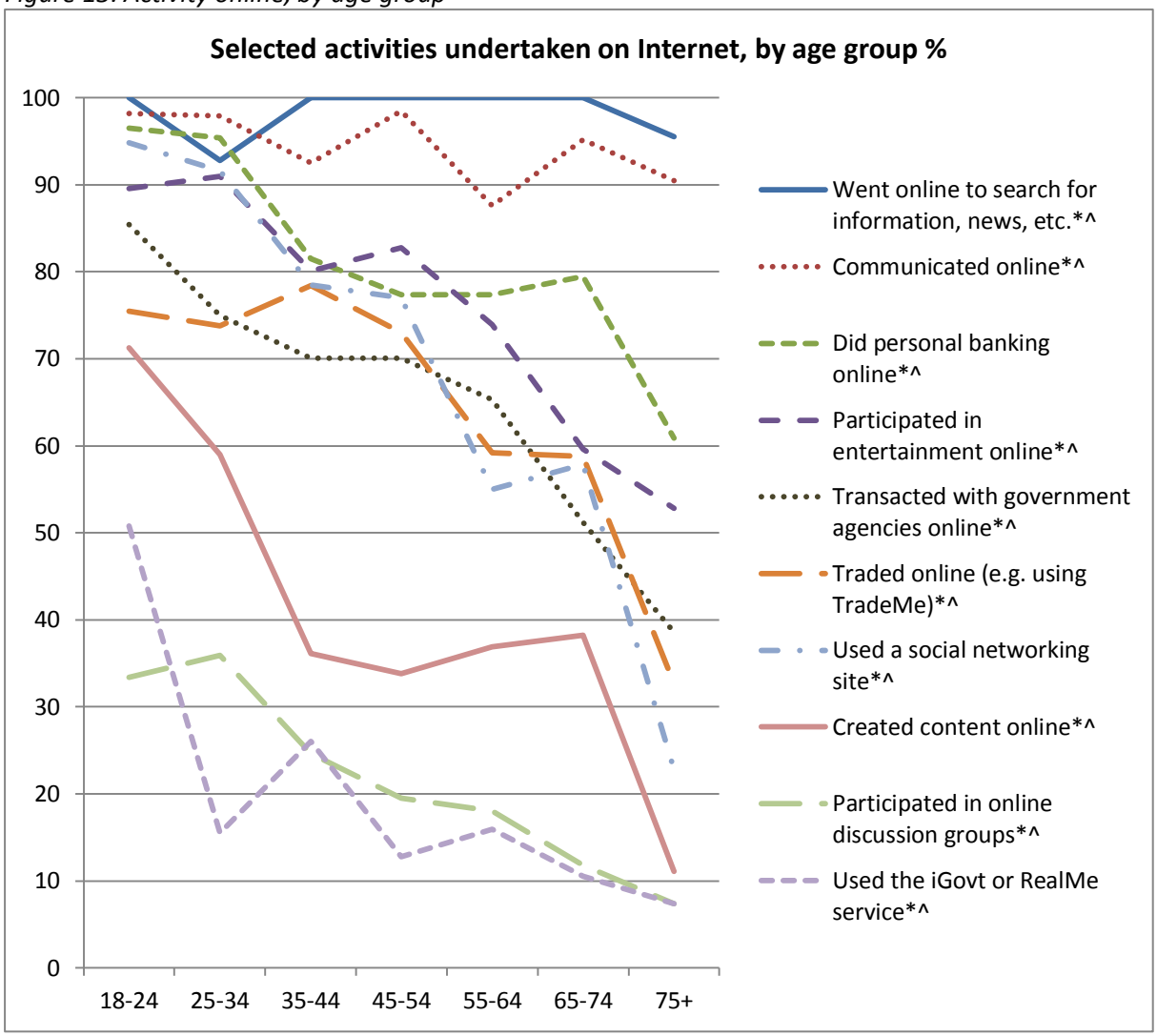


Mobile device (p=.000); school (p=.000); public library (p=.019)
^Confidence intervals: At work (18-24yrs: 2.99-4.53; 25-34 years: 1.70-2.92; 35-44 years: 1.78-2.99; 45-54 years: 1.70-2.66; 55-64 years: 2.09-3.18; 65-74 years: 4.17-5.32; 75+ years: 4.27-6.36); at school (18-24yrs: 3.72-5.20; 25-34 years: 4.88-5.84; 35-44 years: 5.37-5.98; 55-64 years: 5.43-6.03); on a mobile (18-24yrs: 1.85-2.80; 25-34 years: 1.74-2.89; 35-44 years: 1.97-3.08; 45-54 years: 2.62-3.65; 55-64 years: 3.62-4.63; 65-74 years: 4.09-5.33); at a public library (18-24yrs: 5.10-5.70; 65-74 years: 5.32-5.88)

Online activities in the last 12 months

In general, a declining trend across age groups can be observed for a variety of activities online, including online personal banking^, online government transactions^, online entertainment^, creating online content^ and using a SNS^. However, exceptions were found for people going online to search for information^ and, to a lesser extent, people communicating online^ (see Figure 13).

Figure 13: Activity online, by age group



Search for information, news etc (p=.000); communicated (p=.036); personal banking (p=.005); entertainment participation (p=.010); transacted with government agencies (p=.011); traded online (p=.047); used social networking site (p=.000); participated in discussion groups (p=.035); used RealMe (formerly iGovt) (p=.000)
^Confidence intervals: Search for information, news (75+ years: 73%-99%); communicated online (18-24yrs: 88%-100%; 25-34 years: 86%-100%; 35-44 years: 83%-97%; 55-64 years: 78%-93%; 65-74 years: 86%-98%; 75+ years: 70%-98%); did personal banking (18-24yrs: 87%-99%; 25-34 years: 83%-99%; 35-44 years: 67%-90%; 45-54 years: 66%-86%; 55-64 years: 66%-86%; 65-74 years: 67%-88%; 75+ years: 39%-79%); participated in entertainment (18-24yrs: 65%-98%; 25-34 years: 78%-97%; 35-44 years: 67%-89%; 45-54 years: 72%-90%; 55-64 years: 63%-83%; 65-74 years: 46%-72%; 75+ years: 30%-75%); transacted with government agencies (18-24yrs: 74%-93%; 25-34 years: 60%-86%; 35-44 years: 56%-81%; 45-54 years: 58%-80%; 55-64 years: 54%-76%; 65-74 years: 38%-64%; 75+ years: 19%-62%); traded online (18-24yrs: 56%-88%; 25-34 years: 59%-85%; 35-44 years: 66%-87%; 45-54 years: 61%-82%; 55-64 years: 47%-70%; 65-74 years: 46%-71%; 75+ years: 15%-57%); used a SNS (18-24yrs: 85%-98%; 25-34 years: 80%-97%; 35-44 years: 65%-88%; 45-54 years: 65%-86%; 55-64 years: 43%-66%; 65-74 years: 45%-70%; 75+ years: 8.9%-47%); created content online (18-24yrs: 59%-81%; 25-34 years: 44%-73%; 35-44 years: 24%-50%; 45-54 years: 24%-46%; 55-64 years: 26%-49%; 65-74 years: 26%-52%; 75+ years: 3.2%-32%); participated in online discussion groups (18-24yrs: 22%-48%; 25-34 years:23%-51%; 35-44 years: 15%-38%; 45-54 years:12%-30%; 55-64 years: 11%-29%; 65-74 years: 5.4%-24%; 75+ years: 1.2%-34%); used iGovt or RealMe (18-24yrs: 34%-68%; 25-34 years: 7.6%-29%; 35-44 years: 16%-40%; 45-54 years: 6.9%-23%; 55-64 years: 8.9%-27%; 65-74 years: 4.4%-23%; 75+ years: 1.2%-34%)

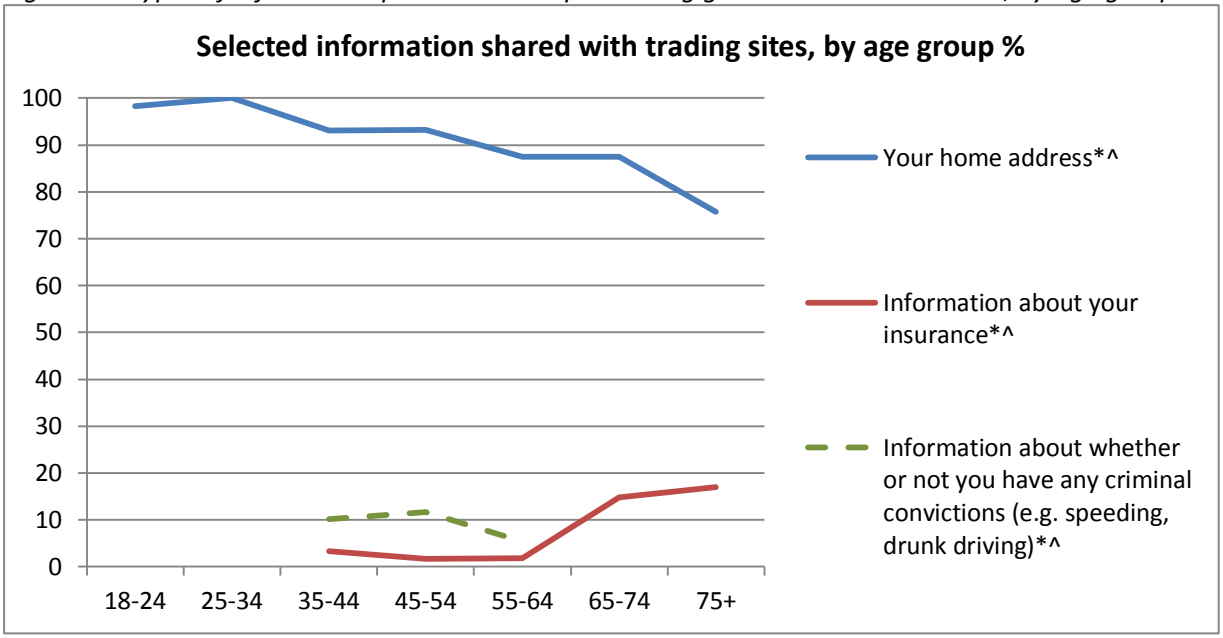
Identity information provided in online commercial transactions

Younger generations demonstrate different online privacy behaviours in commercial transactions, compared with older generation. For instance, the sharing of a home address^ in online commercial activities declined with age, with almost 100 percent of respondents between 18 and 34 years of age^ indicating that they had provided their home address in these online transactions and only 76 percent of the oldest age group (75 years and older^) doing so (see Figure 14).

Respondents between 35 and 74 years of age^ provided in online commercial transactions identity information on their insurance^[43]. This development slightly increased for people of 55 and 64 years^ of age and then again for people between 65 and 74 years of age^.

A small proportion of respondents between 35 and 64 years of age^ provided in online commercial activities personal information on whether or not they have any criminal convictions^[44]

Figure 14: Types of information provided when purchasing goods and services online, by age group.



Home address (p=.027); insurance information (p=.001); information about criminal convictions (p=.012)
^Confidence intervals: home address (18-24yrs: 88%-100%; 35-44 years: 81%-98%; 45-54 years: 83%-98%; 55-64 years: 77%-94%; 65-74 years: 76%-94%; 75+ years: 47%-92%); insurance information (18-24yrs: 0.2%-12%; 25-34 years: no data; 35-44 years: 0.7%-14%; 45-54 years: 0.2%-12%; 55-64 years: 0.2%-12%; 65-74 years: 7.3%-28%; 75+ years: 4.2%-49%); whether or not you have criminal convictions (18-24yrs: 0.3%-12%; 25-34 years: no data; 35-44 years: 4.1%-23%; 45-54 years: 5.7%-22%; 55-64 years: 1.7%-16%; 65-74 years: no data; 75+ years: no data)

Why identity information is provided in online commercial transactions

14 percent of young people up to 24 years of age^ indicated that they don't know^[45] why they provide their identity information in online commercial transactions. They provided this particular main reason significantly more than people of 25 years and older^.

[43] 25-34 years: no data
[44] 25-34 years: no data; 65-74 years: no data; 75+ years: no data

Identity information provided in transactions with government online

Younger generations demonstrate different online privacy behaviours in transactions with government, compared with older generations. Significant differences across age groups can be found for sharing an IRD number^, student number^, passport number^, health services number^, educational background^, information about New Zealand citizenship, residence or visa status^ and community service card number^ (see Figure 15).

Respondents belonging to the younger age groups^ much more often provided their IRD number^, student number^[46], and educational background information^ in online transactions with government than people belonging to older generations^. However, people who are 45 years and older^ shared their passport number^ more in online transactions with government, compared with those from younger generations^.

A possible explanation for these different online privacy behaviours across generations might be that younger generations prefer online channels over offline channels in their interactions with government, whereas older generations seem to prefer offline over online channels in government transactions.

Why identity information is provided in online government transactions

The value proposition for providing identity information in online transactions with government is different for varying age groups. For instance, significant differences across age groups could be found with regard to the main reasons for providing identity information in online government transactions, particularly around convenience^ and, to a lesser extent, receiving a price reduction^ and the reason "*it doesn't bother me*"^[47].

Participants of 35 years and older^ more frequently indicated convenience^ as one of the main reasons to provide identity information in online government transactions, compared with people under 35 years of age^.

Respondents between 55 and 74 years of age^ mentioned receiving a price reduction^[48] as one of the most important reasons to provide their personal information in online transactions with government.

Participants from the younger age groups^ in particular, but also people between 55 and 64 years of age^ (4%), indicated as one of the main reasons to provide identity information in online government transactions that it doesn't bother them^[49].

---

[45] P= 0.036; ^Confidence intervals: 18-24 years: 4.4%-36%; 25-34 years: 0.3%-14%; 35-33 years: 1.6%-17%; 45-54 years: no data; 55-64 years: 2.0%-14%

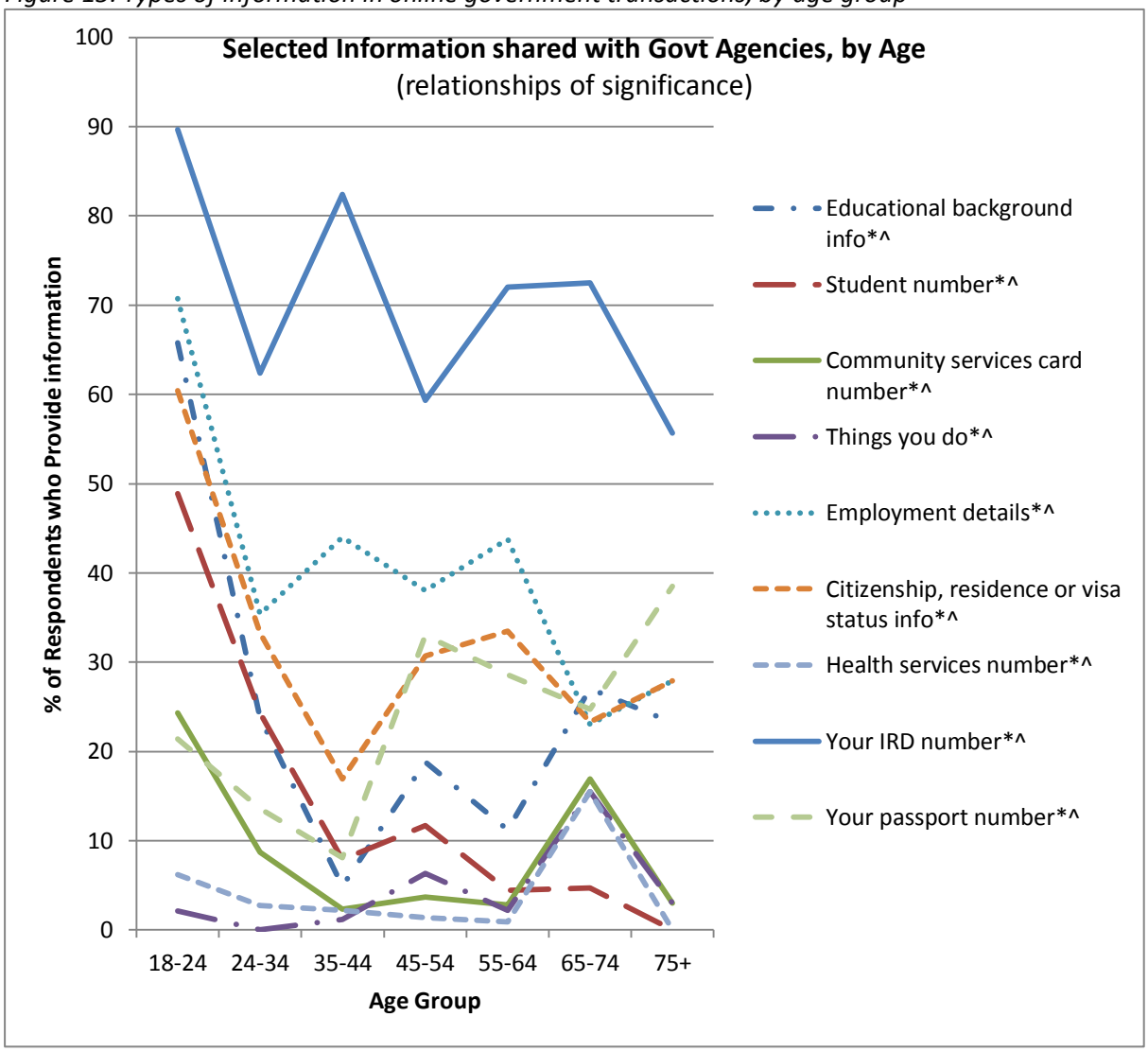
[46] 75+ years: no data

[47] ^Confidence intervals: convenience (18-24yrs: 3.0%-19%; 25-34 years: 6.8%-30%; 35-44 years: 17%-44%; 45-54 years: 22%-48%; 55-64 years: 33%-60%; 65-74 years: 21%-51%; 75+ years: 7.2%-60%); receive a discount (18-24yrs: no data; 25-34 years: no data 35-44 years: no data; 45-54 years: no data; 55-64 years: 1.9%-17%; 65-74 years: 0.4%-17%; 75+ years: no data); it doesn't bother me (18-24yrs: 0.3%-13%; 25-34 years: 2.5%-22%; 35-44 years: no data; 45-54 years: no data; 55-64 years: 1.0%-15%; 65-74 years: no data; 75+ years: no data)

[48] 18-24yrs: no data; 25-34 years: no data 35-44 years: no data; 45-54 years: no data; 75+ years: no data

[49] 35-44 years: no data; 45-54 years: no data; 65-74 years: no data; 75+ years: no data

Figure 15: Types of information in online government transactions, by age group



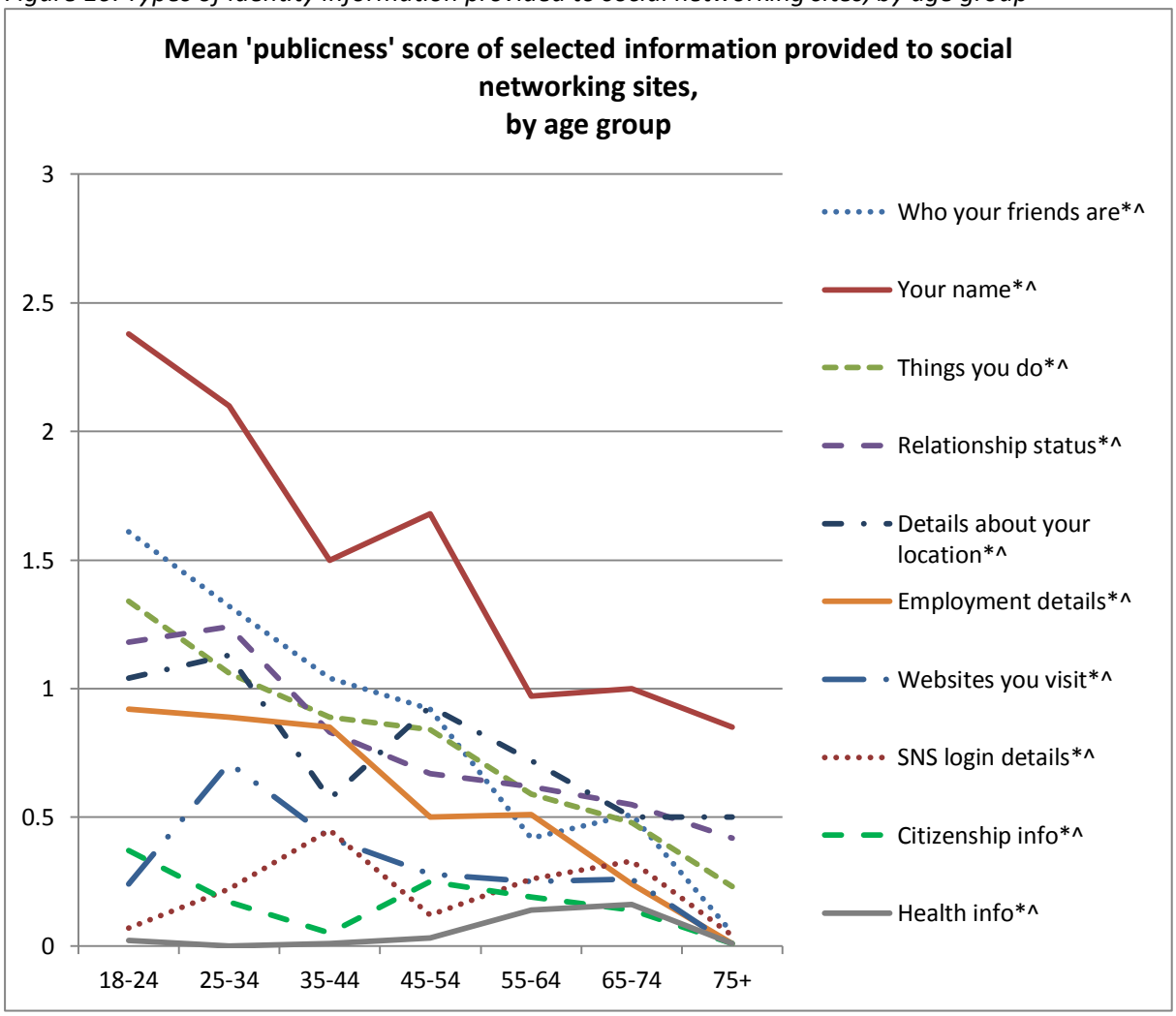
Educational background information (p=.000); student number (p=.000); community services card number (p=.001); things you do (p=.003); employment details (p=.004); NZ citizenship, residence or visa status information (p=.006); health services number (p=.006); your IRD number (p=.014); your passport number (p=.034)

^Confidence intervals: educational background (18-24yrs: 52%-77%; 25-34 years: 13%-40%; 45-54 years: 12%-32%; 55-64 years: 4.7%-24%; 65-74 years: 15%-44%; 75+ years: 3.8%-70%); student number (18-24yrs: 30%-68%; 25-34 years: 13%-41%; 35-44 years: 2.7%-21%; 45-54 years: 5.2%-24%; 55-64 years: 1.1%-16%; 65-74 years: 1.1%-19%; 75+ years: no data); community services card number (18-24yrs: 11%-46%; 25-34 years: 2.7%-24%; 45-54 years: 0.9%-15%; 65-74 years: 7.8%-33%; 75+ years: 0.3%-21%); things you do (18-24yrs: 0.3%-14%; 25-34 years: no data; 45-54 years: 2.4%-16%; 55-64 years: 0.3%-14%; 65-74 years: 6.8%-32%; 75+ years: 0.3%-22%); employment details (18-24yrs: 57%-81%; 25-34 years: 22%-52%; 35-44 years: 29%-60%; 45-54 years: 26%-52%; 55-64 years: 31%-58%; 65-74 years: 12%-39%; 75+ years: 5.9%-79%); citizenship info (18-24yrs: 40%-78%; 25-34 years: 20%-50%; 35-44 years: 7.9%-33%; 45-54 years: 19%-45%; 55-64 years: 22%-48%; 65-74 years: 12%-40%; 75+ years: 5.9%-79%); health services number (18-24yrs: 2.0%-18%; 25-34 years: 0.4%-17%; 65-74 years: 6.8%-32%; 75+ years: no data); IRD number (18-24yrs: 78%-96%; 25-34 years: 46%-77%; 35-44 years: 68%-91%; 45-54 years: 45%-72%; 55-64 years: 58%-83%; 65-74 years: 56%-85%; 75+ years: 21%-86%); passport number (18-24yrs: 12%-35%; 25-34 years: 5.7%-29%; 35-44 years: 2.8%-21%; 45-54 years: 21%-47%; 55-64 years: 17%-43%; 65-74 years: 13%-41%; 75+ years: 11%-76%)

Sharing identity information as part of social networking

In general, younger generations are less private with their personal information on SNSs compared to older generations: a declining trend is observable for most types of personal information provided on SNSs across different age groups (see Figure 16). However, a different pattern is visible for providing SNS account details^ and personal information about the websites you visit on SNSs^, with respondents from the youngest and oldest age brackets being more private about this personal information than others. Also, health information is less shared on SNSs by people from younger generations compared to others, with the exception of respondents of 75 years and over.

Figure 16: Types of identity information provided to social networking sites, by age group



Name (p=.000), current location (p=.000), health information (p=.009), employment details p=.000), information about educational background (p=.004), information about NZ residential status (p=.011), hobbies (p=.000), personal information and taste (p=.000), photos of you (p=.000), friends (p=.000), relationships (p=.008), personal account details (p=.002), websites you visit (p=.000).

^Confidence intervals: your name (18-24yrs: 2.02-2.73; 25-34 years: 1.79-2.40; 35-44 years: 1.19-1.82; 45-54 years: 1.39-1.97; 75+ years: 0.38-1.33); details about location (25-34 years: 0.83-1.44; 75+ years: 0.07-0.93); employment details (18-24yrs: 0.42-1.43; 25-34 years: 0.59-1.19; 35-44 years: 0.54-1.17); things you do (25-34 years: 0.80-1.33; 35-44 years: 0.60-1.19; 45-54 years: 0.58-1.10; 55-64 years: 0.32-0.86); who your friends are (18-24yrs: 1.35-1.87; 25-34 years: 1.06-1.58; 35-44 years: 0.76-1.31; 45-54 years: 0.65-1.19); relationship status (18-24yrs: 0.72-1.65; 25-34 years: 0.94-1.54; 35-44 years: 0.53-1.13; 45-54 years: 0.41-0.92; 55-64 years: 0.35-0.88; 65-74 years: 0.27-0.82; 75+ years: -0.35-1.19); citizenship information (18-24yrs: -0.07-0.82); your SNS login details (35-44 years: 0.18-0.72); websites you visit (25-34 years: 0.41-1.00)

Why identity information is provided on Social Networking Sites

There is a different value proposition for providing identity information on SNSs for older generations compared with younger generations.

People of 65 years and older^ much more often indicated convenience^[50] as the main reason for providing identity information on SNSs, compared to people of 64 years and younger^.

A small proportion of the respondents of 75 years and older^ (8.4%) indicated getting a discount^[51] as an important reason for providing personal information on SNSs.

However, younger people until 44 years of age^ indicate the reason to connect with others^[52] significantly more than people of 45 years and older^.

Trust in organisations to protect identity information

Trust patterns around what public and private sector organisations do to protect personal information are similar across age groups and for different types of institutions. In general, younger generations tend to trust organisations more to protect their identity information than older generations (see *Figure 17)*.

Steps taken to protect online identity information

In general, younger generations use different tools and strategies to protect their identity information online compared with older generations (see Figure 18). An example is the use of RealMe (formerly iGovt)^ by 48 percent of the youngest age group^ compared to 8.8 percent of the 65-74 years old^, which makes the youngest age group the most active users of RealMe.

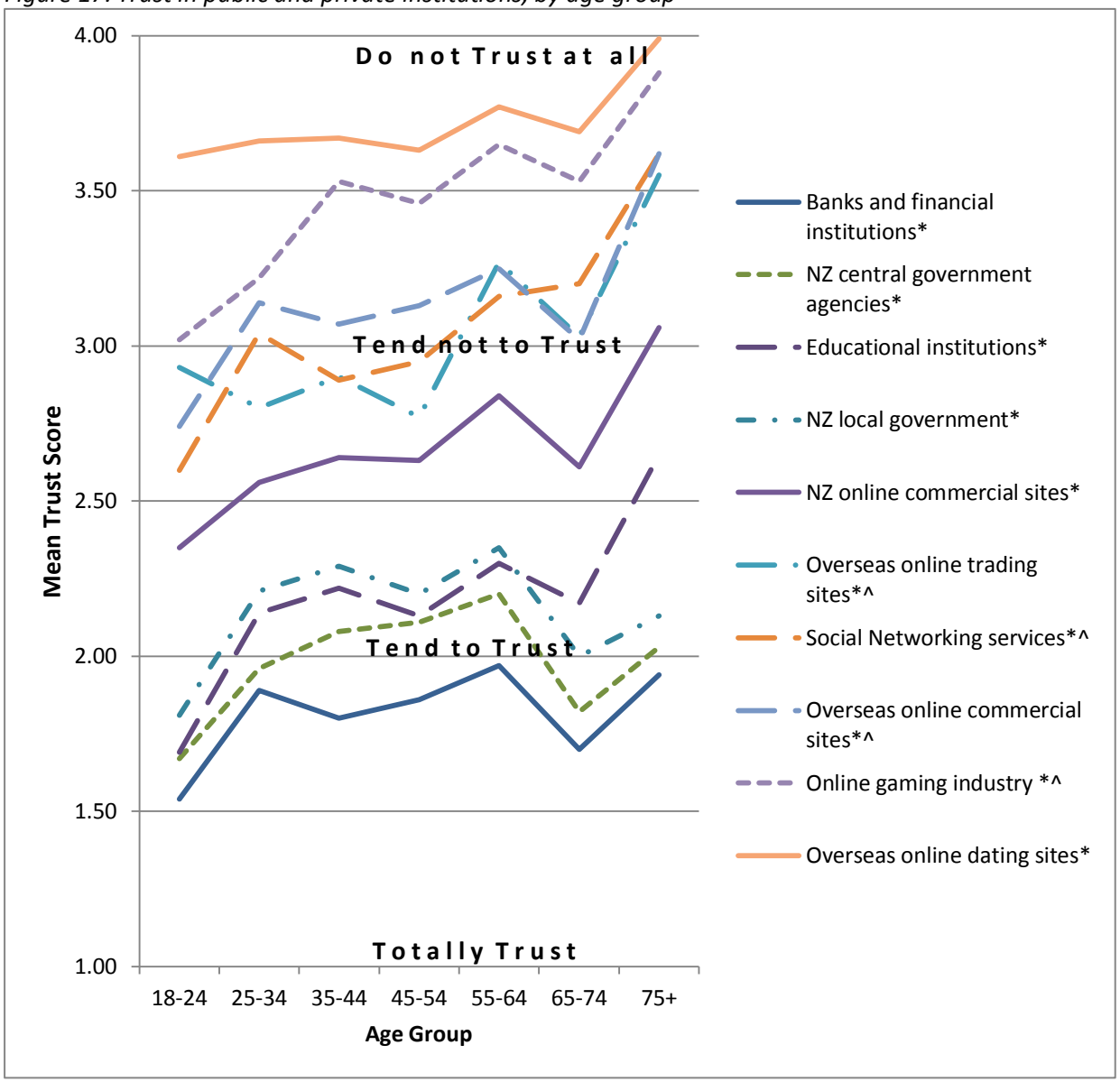
People between 24-35 years of age^ used the protection strategy of changing privacy settings^ not only more frequently (90%) than respondents belonging to the youngest age group^ (75%) and those respondents between 35 and 44 years of age^ (70%), but also much more frequently than older generations^.

Similarly, in the case of using tools and strategies to limit unsolicited emails^, people from the age group of 24-35^ are the most active users (93%), followed by respondents belonging to the youngest age group^ (83%) and those between 35 and 44 years of age^ (72%).

A significantly larger proportion of people from the age groups of 45 years of age and over^ do not provide any identity information via online channels^, compared with people of 44 years of age and younger^.

[50] P= 0.019; ^Confidence intervals: Convenience (18-24yrs: 1.7%-16%; 25-34 years: 1.1%-16%; 35-44 years: 3.0%-19%; 45-54 years: 3.2%-18%; 55-64 years: 4.3%-21%; 65-74 years: 14%-39%; 75+ years: 8.9%-56%);
[51] P= 0.000; ^Confidence intervals: to get a discount (18-24yrs: no data; 25-34 years: no data; 35-44 years: no data; 55-64 years: no data; 65-74 years: no data; 75+ years: 1.1%-42%);
[52] P= 0.000; ^Confidence intervals: to connect with people (18-24yrs: 53%-87%; 25-34 years: 53%-81%; 35-44 years: 52%-79%; 45-54 years: 27%-50%; 55-64 years: 32%-57%; 65-74 years: 27%-54%; 75+ years: 5.3%-49%)

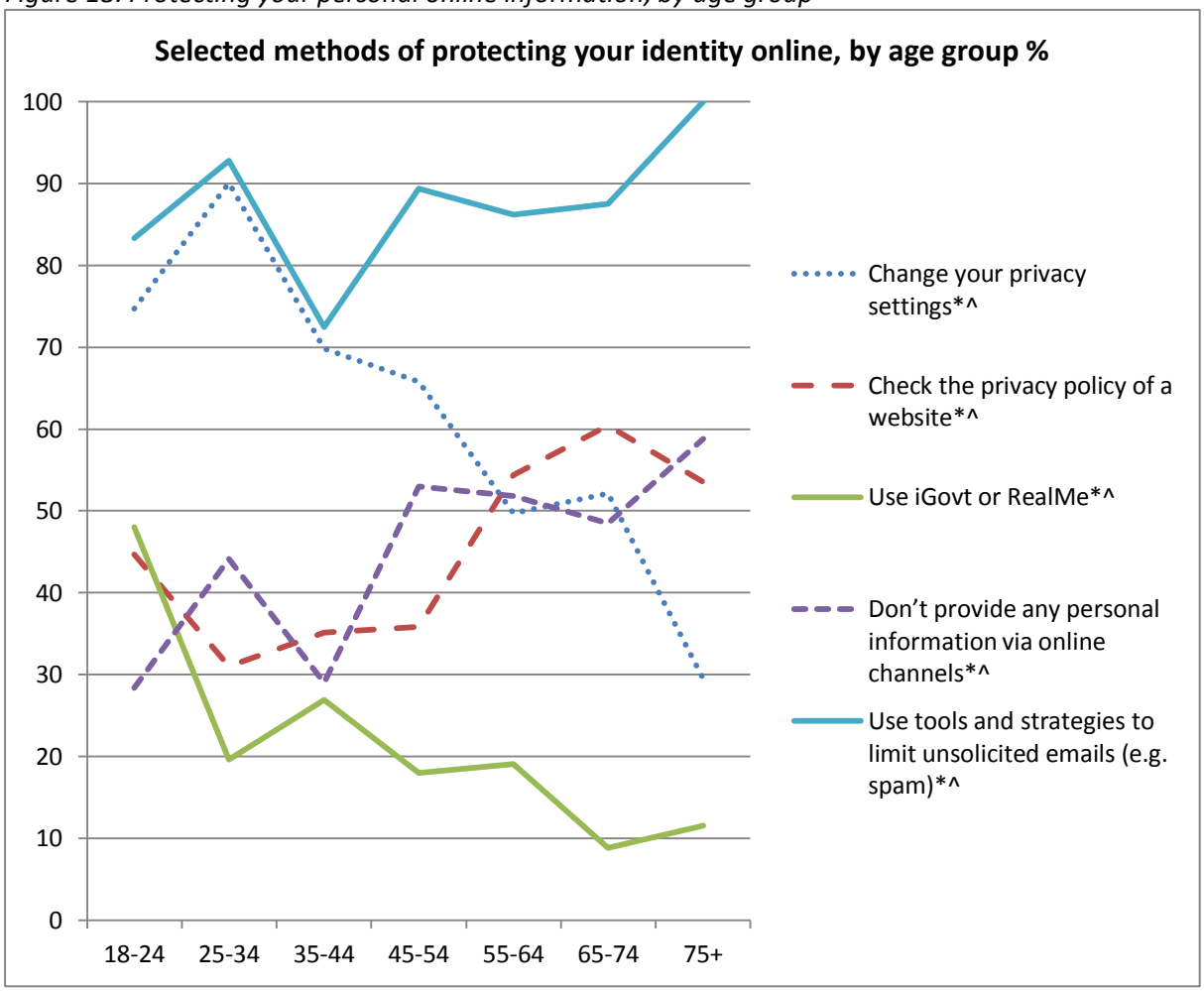
Figure 17: Trust in public and private institutions, by age group



Banks and financial institutions (p=.037); NZ central government agencies (p=.004); educational institutions (p=.000); NZ local government (p=.004); NZ online commercial sites (p=.005); overseas online trading sites (p=.002); social networking sites (p=.000); overseas online commercial sites (p=.002); online gaming industry (p=.000); overseas online dating sites (p=.000)

^Confidence intervals: Overseas commercial sites (75+ years: 3.30-3.94); social networking sites (75+ years: 3.32-3.91); overseas trading sites (35-44 years: 2.64-3.16; 75+ years: 3.19-3.92); online gaming (25-34 years: 2.93-3.51)

Figure 18: Protecting your personal online information, by age group

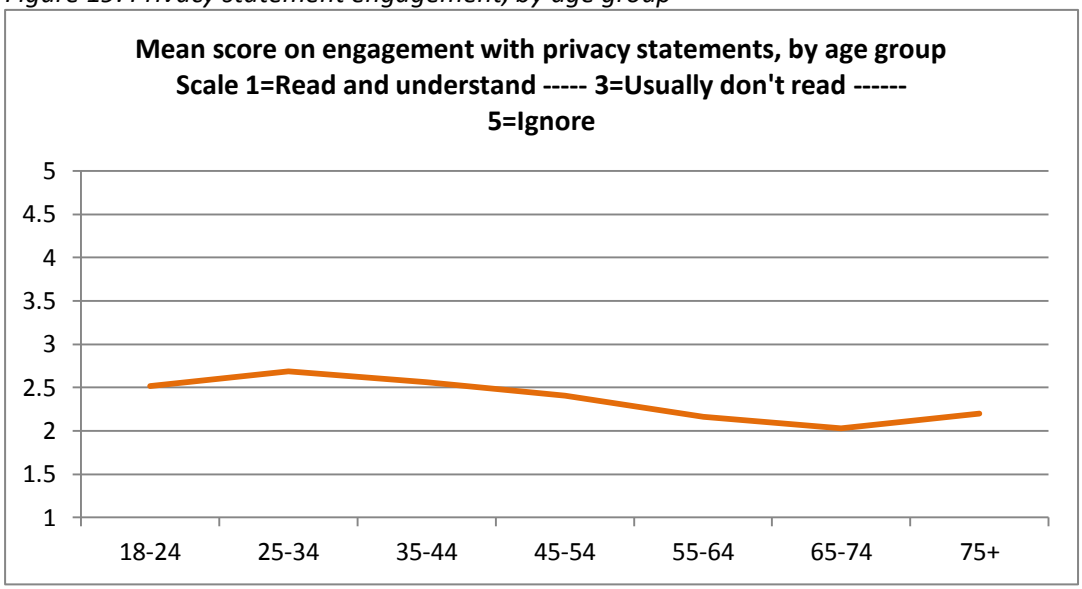


Changing privacy settings (p=.000; ^confidence intervals – 18-24yrs: 55%-88%; 25-34yrs: 76%-96%; 35-44yrs: 55%-81%; 45-54yrs: 53%-77%; 55-64yrs: 38%-62%; 65-74yrs: 38%-65%; 75+yrs: 11%-59%), using tools and strategies to limit unsolicited e-mails (p=.029: confidence intervals – 18-24yrs: 71%-91%; 25-34yrs: 79%-98%; 35-44yrs: 59%-83%; 45-54yrs: 80%-95%; 55-64yrs: 76%-93%; 65-74yrs: 77%-94%), checking the privacy policy of a website (p=.033; ^confidence intervals – 18-24yrs: 28%-63%; 25-34yrs: 19%-47%; 35-44yrs: 23%-50%; 45-54yrs: 25%-48%; 55-64yrs: 42%-62%; 65-74yrs: 47%-73%; 75+yrs: 27%-78%), using iGovt or Realme (p=.003: confidence intervals – 18-24yrs: 30%-67%; 25-34yrs: 9.6%-36%; 35-44yrs: 16%-42%; 45-54yrs: 10%-30%; 55-64yrs: 11%-31%; 65-74yrs: 3.3%-21%; 75+yrs: 1.9%-47%) and not providing any personal information via online channels (p=.038: ^confidence intervals – 18-24yrs: 17%-44%; 25-34yrs: 29%-60%; 35-44yrs: 18%-44%; 45-54yrs: 40%-66%; 55-64yrs: 39%-64%; 65-74yrs: 35%-62%; 75+yrs: 32%-81%).

Privacy statements

Older generations usually read privacy statements^ on the Internet but do not fully understand them, whereas younger generations^ usually do not read privacy statements on the Internet (see Figure 19).

Figure 19: Privacy statement engagement, by age group



(p=.008; ^confidence intervals – 18-24yrs: 2.19-2.85; 25-34yrs: 2.36-3.02; 35-44yrs: 2.24-2.88; 75+yrs: 1.61-2.80)

User experiences with forms of cybercrime or cyber-enabled crime

Older generations seem to have different personal experiences with forms of cyber-enabled crime, compared with younger generations (see Figure 20).

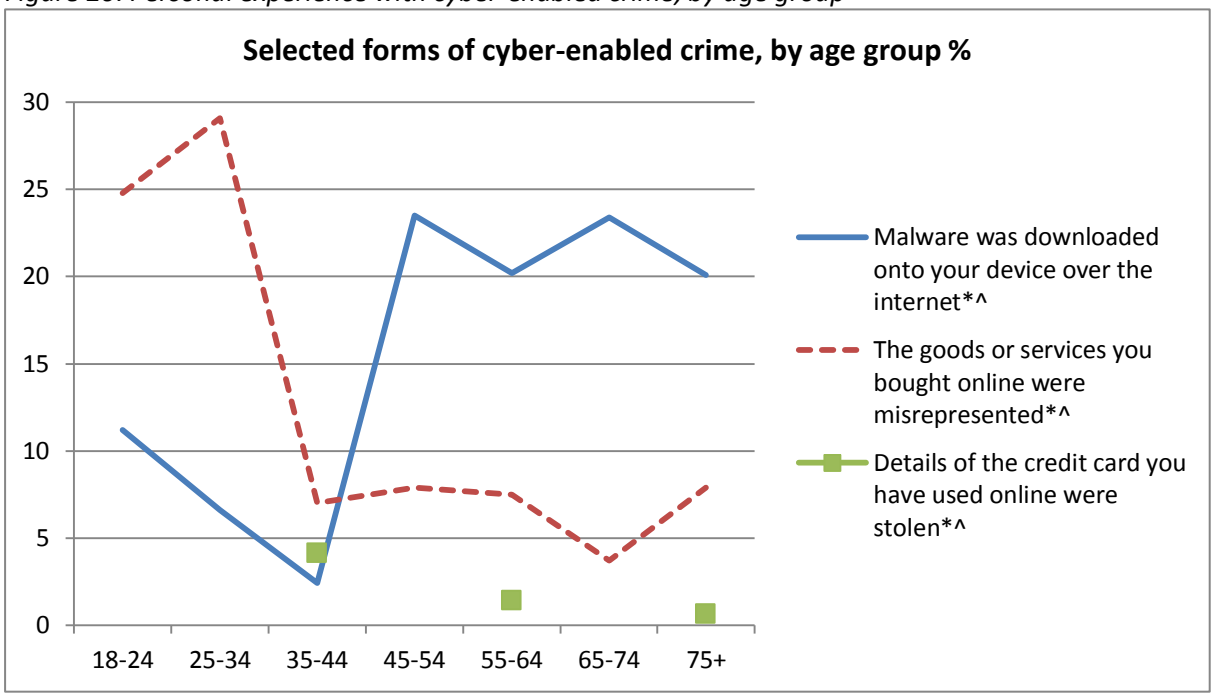
For instance, people from 45 years and over^ had more frequently experienced situations in which malware^ was downloaded onto their device, compared to younger generations^.

However, personal experiences around misrepresented goods and services bought online^ were far more common amongst respondents from the 25-34 age group^ (29%) and those between 18 and 24 years of age^ (25%), compared to others^.

Stolen credit card details^[53] was a personal experience reported by people of 35-44 years of age^, those of 55-64 years of age, and people of 75 years and older.

[53] *18-24yrs: no data; 25-34 years: no data; 45-54 years: no data; 65-74 years: no data*

Figure 20: Personal experience with cyber-enabled crime, by age group



Malware downloaded (p=.005); goods or services misrepresented (p=.000); credit card details stolen (p=.041)
^Confidence intervals: Malware downloaded (18-24yrs: 5.1%-23%; 25-34 years: 2.1%-19%; 35-44 years: 0.3%-15%; 45-54 years: 15%-35%; 55-64%: 12%-31%; 65-74 years: 14%-37%; 75+ years: 7.0%-46%); goods or services misrepresented (18-24yrs: 12%-44%; 25-34 years: 18%-44%; 35-44 years: 2.5%-18%; 45-54 years: 3.5%-17%; 55-64%: 3.4%-16%; 65-74 years: 0.9%-14%; 75+ years: 1.7%-30%); credit card details stolen (18-24yrs: no data; 25-34 years: no data; 35-44 years: 1.0%-15%; 45-54 years: no data; 55-64 years: 0.2%-9.3%; 65-74 years: no data; 75+ years: 0.1%-4.1%)

Ethnicity

Using the Internet

Māori^ are significantly more likely to access the Internet via a mobile device^[54] (mean frequency score: 2.76), than non- Māori^ (mean frequency score: 3.25). However, Asian people^ use a mobile device^ most frequently to go onto the Internet (mean frequency score: 1.53).

Of all ethnic groups, NZ Europeans were the highest users of an e-book reader^ to go online (9.3%).

Online activities in the last 12 months

People from different ethnic backgrounds indicate varying engagement in several online activities in the last 12 months (see Table 11).

All NZ Europeans and Asians indicated to have searched for information online^ in the last 12 months. However, small proportions of the Māori population^ (6%) and Pasifika^ population (9%) didn't go online to search for information.

[54] ^Confidence intervals: Accessing via a mobile device (Māori: 2.39-3.14; non-Māori: 2.99-3.50)

NZ Europeans (89%) and Māori^ (88%) were more likely to have purchased commercial goods or services online^, than Asian people^ (74%) or Pasifika^ (65%).

Of all ethnic groups, Asian people^ were mostly engaged in the creation of content online^ (63%), followed by Māori^ (55%) and NZ Europeans (41%). Pasifika^ were the least engaged in this online activity (30%).

Table 11: Online activities in the last 12 months, by ethnicity group

Online Activity	NZ Europeans	Māori	Pasifika	Asians	Sig
Went online to search for information, news, etc.*^	100	94	91	100	0.000
Purchased something online*^	89	88	65	74	0.025
Created content online*^	41	55	30	63	0.038

^Confidence intervals: Searched for information (Maori 80%-98%; Pasifika 58%-99%), purchased online (Maori 78%-94%; Pasifika 35%-87%; Asians 53%-88%), created content (Maori 34%-57%; Pasifika 40%-89%; Asians 20%-58%)

Identity information provided in online commercial transactions

People from different ethnic backgrounds demonstrate varying identity information behaviours in online commercial transactions.

Māori were significantly more likely than non-Māori to share the following types of identity information in online commercial transactions^[55]:

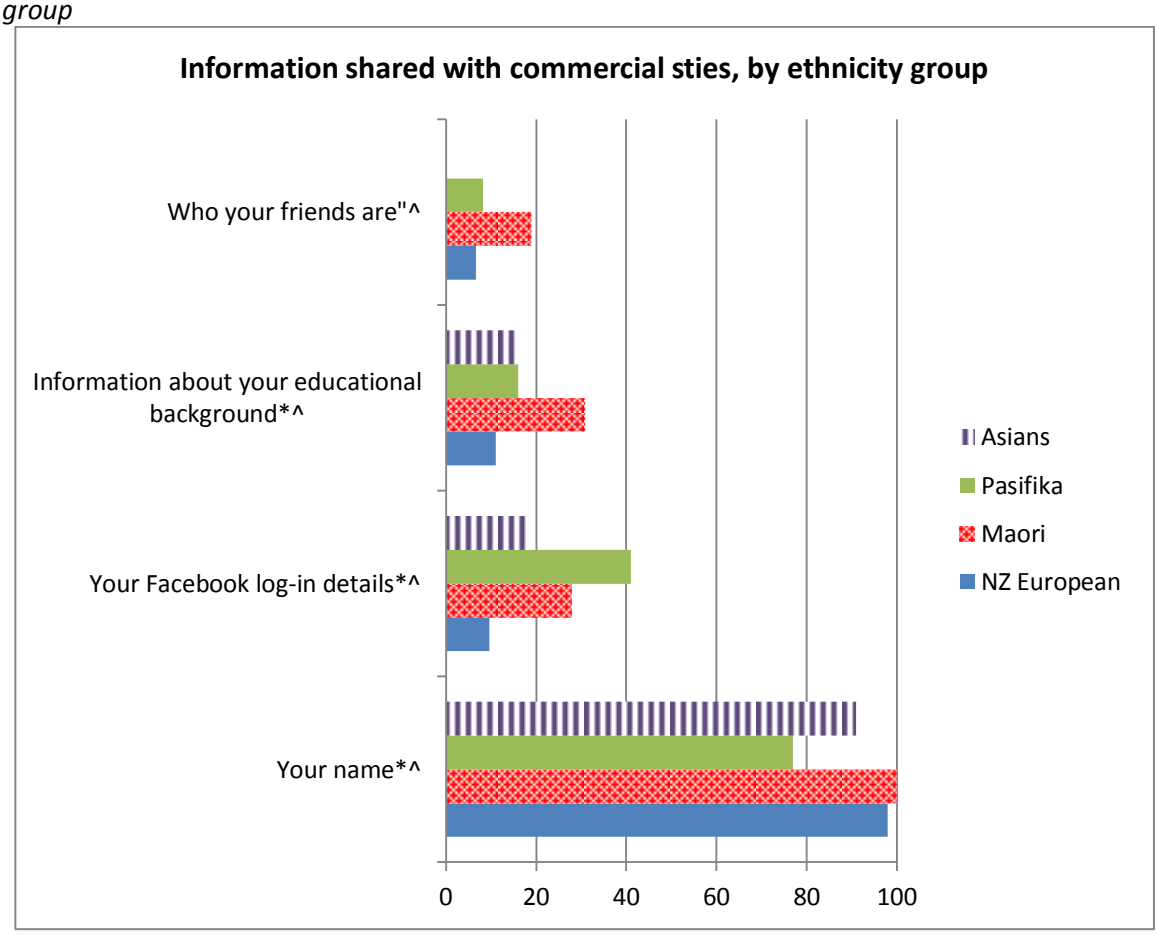
- Name*: 100%, compared to 97% for non-Māori (p= .000);
- Home address*: 98%, compared to 92% for non-Māori (p=.040);
- Billing address*: 97%, compared to 86% for non-Māori (p=.006);
- Information about their educational background*^: 31%^, compared to 11% for non-Māori (p=.008);
- Information about their New Zealand citizenship, residence or visa status*^: 27%^, compared to 13% for non-Māori (p=.015);
- Employment details*^: 30%^, compared to 13% for non-Māori (p=.019);
- Health information*^: 11%^, compared to 4.3% for non-Māori (p=.040).
- Facebook log-in details*^: 28%^, compared to 11% for non-Māori (p=.024);
- Who their friends are*^: 19%^, compared to 6.3% for non-Māori (p=.004); and
- Personal opinions and tastes*^: 28%, compared to 16% for non-Māori (p=.038).

Across ethnic groups, the following differences in identity information behaviours could be observed (see Figure 21)

[55] ^Confidence intervals: Educational background (Māori: 16%-51%); information about citizenship etc (Māori: 17%-41%); employment details (Māori: 15%-51%); health information (Māori: 5.1%-24%); Facebook log-in details (Māori: 14%-48%); who your friends are: (Māori: 10%-33%); personal opinions (Māori: 17%-41%)

- Name*^: 100 percent of the Māori population provided their name in online commercial transactions, followed by 98 percent of the NZ Europeans and 91 percent of the Asian people^. However, only 77 percent of the Pasifika^ did so;
- Educational background information*^: Māori^ were significantly more likely in online commercial transactions to provide information about their educational background (31%), than Pasifika^ (16%), Asians^ (16%) or NZ Europeans^ (11%);
- Facebook log-on details*^: Pasifika^ were significantly more likely in online commercial transactions to provide their Facebook log-on details (41%), compared to Māori^ (28%), Asians^ (18%) or NZ Europeans (9.7%);
- Who your friends are*^: Māori^ were significantly more likely in online commercial transactions to provide information about who their friends are (19%) than Pasifika^ (8.2%) or NZ Europeans (6.7%).

Figure 21: Types of information provided when purchasing goods and services online, by ethnicity group



^Confidence intervals: your name (Pasifika 40%-94%; Asians 68%-98%), educational background (Māori 16%-51%; Pasifika 3.9%-49%; Asians 4.9%-40%), Facebook login details (Māori 14%-48%; Pasifika 15%-73%; Asians 6.0%-44%), who your friends are (Māori 10%-33%; Pasifika 1.1%-42%, Asians no data)

Why identity information is provided in online commercial transactions

The most important reasons for providing identity information in online commercial transactions varied for participants from different ethnic backgrounds.

Non-Māori more frequently indicated getting a financial discount as an important reason for disclosing their identity information in online commercial transactions (10%), compared with Māori (0.1%).

Pasifika^ more frequently indicated to provide their identity information in online commercial relationships in order to connect with others^[56] (28%), compared to Māori^ (6%) or NZ Europeans (2.9%).

Identity information provided in transactions with government online

People from different ethnic backgrounds also demonstrate varying identity information behaviours in their online transactions with government.

Māori^ are significantly more likely than non-Māori^ to share the following types of identity information when transacting with government agencies online[57]:

- Educational background information*^: 46%^, compared to 20% for non-Māori (p=.000);
- Employment details*^: 61%^, compared to 40% for non-Māori^ (p=.007);
- Social welfare number*^: 34%^, compared to 7.6% for non-Māori (p=.000);
- Community services card number*^: 34%^, compared to 4.5% for non-Māori (p=.000);
- Health information*^: 24%^, compared to 7% for non-Māori (p=.013);
- Things they do*^: 9.4%^, compared to 2.9% for non-Māori (p=.019); and
- Personal opinions*^: 19%^, compared to 7.8% for non-Māori (p=.024).

Across ethnic groups, the following differences in identity information behaviours could be observed (see Figure 22).

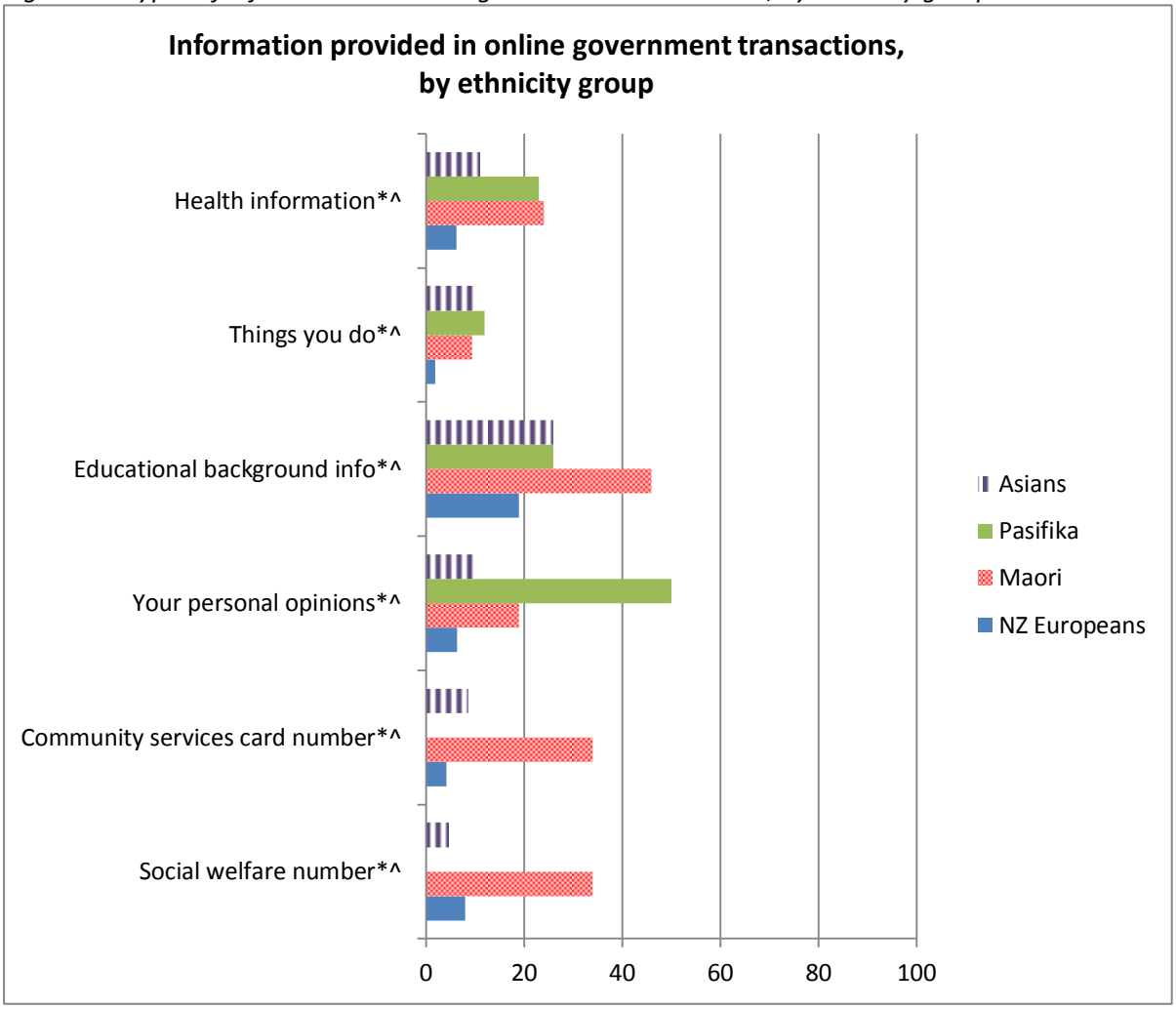
- Educational background information*^: Māori^ (46%) were the most likely to disclose educational background information in online transactions with government, followed by Pasifika^ (26%) and Asians^ (26%). NZ Europeans^ (19%) were the least likely to do so (p=0.003);
- Social welfare number*^: Māori^ (34%) were significantly more likely than NZ Europeans (8%) or Asians^ (4.7%) to disclose their social welfare number in online government transactions (p=0.000);
- Community service card number*^: Māori^ (34%) were far more likely than Asians^ (8.7%) or NZ Europeans (4.2%) to disclose their community service card number in online government transactions (p=0.000);
- Health information*^: Māori^ (24%) and Pasifika^ (23%) were more likely than Asians^ (11%) to provide health information in online transactional relationships with government. However, NZ Europeans were the least likely to do so (6.2%) (p=0.024);
- Things you do*^: Pasifika^ were more likely to disclose the things they do in online government transactions (12%), than Asians^ (9.9%) or Māori^ (9.4%). However, NZ Europeans were significantly less likely to do so (1.9%) (p=0.017);

[56] ^Confidence intervals: To connect with others (Pasifika 8.6%-61%; Asians no data)

[57] ^Confidence intervals: Health information (Māori: 9.6%-49%); employment details (Māori: 47%-73%; non-Māori: 34%-47%); educational background (Māori: 36%-57%); things you do (Māori: 4.3%-19%); social welfare number (Māori: 17%-57%); community services card (Māori: 17%-56%); personal opinions (Māori: 9.9%-35%)

- Personal opinions*^: 50% of the Pasifika population^ provided their personal opinions in online government transactions, compared to 19% of the Māori population^ and 9.9% of the Asian people^. However, NZ Europeans were the least likely to do so (6.3%) (p=0.001).

Figure 22: Types of information in online government transactions, by ethnicity group



^Confidence intervals: Health info (Māori 9.6%-49%; Pasifika 3.3%-73%; Asians 2.7%-35%); educational background (NZ European 14%-25%; Māori 36%-57%; Pasifika 6.1%-67%; Asians 11%-51%); things you do (Māori 4.3%-19%; Pasifika 1.7%-57%; Asians 2.4%-33%), social welfare number (Māori 17%-57%; Pasifika no data; Asians 0.6%-27%), community services card (Māori 17%-56%; Pasifika no data; Asians 2.1%-30%), personal opinions (Māori 9.9%-35%; Pasifika 16%-84%; Asians 2.4%-33%)

Why identity information is provided in online government transactions

The most important reasons for providing identity information in online government transactions varied for participants from different ethnic backgrounds^[58].

Māori^ (14%) were significantly more likely than non-Māori (2.8%) to share information with government agencies online in order to get a service adapted to their personal needs^. They^ also

[58] ^Confidence intervals: to comply with the law (Māori: 9.0%-25%; non-Māori: 24%-36%); to get a service adapted (Māori: 4.1%-38%); to ask a question (Māori: 4.0%-17%)

were more likely to do so in order to ask a question^ (8.6%), compared with non-Māori (2.8%). However, non-Māori^ (29%) were more likely to indicate compliance with the law^ as one of their most important reasons to share their identity information with government agencies in online transactions, than Māori^ (16%).

Across ethnic groups, the following differences around the most important reasons to disclose identity information in online government transactions could be observed (see Table 12).

Table 12: Reasons to provide information to Government agencies, by ethnicity group

	NZ Europeans	Māori	Pasifika	Asians	Sig
To be a good New Zealander*^	1.4	1.4	11.0	12.0	0.005
To get a service adapted to your personal needs*^	2.1	14.0	18.0	3.6	0.011
To engage with government*^	4.5	3.2	29.0	5.7	0.029

^Confidence intervals: good New Zealander (Pasifika 1.4%-50%; Asians 3.0%-38%), get a service adapted (Māori 4.1%-48%; Pasifika 2.6%-66%; Asians 0.5%-22%), engage with government (Māori 0.9%-11%; Pasifika 6.8%-69%; Asians 0.8%-32%)

Asians^ (12%) and Pasifika^ (11%) were more likely to disclose identity information in online government transactions for the reason of being a good New Zealander^. However, only few Māori (1.4%) and NZ Europeans (1.4%) indicated this particular reason.

Pasifika^ (18%) and Māori^ (14%) were more likely to provide identity information to government online in order to get a service adapted to their personal needs^, than Asians^ (3.6%) or NZ Europeans (2.1%).

Pasifika^ (29%) were much more likely to provide their identity information in order to engage with government online^, compared with Asians^ (5.7%), NZ Europeans (4.5%) or Māori^ (3.2%).

Sharing identity information as part of social networking

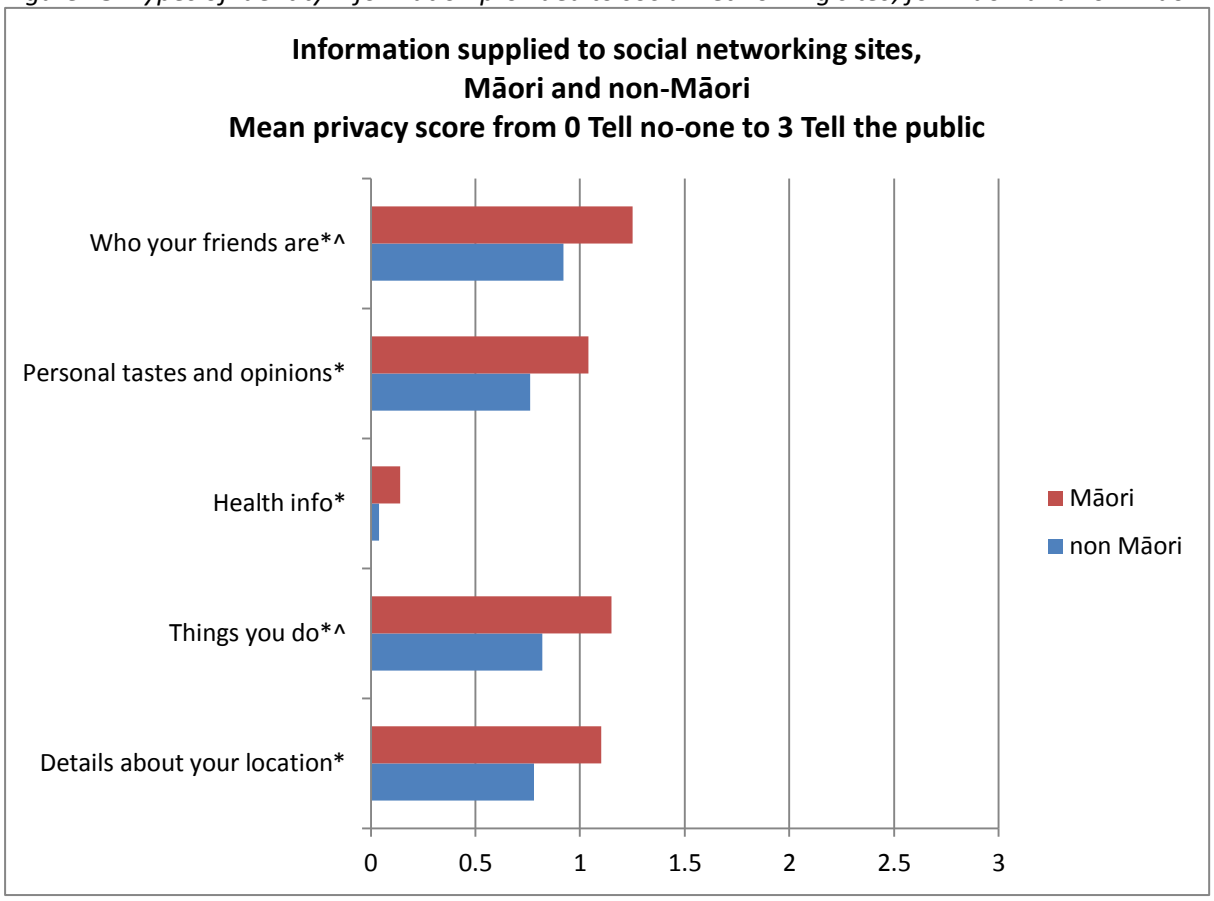
People from different ethnic backgrounds demonstrate varying identity information behaviours as part of social networking.

Māori^ are significantly more likely than non-Māori to disclose the following types of identity information on SNSs^[59] (see Figure 23):

- Things they do*^: 1.15^ (mean score), compared to 0.82 for non-Māori;
- Personal tastes and opinions*: 1.04 (mean score), compared to 0.76 for non-Māori;
- Who their friends are*^: 1.25^ (mean score), compared to 0.92 for non-Māori;
- Health Information*: 0.14 (mean score), compared to 0.04 for non-Māori; and
- Details about your location*: 1.10 (mean score) compared to 0.78 for non-Māori.

[59] ^Confidence intervals: Things you do (Māori: 0.89-1.41); who your friends are (Māori: 0.96-1.53)

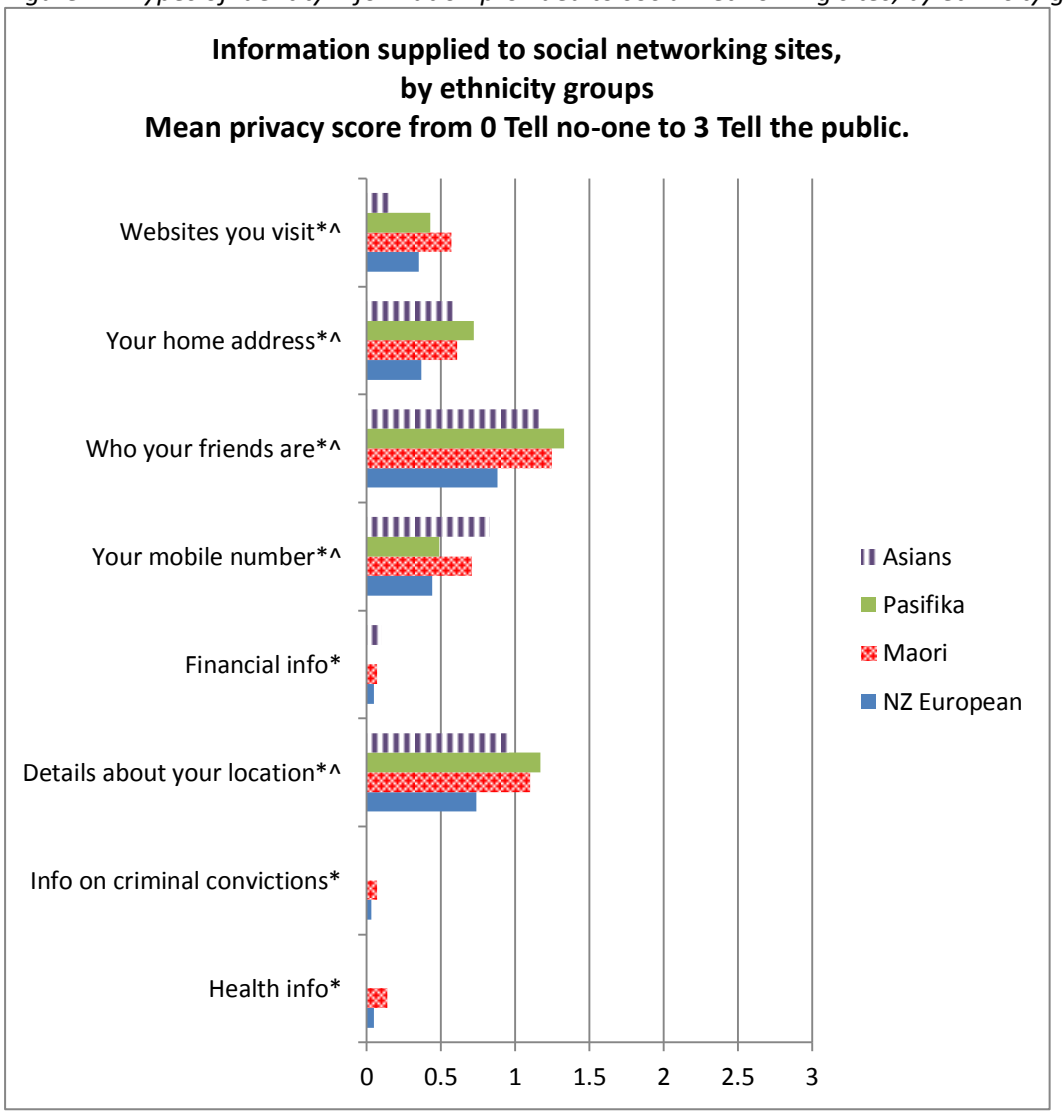
Figure 23: Types of identity information provided to social networking sites, for Maori and non-Maori



Across ethnic groups, the following differences in identity information behaviours could be observed (see Figure 24)

- Home address*^: NZ Europeans were the most private about their home address on SNSs, followed by Asians, Māori and Pasifika^ (p= 0.049);
- Mobile number*^: NZ Europeans were the most private about their mobile number on SNSs, followed by Pasifika^, Māori^ and Asians^ (p= 0.045);
- Who your friends are*^: NZ Europeans were the most private on SNSs about who their friends are, compared with other ethnic groups^ (p= 0.048);
- Details about your location*^: NZ Europeans were more private about their location details than other ethnic groups^ (p= 0.016);
- Financial information*: Pasifika were the most private about their financial information on SNSs and did not disclose this information at all. NZ Europeans, Māori and Asian people were slightly less private about their financial information on SNSs (p= 0.030);
- Health information*: Pasifika and Asian people were the most private on SNSs about their health information and did not disclose this information at all. NZ Europeans and Māori were slightly less private about their health information on SNSs (p= 0.000); and
- Information about any criminal convictions*: Pasifika and Asian people were the most private on SNSs with information about any criminal convictions and did not share this information at all. NZ Europeans and Māori were slightly less private about such information (p= 0.013).

Figure 24: Types of identity information provided to social networking sites, by ethnicity group



^Confidence intervals: home address (Pasifika .27-1.16), location details (Pasifika .64-1.71; Asians .67-1.25), mobile number (Māori .46-.97; Pasifika .17-.82; Asians .51-1.14), who your friends are (Māori .96-1.53; Pasifika .73-1.93; Asians .68-1.63), websites you visit (Māori .29-.85; Pasifika .03-.83)

Why identity information is provided on Social Networking Sites

People from different ethnic backgrounds also have varying reasons for disclosing their identity information on SNSs.

Non-Māori were significantly more likely to share identity information on social networking sites for fun (15%) than Māori (4.8%). Within this subpopulation of non-Māori, NZ Europeans indicated to share their identity information on SNSs for fun^[60] significantly more often (17%) than other ethnic groups^.

However, Māori were significantly more likely to share their information in order to get a discount (1.3%) compared with non-Māori (0.1%).

[60] Pasifika: no data

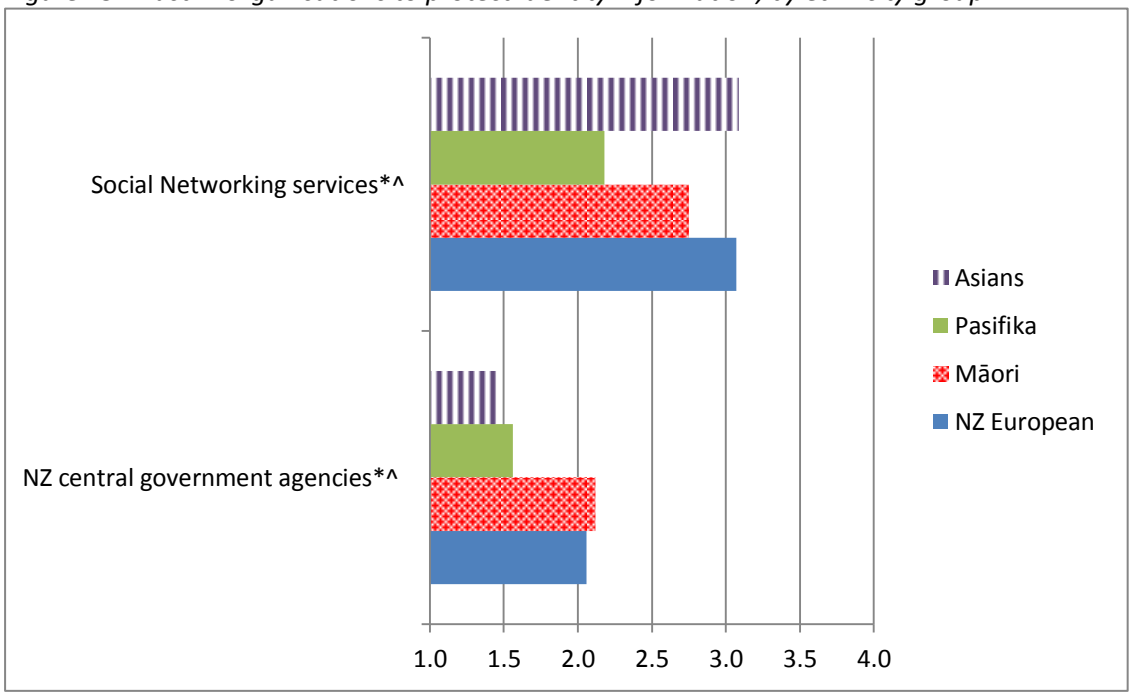
Trust in organisations to protect identity information

People from varying ethnic backgrounds demonstrate differences in trust of New Zealand central government agencies^ and Social Networking Services^ around the protection of their identity information.

Asians and Pasifika^ had higher trust in New Zealand central government agencies^ to protect their identity information, compared with NZ Europeans and Māori (see Figure 25);

Māori^ tended to trust Social Networking Services^[61] more than non-Māori. However, Pasifika^ had the highest trust in Social Networking Services^ to protect their identity information.

Figure 25: Trust in organisations to protect identity information, by ethnicity group



NZ central government (p=0.000); social networking sites (p=0.003)
^Confidence intervals: NZ central government (Pasifika 1.25-1.86), social networking sites (Māori 2.50-3.01; Pasifika 1.64-2.73; Asians 2.76-3.42)

User experiences with forms of cybercrime and cyber-enabled crime

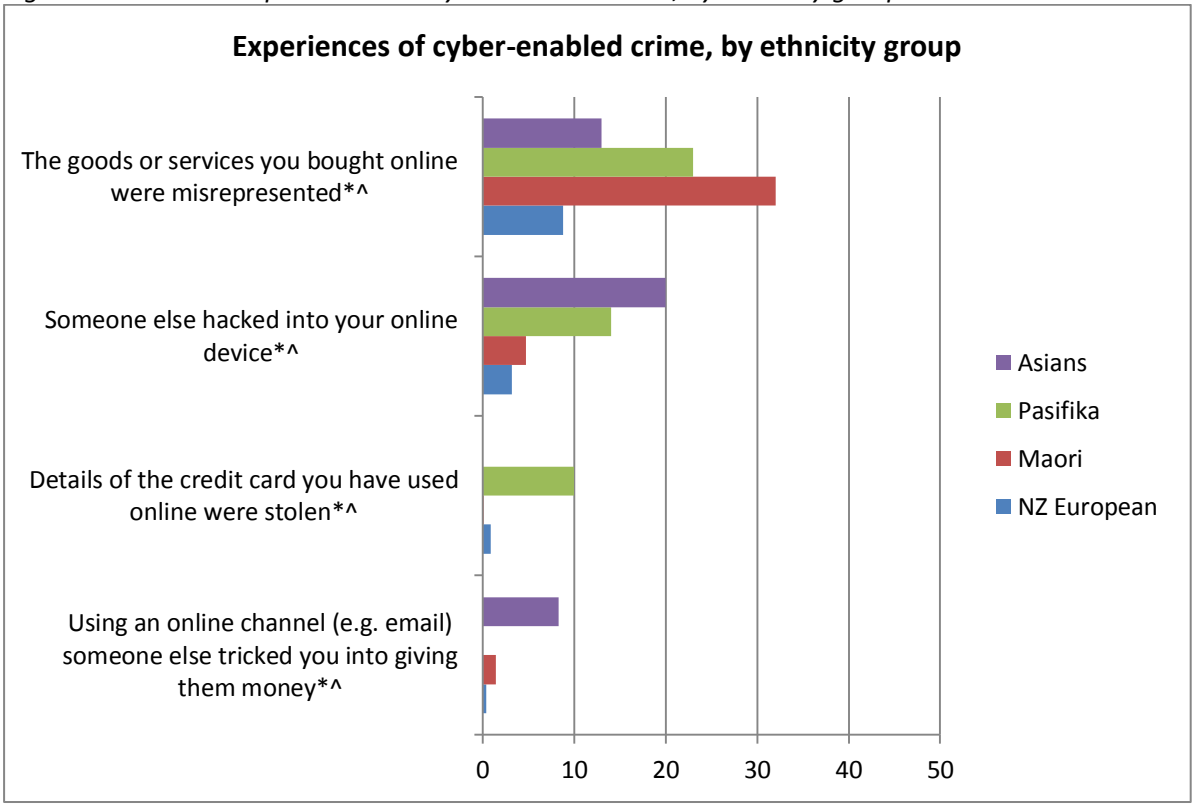
People from different ethnic backgrounds have had varying experiences with forms of cyber-enabled crime (see also Figure 26).

- Credit card details stolen*^: A larger proportion of Pasifika^ reported to have had the personal experience of stolen credit card details (10%), compared with other ethnic groups (p= 0.012);
- Someone else hacked into your online device*^: Significantly more Asians^ (20%) and Pasifika^ (14%) reported the personal experience of someone else hacking into their online device, compared with Māori^ (4.7%) and NZ Europeans (3.2%) (p= 0.004);
- Goods or services bought online were misrepresented*^: Significantly more Māori respondents^ (32%) and Pasifika^ (23%) reported the personal experience of misrepresented goods or services bought online, compared with Asians^ (13%) or NZ Europeans (8.8%) (p= 0.001);

[61] ^Confidence intervals: SNS (Māori: 2.50-3.01)

- Someone else tricked you into a romantic relationship*: Slightly more Māori respondents reported to have had the personal experience of being tricked into a romantic relationship (2.3%), compared with non-Māori participants (0.2%) (p=0.027); and
- Someone else tricked you into giving them money*^: Substantially more Asians^ (8.3%) reported the personal experience of someone else tricking them into giving money, compared with Māori (1.4%) and NZ European respondents (0.4%) (p=0.013).

Figure 26: Personal experience with cyber-enabled crime, by ethnicity group



^Confidence intervals: credit card details stolen (Pasifika 1.4%-48%; Asians no data), device was hacked (Māori 1.8%-12%; Pasifika 2.0%-58%; Asians 7.4%-43%), goods or services bought were misrepresented (Māori 18%-49%; Pasifika 5.9%-60%; Asians 4.0%-34%), tricked into giving money (Pasifika no data; Asians 1.1%-42%)

Income

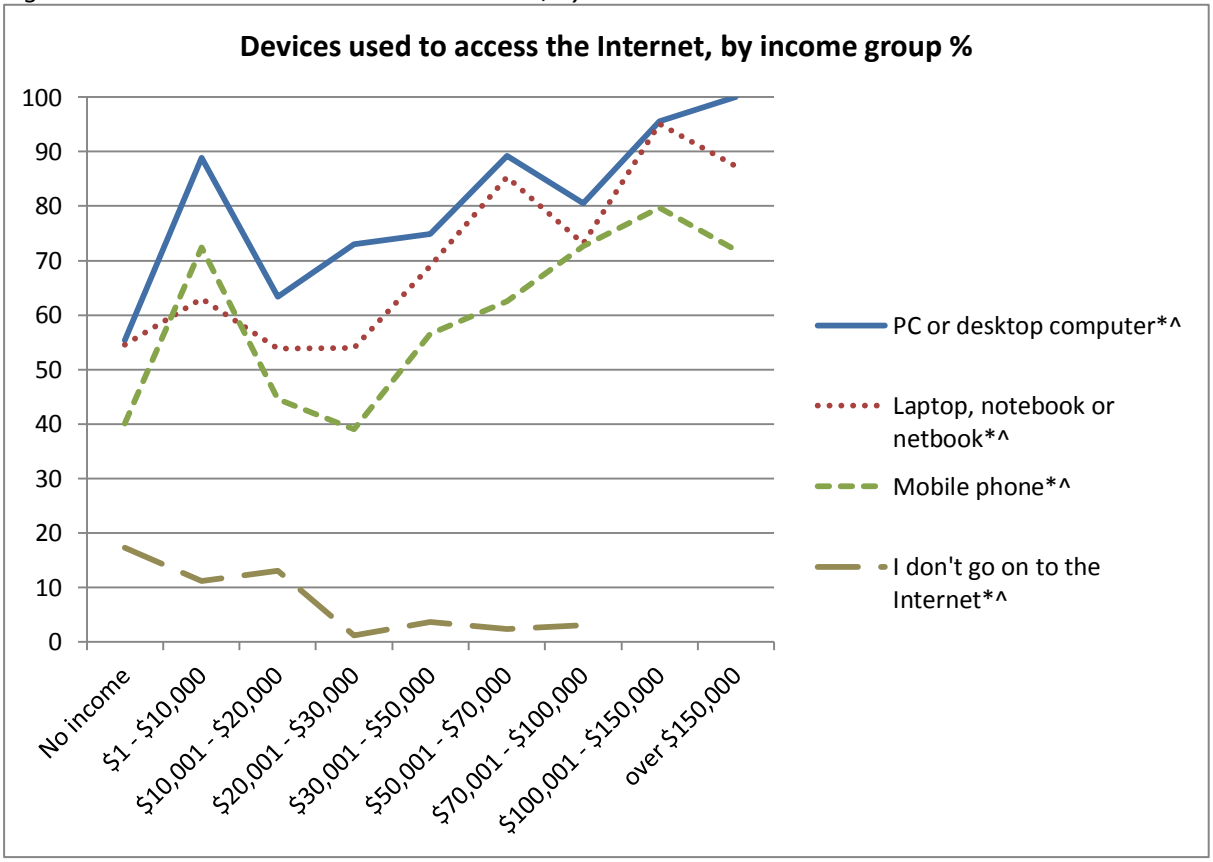
Using the internet

The proportion of people that used a PC^, laptop^ or mobile phone^ to go on to the Internet increases with income, with the exception of people with an income between $1-$10k^ (see Figure 27). A possible explanation for higher use of these devices by this income group is that it involves a relatively large number of individuals from the younger generations (e.g. students):

- PC or desktop*^: Only 55% of the respondents with no income^ and 63% of the respondents with an income between $10k - $20k^ used a PC or desktop computer in the last 12 months, compared to all respondents earning more than $150k using a PC or desktop computer.
- Laptop, notebook etc*^: The proportion of people that used a laptop or notebook to go on to the Internet is significantly higher amongst respondents with an income of more than $30k^.

- Mobile phone*^: With the exception of respondents earning a personal income of up to $10k^, a significantly smaller proportion of people belonging to the lower or no income groups^ used a mobile phone to go on to the Internet, compared to people with higher personal incomes^.
- I don't go on to the Internet*^: Most people who did not go on to the Internet in the last 12 months, belong to the low or no personal income groups^. These findings suggest that personal income has an impact on Internet use. A possible explanation could be that the costs of Internet use in New Zealand have an impact on the decision to use the Internet.

Figure 27: Devices used to access the Internet, by income



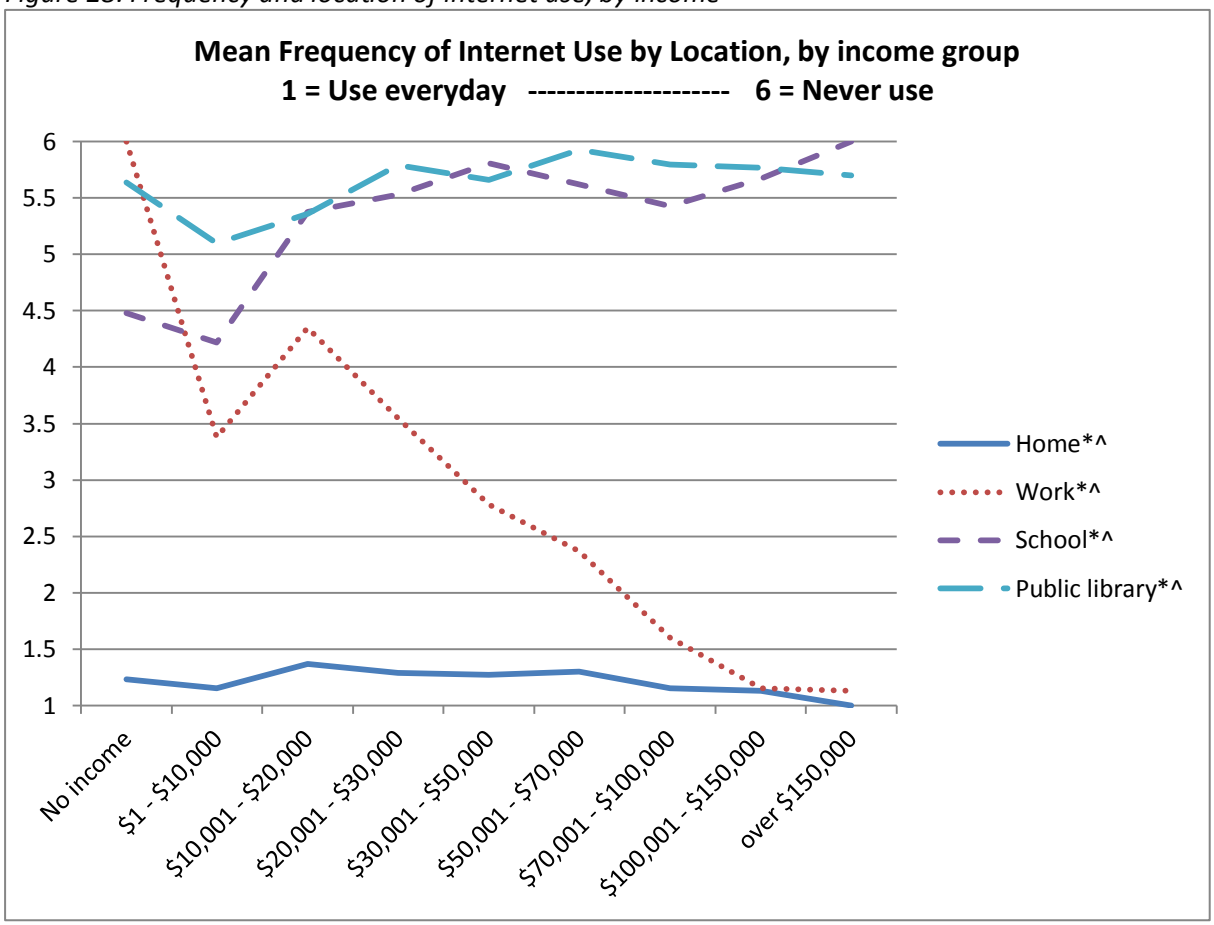
PC or desktop (p=.003; ^confidence intervals: $0: 29%-79%; $1-$10k: 64%-97%; $10k-$20k: 49%-76%; $20k-$30k: 58%-84%; $30k-$50k: 64%-83%; $50k-70k: 78%-95%; $70k-$100k: 66%-90%; $100k-$150k: 74%-99%*); laptop, notebook etc (p=.001: ^confidence intervals: $0: 28%-79%; $1-$10k: 40%-82%;* $10k-$20k: 40%-67%; $20k-$30k: 39%-69%; $30k-$50k: 60%-78%; $50k-70k: 75%-92%; $70k-$100k: 60%-84%; $100k-$150k: 72%-99%; $150k+: 46%-98% *); mobile phone (p=.005:^ confidence intervals: $0: 18%-67%; $1-$10k: 49%-88%;* $10k-$20k: 33%-57%; $20k-$30k: 25%-55%; $30k-$50k: 46%-67%; $50k-70k: 49%-74%; $70k-$100k: 57%-84%; $100k-$150k: 56%-92%; $150k+: 34%-93% *); I don't go on to the Internet (p=.015; ^confidence intervals: $0: 4.4%-49%; $1-$10k: 2.8%-36%;* $10k-$20k: 7.3%-22%; $70k-$100k:0.7%-12 %; $100k-$150k: no data; $150k+: no data*).*

People with the highest personal incomes used the Internet slightly more at home compared to others. People with the highest personal incomes^ also used the Internet almost every day at work, whilst respondents belonging to income groups of $70k and less^ used the Internet at work less frequently.

Respondents with no personal income^ or an income of up to $10k^ made more frequent use of the Internet at school^ compared to others^.

People hardly used the Internet at a public library^; those with a personal income of up to $10k^ used the Internet at a public library slightly more than others^.

Figure 28: Frequency and location of internet use, by income



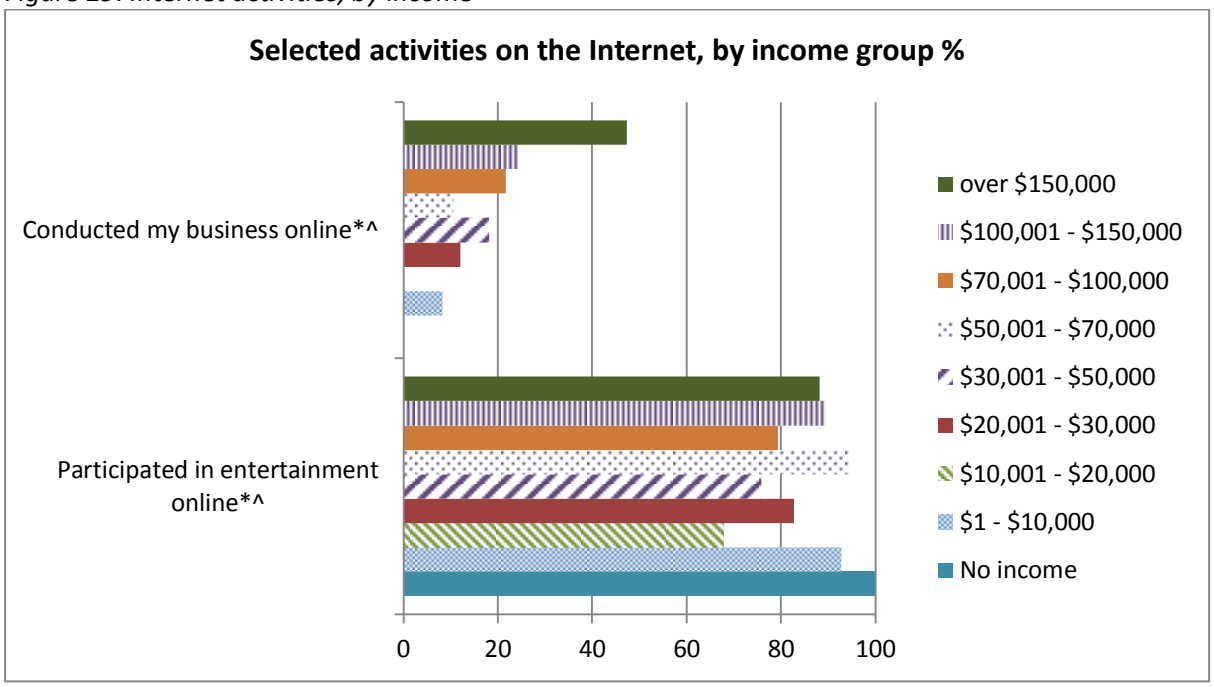
At home (p=.000: ^confidence intervals: $0:.79-1.67 ; At work (p=.000: ^confidence intervals: $1-$10k:.2.23-4.52 ; $10k-$20k: 3.73-4.95; $20k-$30k: 2.67-4.43; $30k-$50k: 2.24-3.33; $50k-70k: 1.78-2.95; $70k-$100k: 1.13-2.07; $100k-$150k: ..86-1.44*); at school (p=.000: ^confidence intervals: $0:.2.65-6.32; $1-$10k:.3.12-5.32 ;* $10k-$20k:4.69-6.06; $20k-$30k: 5.01-6.03; $50k-70k: 5.24-5.99; $70k-$100k: 4.82-6.03; $100k-$150k: 5.04-6.30*); public library (p=.002: ^confidence intervals: $0:.5.22-6.06 ; $1-$10k:4.35-5.85 ;* $10k-$20k: 5.05-5.67; $150k+:5.36-6.05*)*

Online activities in the last 12 months

Participation in online entertainment^ was high amongst all income groups^ (see Figure 29). However, respondents with no personal income participated significantly more (100%) in online entertainment compared to other income groups^, with people earning a personal income between $10k and $20k^ participating the least (68%).

People with higher incomes^ were more involved in conducting their business online^ than people from lower income groups. Respondents with a personal income of more than $150k^ were mostly involved in conducting their business online in the last 12 months (47%), followed by people belonging to personal income groups of $100k-$150k^ (24%) and $70k-$100k^ (22%).

Figure 29: Internet activities, by income

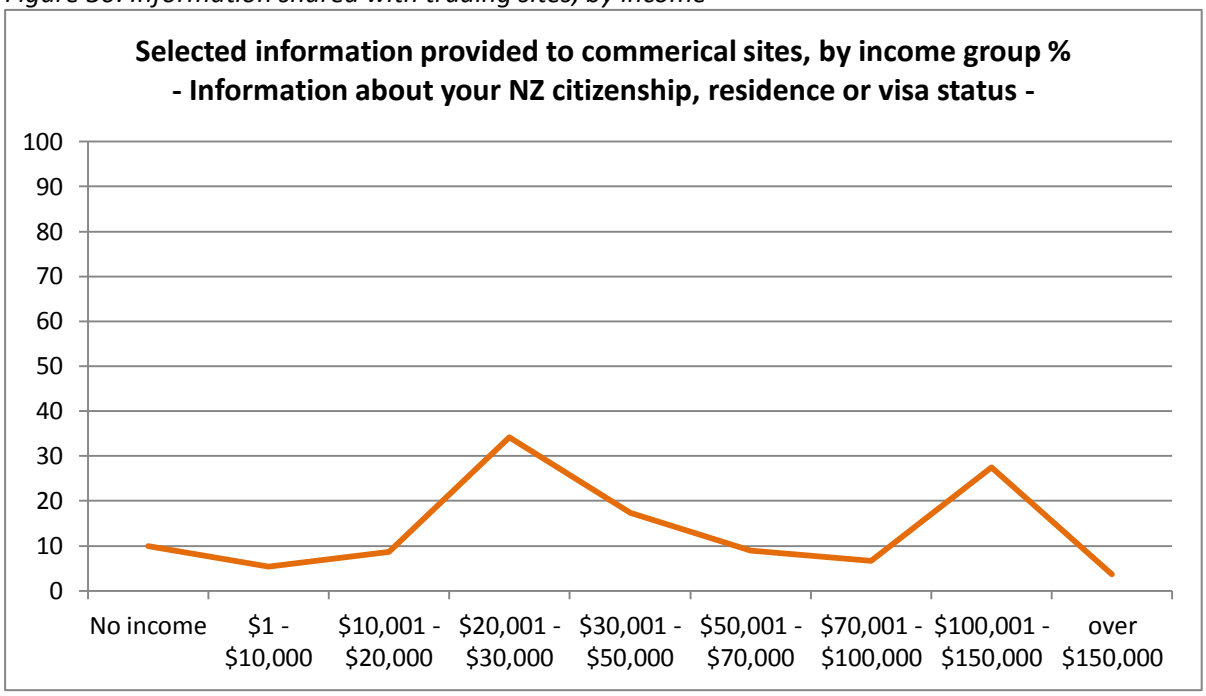


Participated in entertainment online (p=.027: ^confidence intervals: $1-$10k:63%-99% ; $10k-$20k:51%-81%; $20k-$30k:67%-92%; $30k-$50k: 65%-84%; $50k-70k: 85%-98%; $70k-$100k: 64%-89%; $100k-$150k: 66%-97%; $150k+: 47%-98%*); conducted my business online (p=.008: ^confidence intervals: $0:.no data ; $1-$10k:1.2%-41% ;* $10k-$20k: no data; $20k-$30k:4.6%-28%; $30k-$50k: 11%-29%; $50k-70k: 4.4%-23%; $70k-$100k: 11%-38%; $100k-$150k: 10%-48%; $150k+: 18%-79%*).*

Identity information provided in online commercial transactions

Compared to other personal income groups, a significantly larger proportion of people earning a personal income between $20k-$30k^ (34%), an income between $100k-$150k^ (28%), or an income between $30k-$50k^ (17%) shared personal information about their New Zealand citizenship, residency or visa status^ in online commercial activities in the last 12 months.

Figure 30: Information shared with trading sites, by income

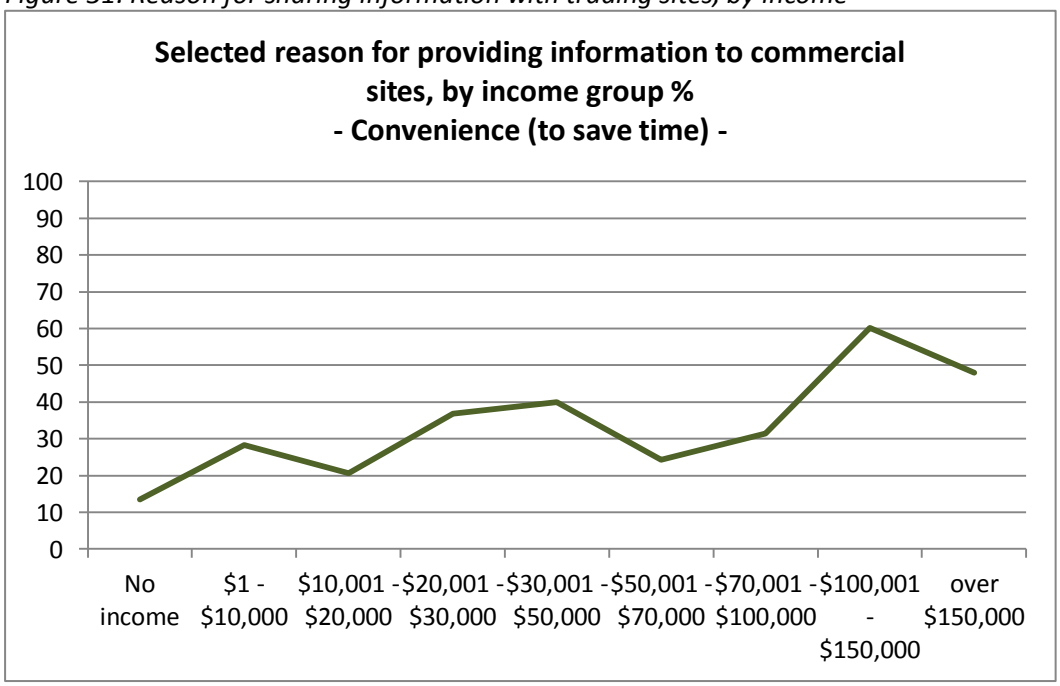


Information about NZ citizenship, residency or visa status (p=.008: ^confidence intervals: $0:.1.3%-48% ; $1-$10k:0.7%-31% ; $10k-$20k:3.1%-22%; $20k-$30k:20%-52%; $30k-$50k: 10%-28%; $50k-70k: 3.6%-21%; $70k-$100k: 1.7%-24%; $100k-$150k: 12%-52%; $150k+: 0.5%-24%*).*

Why identity information is provided in online commercial transactions

Respondents earning higher personal incomes^ indicated convenience^ more often as an important reason for providing identity information in online commercial activities than people belonging to lower income groups^.

Figure 31: Reason for sharing information with trading sites, by income



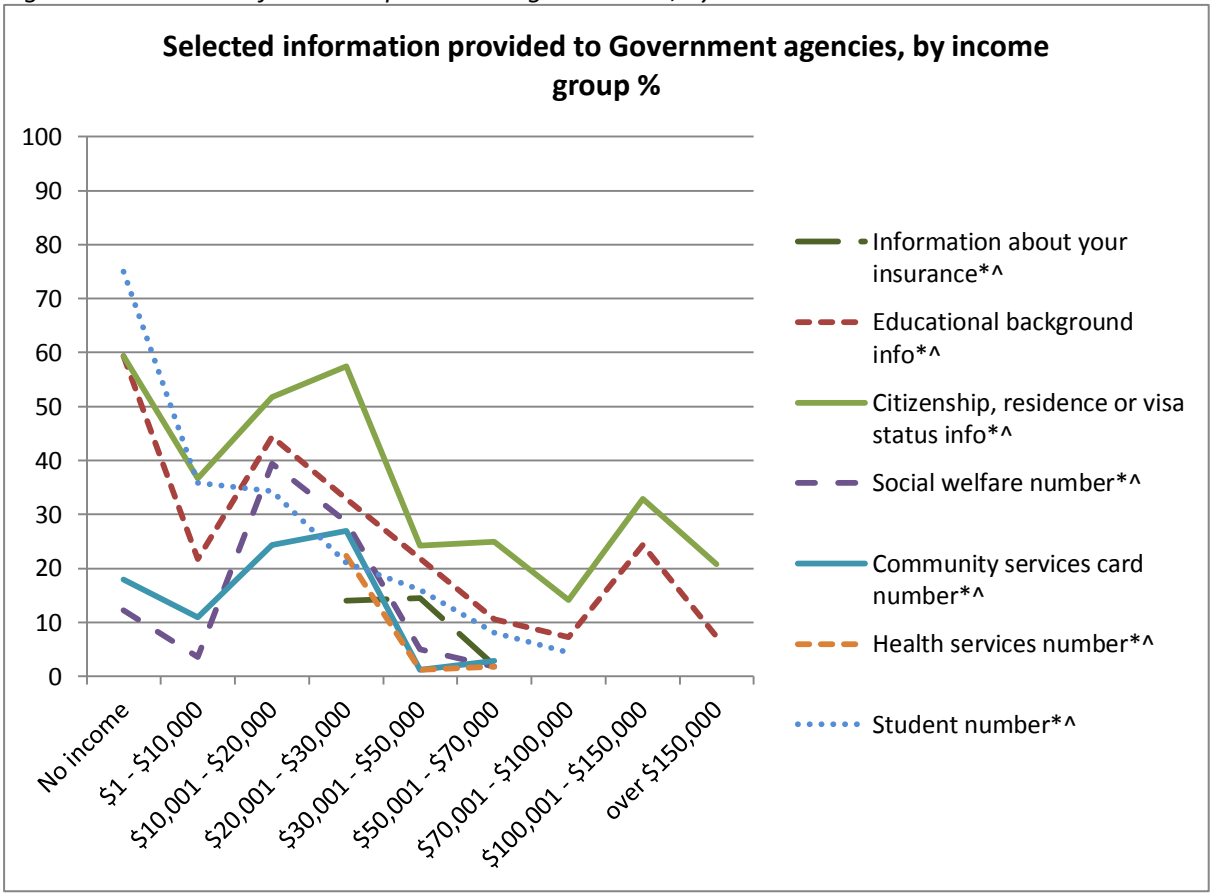
Convenience (p=.038: ^confidence intervals: $0:.3.2%-43% ; $1-$10k:12%-55% ; $10k-$20k:11%-35%; $20k-$30k: 23%-54%; $30k-$50k: 29%-52%; $50k-70k: 14%-58%; $70k-$100k: 19%-48%; $100k-$150k: 37%-79%; $150k+: 19%-79%*).*

Identity information provided in transactions with government online

People with no income and those from the lower income groups demonstrate different privacy behaviours around particular types of identity information in their online transactions with government, compared to those with a higher income (see Figure 32). In several cases, an exception can be observed for those belonging to the $0 to $10k income group:

- Insurance information*^: Respondents with no personal income^ (18%) more frequently shared their insurance information in online transactions with government, compared to people with an income^.
- Educational background information*^: A significantly larger proportion of respondents with no personal income^ (59%), an income between $10k-$20k^ (44%), or an income between $20k-$30k^ (33%), shared information about their educational background in online government transactions, compared with other income groups^.
- Information about NZ citizenship, residency or visa status*^: More than half of the people with no personal income^ (59.3%), an income between $10k-$20k^ (52%), or an income between $20k-$30k^ (57%), shared information about their New Zealand citizenship, residency or visa status in transactional relationships with government.
- Social welfare number*^: A significantly larger proportion of respondents earning a personal income between $10k-$20k^ (39%), an income between $20k-$30k^ (29%), or respondents with no personal income^ (12.2%) shared their social welfare number with government online.
- Community service card number*^: A significantly larger proportion of respondents earning a personal income of $30k or less^, or with no personal income^ (18%), shared their community service card number with government online.
- Health services number*^: A significantly larger proportion of respondents earning an income between $20k and $30k^ (22%) shared their health services number with government online.
- Student number*^: The large majority of respondents with no personal income^ (75%), but to a lesser extent also those with a personal income of up to $10k^ (36%), a personal income between $10k-$20k^ (34%), or an income between $20k-$30k^ (21%), shared their student number with government online.

Figure 32: Personal information provided to government, by income



Information about their insurance (p=.028: ^confidence intervals: $0:.2.3%-67% ; $1-$10k:no data ; $10k-$20k:no data; $20k-$30k: 5.4%-32%; $30k-$50k: 6.6%-29%; $70k-$100k: no data; $100k-$150k: 0.7%-29%; $150k+: no data*); educational background (p=.004: ^confidence intervals: $0:.20%-89% ; $1-$10k:8.1%-47% ;* $10k-$20k:27%-64%; $20k-$30k: 18%-53%; $30k-$50k: 12%-36%; $50k-70k: 4.5%-23%; $70k-$100k: 1.8%-25%; $100k-$150k: 9.4%-50%; $150k+: 0.9%-40%*); information about NZ citizenship, residency or visa status (p=.013:^confidence intervals: $0: 20%-89% ; $1-$10k:8.1%-47% ;* $10k-$20k:27%-64%; $20k-$30k: 18%-53%; $30k-$50k: 12%-36%; $50k-70k: 4.5%-23%; $70k-$100k: 1.8%-25%; $100k-$150k: 9.4%-50%; $150k+: 0.9%-40%*); social welfare number (p=.000: ^confidence intervals: $0: 1.6%-54 % ; $1-$10k:0.5%-24% ;* $10k-$20k:19%-64%; $20k-$30k: 15%-48%; $30k-$50k: 1.6%-15%; $50k-70k: 0.3%-12%; $70k-$100k: no data; $100k-$150k: no data; $150k+: no data*); community service card number (p=.000: ^confidence intervals: $0:.2.3%-67% ; $1-$10k:2.7%-35% ;* $10k-$20k:8.8%-52%; $20k-$30k: 14%-46%; $30k-$50k: 0.2%-8.3%; $50k-70k: 0.4%-18%; $70k-$100k: no data; $100k-$150k: no data; $150k+: no data*); health services number (p=.000: ^confidence intervals: $0: no data ; $1-$10k:0.7%-31% ;* $10k-$20k:no data %; $20k-$30k: 11%-40%; $30k-$50k: 0.2%-8.3%; $50k-70k: 0.3%-12%; $70k-$100k: no data; $100k-$150k: no data; $150k+: no data*); student number (p=.001: ^confidence intervals: $0: 26%-96% ; $1-$10k:16%-62% ;* $10k-$20k:16%-60%; $20k-$30k: 9.0%-42%; $30k-$50k: 7.8%-31%; $50k-70k: 2.6%-23%; $70k-$100k: 0.6%-25%; $100k-$150k: no data; $150k+: no data*).*

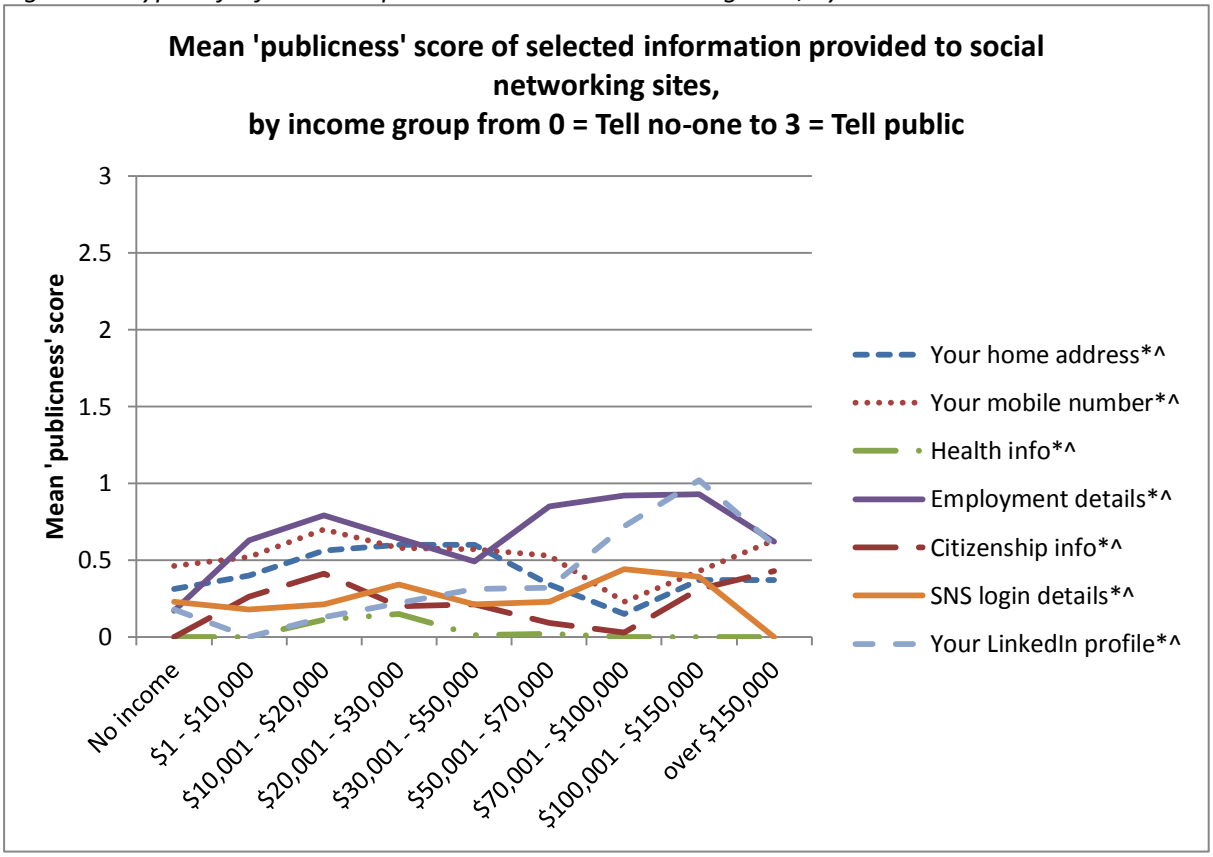
Sharing personal information as part of social networking

People from varying income groups demonstrate different privacy behaviours on social networking sites around the following types of identity information (see also Figure 33):

- Home address*^: Respondents with a personal income between $10k-$20k, an income between $20k-$30k^, or an income between $30k-$50k, shared their home address on SNSs slightly more than others and, if they did so, only with close friends.

- Mobile phone number*^: Respondents across all income groups^ and including people with no personal income^ had shared their mobile phone number via SNSs. However, they only shared this with close friends.
- Health information*: Only people with a personal income between $10k and $30k shared their health information on SNSs, and restricted to close friends.
- Employment details*^: Respondents with a personal income between $50k and $150k^, or those with a personal income between $10k-$20k^, shared their employment details on SNSs more than people belonging to other income groups.
- Information about NZ citizenship, residency or visa status*^: People from all income groups^ shared information about their New Zealand citizenship, residency or visa status on SNSs with close friends only, except for respondents with no personal income, who did not share any information at all.
- Personal SNS site account details*^: People from all income groups^ shared their personal SNS site account details on SNSs with close friends only, except for participants with a personal income of $150k or more, who did not share this information at all.
- LinkedIn profile*^: People with a personal income of $70k or more^ shared their LinkedIn profile on SNSs significantly more than respondents from other income groups.

Figure 33: Types of information provided on social networking sites, by income



Home address (p=.001: ^confidence intervals: $0: .00-.62; $1-$10k: .10-.71; $20k-$30k: .33-.87; $100k-$150k: .04-.69; $150k+: .04-.70*); Mobile phone number (p=.032: ^confidence intervals: $0:.12-.80; $1-$10k:.20-.83 ;* $20k-$30k:.30-.85; $50k-70k: .27-.78; $100k-$150k: .10-.79; $150k+: -.09-1.35*); health information (p=.009); employment details (p=.010: ^confidence intervals: $1-$10k:.22-1.04 ;* $10k-$20k: .29-1.29; $20k-$30k: .25-1.02; $50k-70k: .51-1.20; $70k-$100k: .54-1.30; $100k-$150k: ..36-1.50; $150k+: -.22-1.46*); information about NZ citizenship, residency or visa status (p=.011: ^confidence intervals: $1-$10k:.*-.02-.55 ; $10k-$20k: -.06-.88; $100k-$150k: -.10-.73; $150k+: -.37-1.24*); personal SNS site account details (p=.000: ^confidence intervals:* $20k-$30k: .07-.61; $70k-$100k: .14-.74; $100k-$150k: -.05-.83*); LinkedIn profile (p=.000: ^confidence intervals:* $50k-70k: .05-.58; $70k-$100k: .33-1.11; $100k-$150k: .39-1.65; $150k+: -.16-1.36*)*

Why identity information is provided on Social Networking Sites

A substantial number of respondents with a personal income of up to $10k^ (26%), those with a personal income between $100k- $150k^ (20%), or those with an income of more than $150k^ (18%), indicated that it didn't bother them^[62] to provide personal information on SNSs. To a lesser extent, participants with an income between $70k- $100k^ (10%), those with an income between $50k- $70k^ (3.9%), those with an income between $10k and $20k^ (3.7%), and those with an income between $30k-$50k (1.2%), also indicated that it didn't bother them to share their identity information on SNSs.

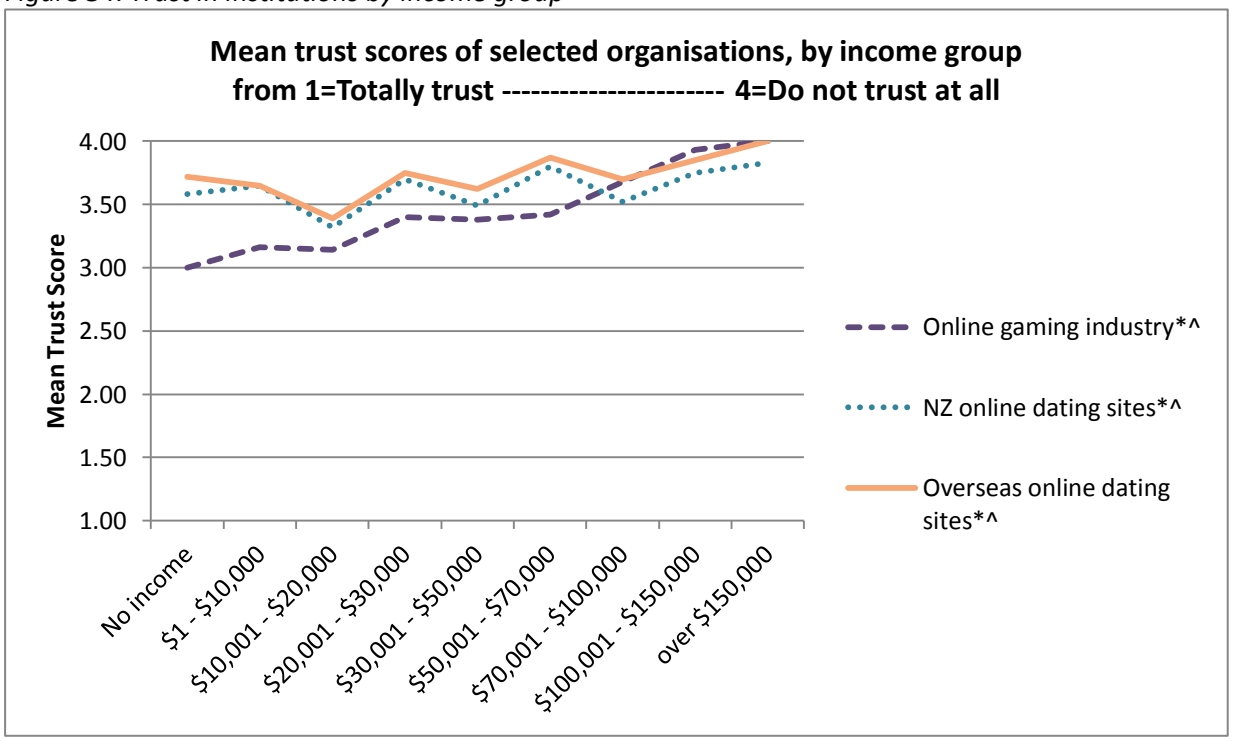
Trust in organisations to protect identity information

Personal income had an impact on the extent to which people trusted the protection of their identity information by the online gaming industry^, New Zealand-based online dating sites^ and overseas online dating sites^ (see Figure 34).

The higher the personal income, the more people were distrustful of the protection of their personal information by the online gaming industry^.

Respondents across all personal income groups tended not to trust online dating sites^ around the protection of their personal information, or did not trust them at all. The geographical location of these online dating sites did not seem to have an influence on the trust levels of respondents.

Figure 34: Trust in institutions by income group



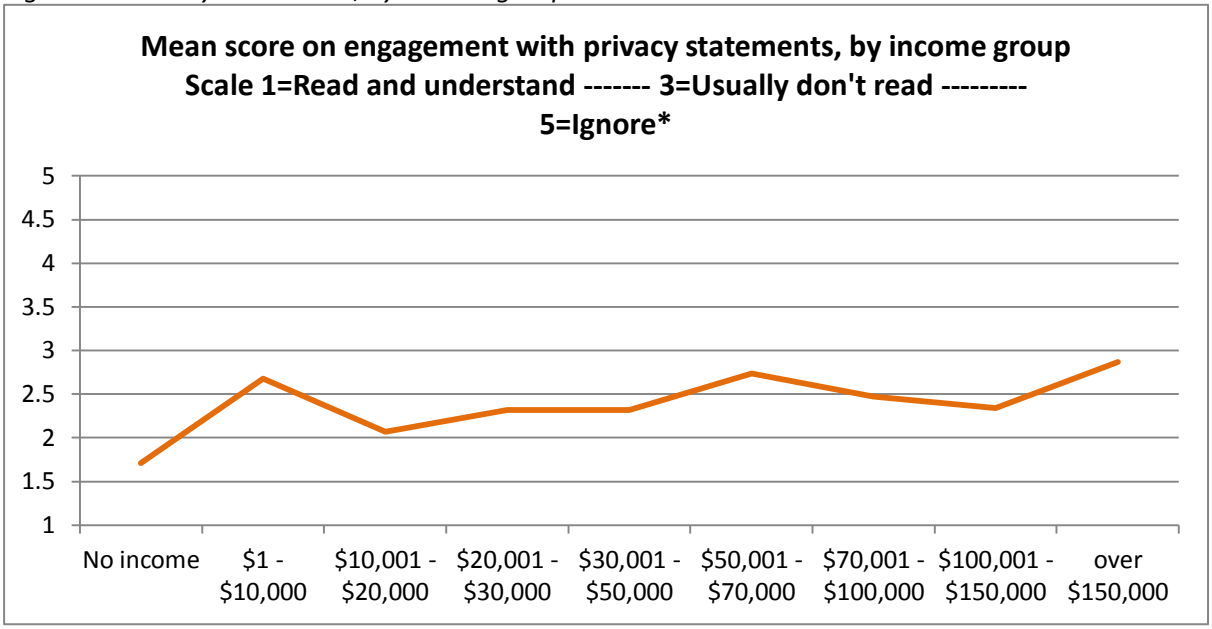
Online gaming industry (p=.000: ^confidence intervals: $0: 2.40-3.61 ; $1-$10k: 2.69-3.62 *;* $10k-$20k: 2.91-3.38; $20k-$30k: 3.05-3.75; $50k-70k: 3.16-3.69); *online dating sites in NZ (p=.029: ^confidence intervals: $0: 3.19-3.97 ; $1-$10k*: 3.39-3.92 *;* $70k-$100k: 3.23-3.81; $100k-$150k: 3.50-4.00; $150k+: 3.53-4.14 *); online dating sites overseas (p=.000: ^confidence intervals: $0:* 3.38-4.07 *; $1-$10k*: 3.39-3.92*).*

[62] *p=.004; ^confidence intervals: $0: no data ; $1-$10k: 9.3%-54% ;* $10k-$20k:0.9%-14%; $20k-$30k: 0.8%-15%; $50k-70k: 0.9%-16%; $70k-$100k: 3.3%-28%; $100k-$150k:7.2%-43%; $150k+: 2.5%-66%

Privacy statements

Most respondents across all income groups^ usually read privacy statements^ but do not fully understand them (see Figure 3). Respondents with a personal income of $150k or more^ are most likely not to read them.

Figure 35: Privacy statements, by income group

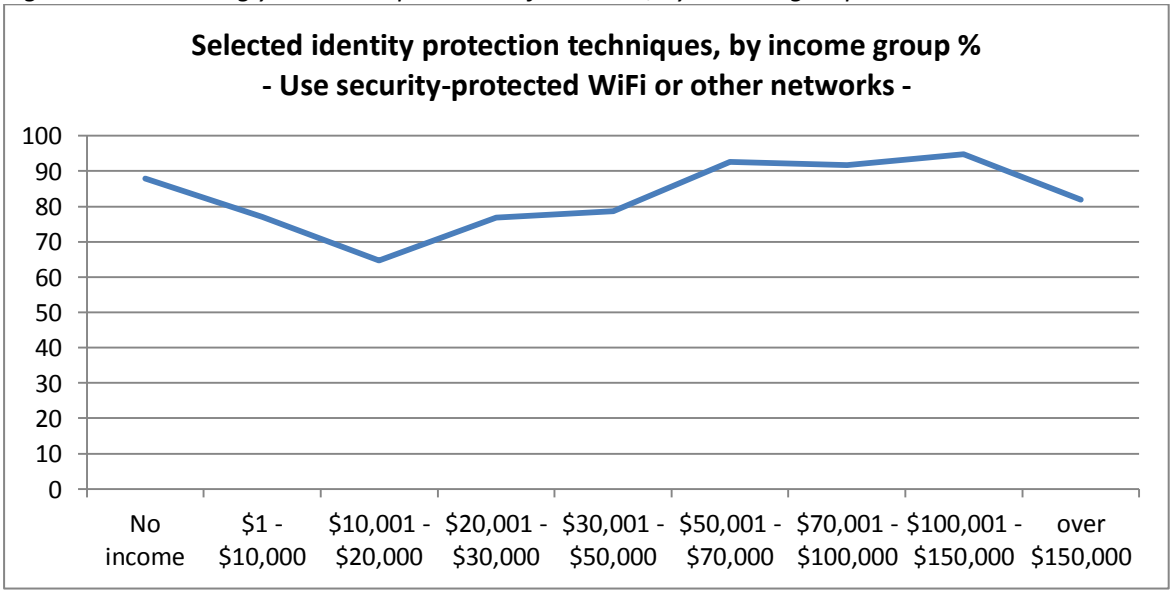


(p=.017: ^confidence intervals: $0: 1.16-2.25 ; $1-$10k: 2.33-3.03 ; $10k-$20k: 1.74-2.40; $20k-$30k: 1.99-2.66; $50k-70k: 2.42-3.06; $70k-$100k: 2.10-2.84; $100k-$150k: 1.96-2.72; $150k+: 2.04-3.70*).*

Steps taken to protect online identity information

A larger proportion of people with a personal income between $50k and $150k^ use security-protected WiFi, compared with other income groups (see Figure 36). Respondents with a personal income between $10k-$20k^ use security-protected WiFi substantially less than other income groups (only 65%).

Figure 36: Protecting your online personal information, by income group



Use security-protected WiFi or other networks (p=.020: ^confidence intervals: $0: 48%-98% ; $1-$10k: 51%-91% *;* $10k-$20k: 47%-79%; $20k-$30k: 59%-89%; $30k-$50k: 67%-87%; $50k-70k: 82%-98%; $70k-$100k: 79%-97%; $100k-$150k: 71%-99%; $150k+: 35%-95%*).*

Education

Using the Internet

The higher the level of educational achievement, the more likely people have used a PC^, laptop^ or mobile phone^ to access the Internet in the last 12 months (see Figure 37).

The higher the level of educational achievement, the more respondents had used a PC or desktop computer^ to go on to the Internet in the last 12 months: PC use differed from 62% of respondents not having had any education^ to 84% of respondents who have completed some form of tertiary education.

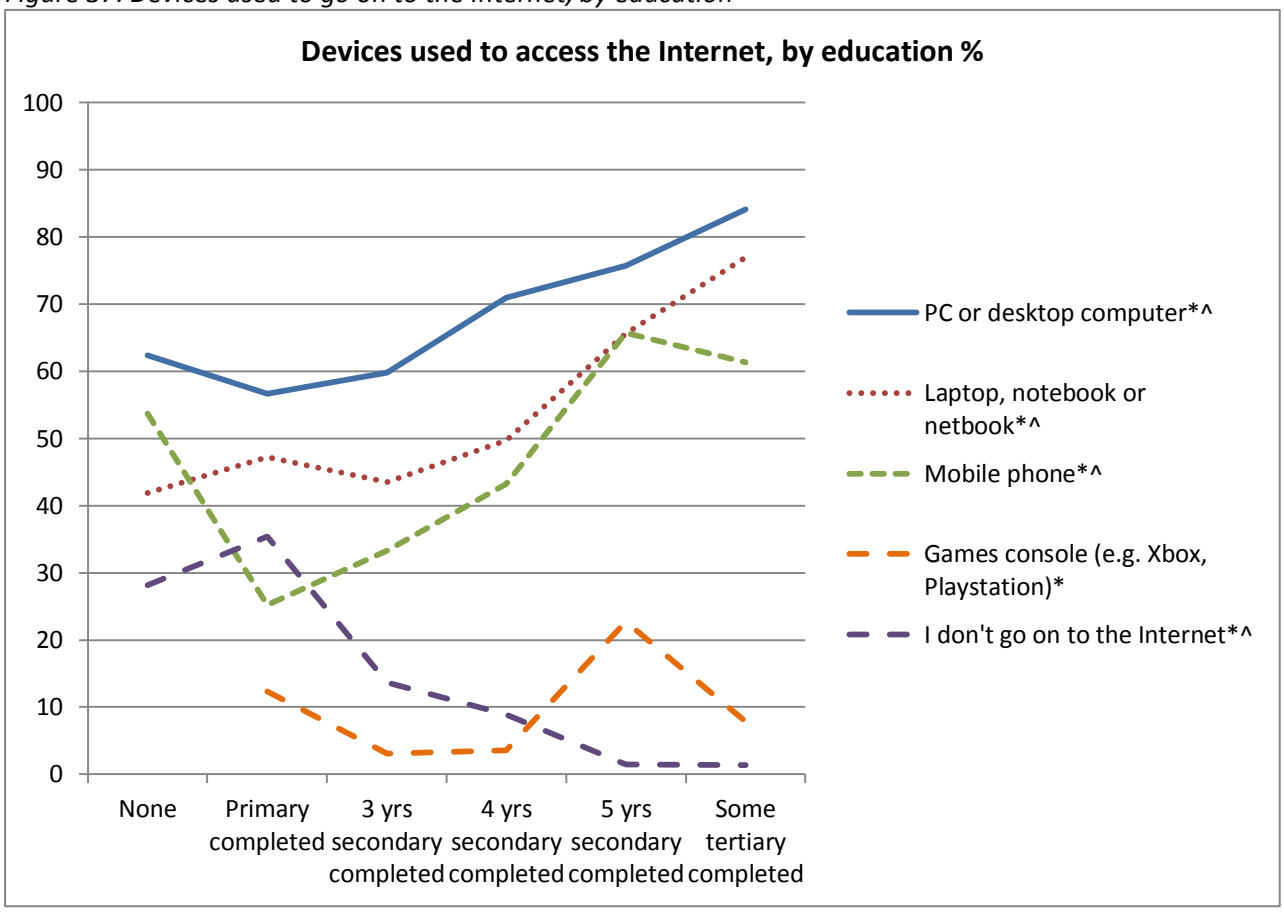
A laptop, notebook or netbook^ was significantly used more by people who have completed some form of tertiary education (77%) and those who have completed at least 5 years of secondary school^ (66%). People without any level of educational achievement^ were the least likely of all educational groups to have used a laptop, notebook or netbook in the last 12 months (42%).

Mobile phones^ had been used mostly by respondents who have completed 5 years at secondary school^ (66%), followed by respondents who have completed some form of tertiary education^ (61%) and people without any level of educational achievement^ (54%). Other education groups^ had used a mobile phone to go on to the Internet to a lesser extent in the last 12 months: 43% of respondents who have completed 4 years at secondary school^, 33% of respondents who have completed 3 years at secondary school^ and 25% of respondents who have completed primary school^.

People who have completed 5 years at secondary school^ had used a game console^ much more than respondents with other education backgrounds^.

Respondents who have completed primary school^ (35%) and those without any level of educational achievement^ (28%) substantially more often indicated that they don't go on to the Internet^, compared to people with a higher level of educational achievement^; only 1.4% of respondents who have completed some form of tertiary education indicated that they don't go on to the Internet^. These findings suggest that educational background has an impact on Internet use.

Figure 37: Devices used to go on to the Internet, by education



PC or desktop computer (p=.002: ^confidence intervals: none:28%-88%; primary: 35%-76%; 3yrs secondary: 45%-73%; 4yrs secondary: 56%-83%; 5yrs secondary: 55%-89%); laptop, notebook or netbook (p=.000: ^confidence intervals: none: 13%-78%; primary: 26%-70%; 3yrs secondary: 30%-58%; 4yrs secondary: 35%-64%; 5yrs secondary: 46%-81%); mobile phone (p=.000: ^confidence intervals: none:21%-84%; primary: 10%-50%; 3yrs secondary: 21%-48%; 4yrs secondary: 29%-58%; 5yrs secondary: 50%-78%; some tertiary: 55%-67%); games console (p=.029: ^confidence intervals: none: no data; primary: 3.1%-38%; 3yrs secondary: 0.4%-19%; 4yrs secondary: 0.5%-22%; 5yrs secondary: 12%-38%); I don't go on to the Internet (p=.000: ^confidence intervals: none:8.0%-64%; primary: 18%-58%; 3yrs secondary: 6.7%-26%; 4yrs secondary: 3.4%-21%)

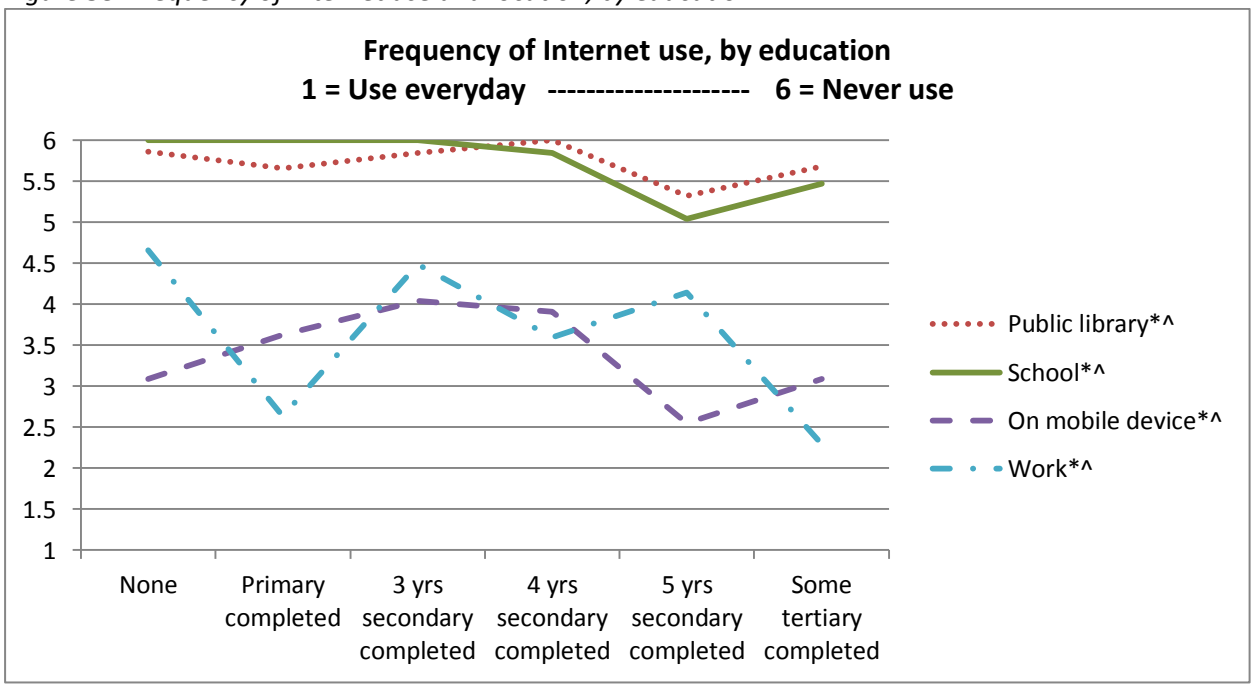
People who have completed 5 years at secondary school^ and those who have completed some form of tertiary education, are more likely to have used the Internet at school^, compared to people with lower levels of educational achievement (see Figure 38).

Respondents from different educational backgrounds^ rarely used the Internet at a public library^, with those who have completed 4 years at secondary school indicating that they never had used the Internet at a public library.

Respondents who have completed some form of tertiary education and those who have completed primary school^ had used the Internet at work^ much more often and at least on a weekly basis, compared to respondents from other education backgrounds^.

Respondents who have completed at least 5 years at secondary school^ and people without any level of educational achievement^ had used a mobile device^ to go onto the Internet more often than people with other levels of educational achievement.

Figure 38: Frequency of Internet use and location, by education



Used the Internet at work (p=.000: ^confidence intervals: none:2.83-6.49; primary: 1.27-4.02; 3yrs secondary: 3.61-5.38; 4yrs secondary: 2.72-4.48; 5yrs secondary: 3.37-4.91); Used the Internet at school (p=.000: ^confidence intervals: 4yrs secondary: 5.57-6.14; 5yrs secondary: 4.23-5.85); used the Internet at a public library (p=.000: ^confidence intervals: none: 5.59-6.14; primary: 5.30-6.02; 5yrs secondary: 4.92-5.72); on a mobile device (p=.033: ^confidence intervals: none: .85-5.33; primary: 2.25-5.01; 3yrs secondary: 3.25-4.84; 4yrs secondary: 3.15-4.65; 5yrs secondary: 1.87-3.23; some tertiary: 2.81-3.37).

Online activities in the last 12 months

People from varying educational backgrounds demonstrate different behaviours with regard to their online activities in the last 12 months (see Figure 39).

People who have completed at least 4 years at secondary school^ had much more purchased commercial products or services online^ in the last 12 months, compared to people with lower levels of educational achievement^ or no education^.

The majority of the respondents who have completed at least 4 years at secondary school^ had transacted with government online^ in the last 12 months, with people who have completed some form of tertiary education^ being the highest users of all education groups (77%). There was significantly less usage of online government transactions by people with 3 years at secondary school^ or lower levels of educational achievement^, and those with no education^.

Participants who have completed some form of tertiary education^ also had participated in online public consultations from government agencies^ substantially more (22%) than people with other levels of educational achievement^, with the exception of respondents with no education^, who had participated in online public consultations the most (24%).

People with a primary school background^ were the highest users of online education (60%), followed by those with no educational background^ (45%) and those with a tertiary education background^ (44%). Those with 5 years of secondary schooling^ (33%), 3 years of secondary schooling^ (13%) or 4 years of secondary schooling^ (6.5%) had much less participated in online education activities in the last 12 months.

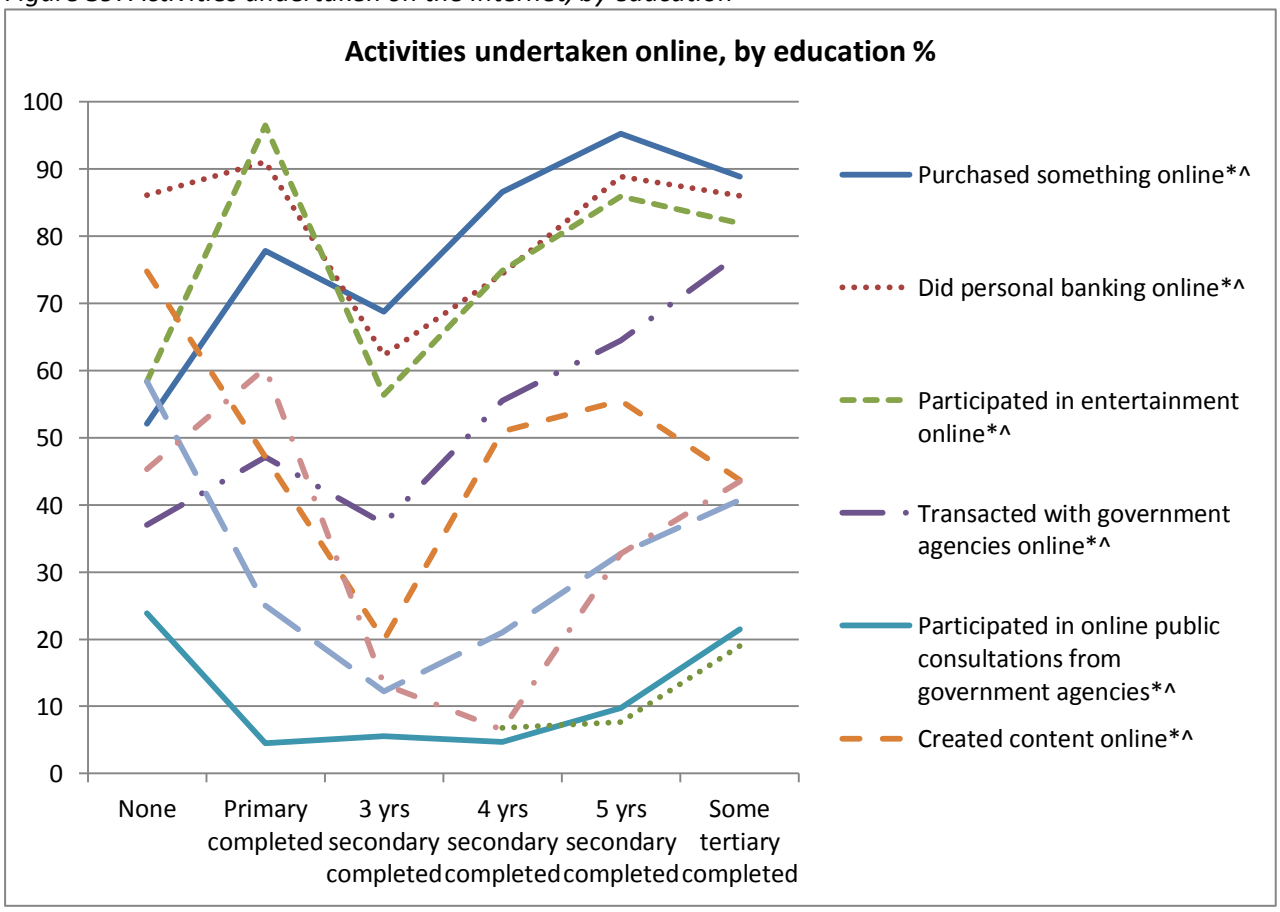
Compared with people who have an educational background, the large majority of respondents with no educational background^ had engaged in the creation of content online^ in the last 12 months (75%). People with 3 years of secondary schooling^ had created content online the least of all education groups (20%).

More than half of the respondents with no educational background^ had stored information online^ in the last 12 months (58%), followed by respondents with a tertiary education background^ (41%). Respondents with 3 years of secondary schooling^ were the least likely of all respondents to have stored information online (12%).

People with a primary school background^ were the highest users of online entertainment^ (97%), followed by people with 5 years of secondary schooling^ (86%) and people with a tertiary education background (82%). The lowest users were people with 3 years of secondary schooling^ (56%).

Particularly people with a primary school background^ (28%), but also people with some form of tertiary education^ (19%) had been engaged in conducting a business online in the last 12 months.

Figure 39: Activities undertaken on the Internet, by education



Purchased something online (p=.003: ^confidence intervals: none:11%-90%; primary: 45%-94%; 3yrs secondary: 52%-82%; 4yrs secondary: 71%-95%; 5yrs secondary: 83%-99%); transacted with government online (p=.000:

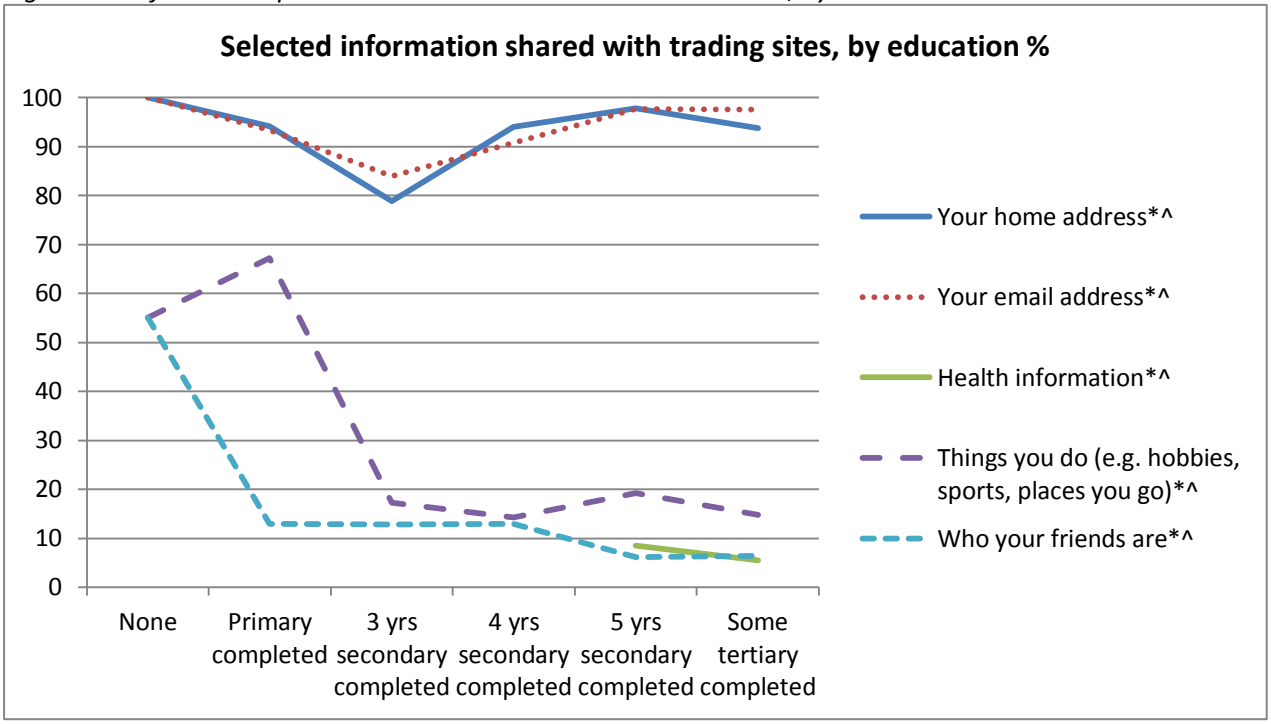
^confidence intervals: none: 5.4%-86%; primary: 21%-75%; 3yrs secondary: 23%-54%; 4yrs secondary: 38%-72%; 5yrs secondary: 48%-79%; some tertiary: 71%-82%); participated in online public consultations from government (p=.027: ^confidence intervals: none:2.6%-79%; primary: 0.6%-27%; 3yrs secondary: 1.7%-17%; 4yrs secondary: 0.6%-27%; 5yrs secondary: 3.0%-28%; some tertiary: 16%-28%); personal banking online (p=.005: ^confidence intervals: none:38%-98%; primary: 57%-99%; 3yrs secondary: 46%-76%; 4yrs secondary: 57%-87%; 5yrs secondary: 75%-96%); participation in education online (p=.001: ^confidence intervals: none:10%-86%; primary: 30%-85%; 3yrs secondary: 5.3%-30%; 4yrs secondary: 1.4%-26%; 5yrs secondary: 45%-84%; some tertiary: 37%-50%); created content online (p=.025: ^confidence intervals: none:32%-95%; primary: 21%-75%; 3yrs secondary: 10%-36%; 4yrs secondary: 34%-68%; 5yrs secondary: 39%-71%; some tertiary: 37%-50%); entertainment online (p=.021: ^confidence intervals: none:17%-91%; primary: 78%-100%; 3yrs secondary: 40%-72%; 4yrs secondary: 58%-87%; 5yrs secondary: 61%-96%); stored information online (p=.020: ^confidence intervals: none: 17%-91%; primary: 7.2%-59%; 3yrs secondary:5.0%-27 %; 4yrs secondary:9.7%-40%; 5yrs secondary: 16%-55%; some tertiary: 34%-47%); conducted my business online (p=.022: ^confidence intervals: none: no data; primary:8.3%-62%; 3yrs secondary: no data; 4yrs secondary: 1.7%-24%; 5yrs secondary: 2.4%-23%; some tertiary: 14%-25%).

Identity information provided in online commercial transactions

People from varying educational backgrounds demonstrate some differences in identity information behaviour in online commercial transactions. The following types of identity information were shared differently by varying educational groups (see Figure 40):

- Home address*^: People with 3 years of secondary schooling^ were the most private in online commercial activities about their home address (79%);
- Email address*^: People with 3 years of secondary schooling^ also did not disclose their email address in online commercial activities (84%) as much as other respondents^;
- Health information*^: People with no schooling background^ were more likely to provide their health information in online commercial activities (55%) than others^;
- Things you do*^: People who had completed primary school^ (67%) or those with no education^ (55%) were significantly more likely to provide information about things they do in online commercial transactions than people with higher levels of educational achievement; and
- Who your friends are*^: People with no education^ were significantly more likely to provide information about who their friends are in online commercial transactions (55%) than people with some level of educational achievement^.

Figure 40: Information provided in online commercial transactions, by education



Home address (p=.040: ^confidence intervals: primary:66%-99%; 3yrs secondary:61%-90%; 4yrs secondary: 79%-99%; 5yrs secondary: 86%-100%); email address (p=.009: ^confidence intervals: primary:64%-99%; 3yrs secondary:67%-93%; 4yrs secondary: 75%-97%; 5yrs secondary: 86%-100%); health information (p=.002: ^confidence intervals: none:10%-93%; primary: no data; 3yrs secondary: 0.2%-11%; 4yrs secondary: no data; 5yrs secondary: 2.6%-24%); things you do (p=.008: ^confidence intervals: none:10%-93%; primary:31%-90%; 3yrs secondary:7.3%-36%; 4yrs secondary: 5.2%-33%; 5yrs secondary: 9.6%-35%); who your friends are (p=.049: ^confidence intervals: none:10%-93%; primary:1.8%-56%; 3yrs secondary:4.2%-33%; 4yrs secondary: 4.6%-32%; 5yrs secondary: 1.9%-18%).

Why identity information is provided in online commercial transactions

People with no education^, those who have completed primary school^ and those who have completed 3 years of secondary education^, indicate different reasons for providing identity information in online commercial transactions^[63], compared to people with higher levels of educational achievement^. The following differences could be observed:

People with no education^ were significantly more likely to respond that they had provided identity information in online commercial activities in order to get a personalised service (22%), than people with some level of educational achievement^.

Respondents who had completed primary school^ (18%) or those who had completed 3 years at secondary school^ (10%) indicated significantly more than people with higher educational achievements^ to provide identity information in online commercial activities for fun^.

[63] *To get a personalised service (p=.043: ^confidence intervals: none:2.3%-78%; primary:3.4%-46%; 3yrs; 4yrs secondary: 5.3%-32%; 5yrs secondary: 5.4%-25%). for fun (p=.001: ^confidence intervals: none: no data; primary:2.7%-65%; 3yrs secondary: 3.2%-27%; 4yrs secondary: no data; 5yrs secondary: 0.8%-14%); to ask a question (p=.031: confidence intervals: none:2.3%-78%; primary: no data%; 3yrs secondary:4.2%-28%; 4yrs secondary: 6.2%-34%; 5yrs secondary: no data)*

People with no schooling background^ (22%), those with 4 years of secondary schooling^ (16%), those with 3 years of secondary schooling^ (12%) and those with some form of tertiary education background (4.7%) indicated to provide identity information in online commercial activities in order to ask a question^.

Identity information provided in transactions with government online

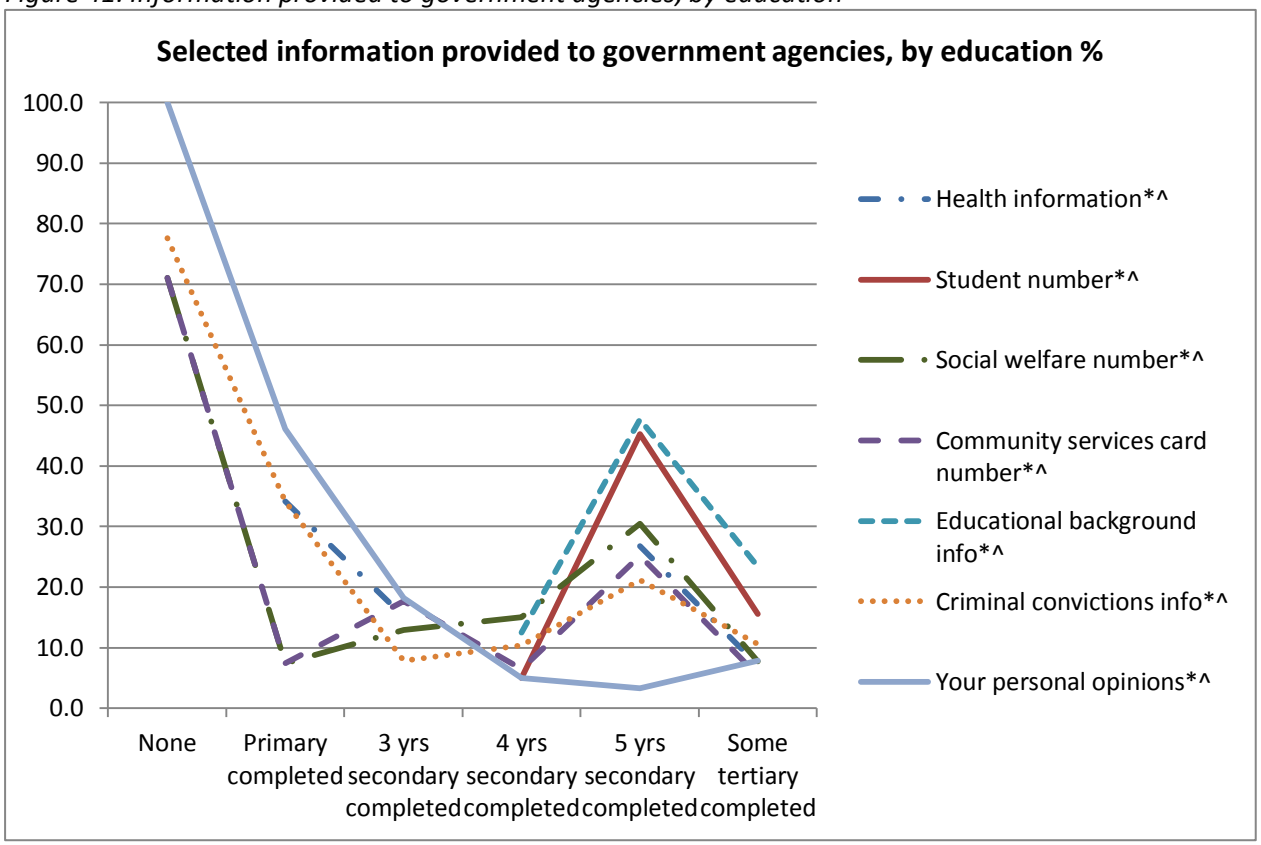
People from varying educational backgrounds demonstrate different identity information behaviours in online transactions with government (see Figure 41). The following differences could be observed:

- Health information*^: Respondents who had completed primary school^ (34%) and those with 5 years of secondary schooling^ (27%) had mostly provided health information in online transactions with government, followed by people with 3 years of secondary schooling^ (15%) and those with some form of tertiary education (7.1%);
- Educational background*^: Respondents with 5 years of secondary schooling^ (48%) and those with some form of tertiary education^ (23%) had much more provided educational background information in online government transactions, compared to people with lower levels of education^;
- Student number*^: Respondents with 5 years of secondary schooling in particular^ (45%), but also those with some form of tertiary education^ (16%) had provided their student number in online transactions with government.

People with no education are significantly more likely than other educational groups to disclose the following types of identity information in online transactions with government (see Figure 41):

- Social welfare number*^: People with no education^ had far more provided their social welfare number in online government transactions (71%) than people with some level of educational achievement^;
- Community service card number*^: People with no education^ had far more provided their community service card number in online government transactions (71%) than people with some level of educational achievement^. 25% of those who have completed 5 years at secondary school^ and 18% of those with 3 years of secondary schooling^ also provided their community service card number in online government transactions;
- Information about any criminal convictions*^: Particularly people with no education^ (78%), but also those with a primary education background^ (34%) had provided information about criminal convictions to government online; and
- Personal opinions*^: Especially people with no education (100%), but also those with a primary education background^ (46%) had provided personal opinions in online transactions with government.

Figure 41: Information provided to government agencies, by education



Health information (p=.033: ^confidence intervals: none: no data; primary:7.2%-78%; 3yrs secondary:4.4%-41%; 4yrs secondary: no data; 5yrs secondary: 8.7%-59%); educational background (p=.011: ^confidence intervals: none: no data; primary:0.9%-41%; 3yrs secondary: no data; 4yrs secondary: 3.9%-34%; 5yrs secondary: 29%-68%; some tertiary: 18%-30); social welfare number (p=.004: ^confidence intervals: none:13%-98%; primary:0.9%-49%; 3yrs secondary:3.9%-35%; 4yrs secondary: 3.7%-45%; 5yrs secondary: 11%-62%); community service card number (p=.003: ^confidence intervals: none:13%-98%; primary:0.9%-41%; 3yrs secondary: 6.4%-41%; 4yrs secondary: 0.9%-35%; 5yrs secondary: 7.6%-58%); student number (p=.006: ^confidence intervals: none: no data; primary:0.9%-41%; 3yrs secondary: no data; 4yrs secondary: 0.7%-29%; 5yrs secondary: 21%-72%; some tertiary:11%-22%); information about any criminal convictions (p=.008: ^*confidence intervals: none:22%-89%; primary:7.2%-78%; 3yrs secondary:1.1%-40%; 4yrs secondary: 2.5%-35%; 5yrs secondary: 9.4%-41%*); personal opinions (p=.000: ^*confidence intervals: primary:13%-83%; 3yrs secondary:5.6%-45%; 4yrs secondary: 0.7%-29%; 5yrs secondary: 0.5%-21%*).

Why identity information is provided in online government transactions

Particularly people with no education^ (22%), but also those with 5 years of secondary schooling (16%), those with 3 years of secondary schooling^ (13%) and those with some form of tertiary education (2.6%), reported as one of the main reasons for them to provide identity information in online transactions with government is to get a service adapted to their personal needs^[64].

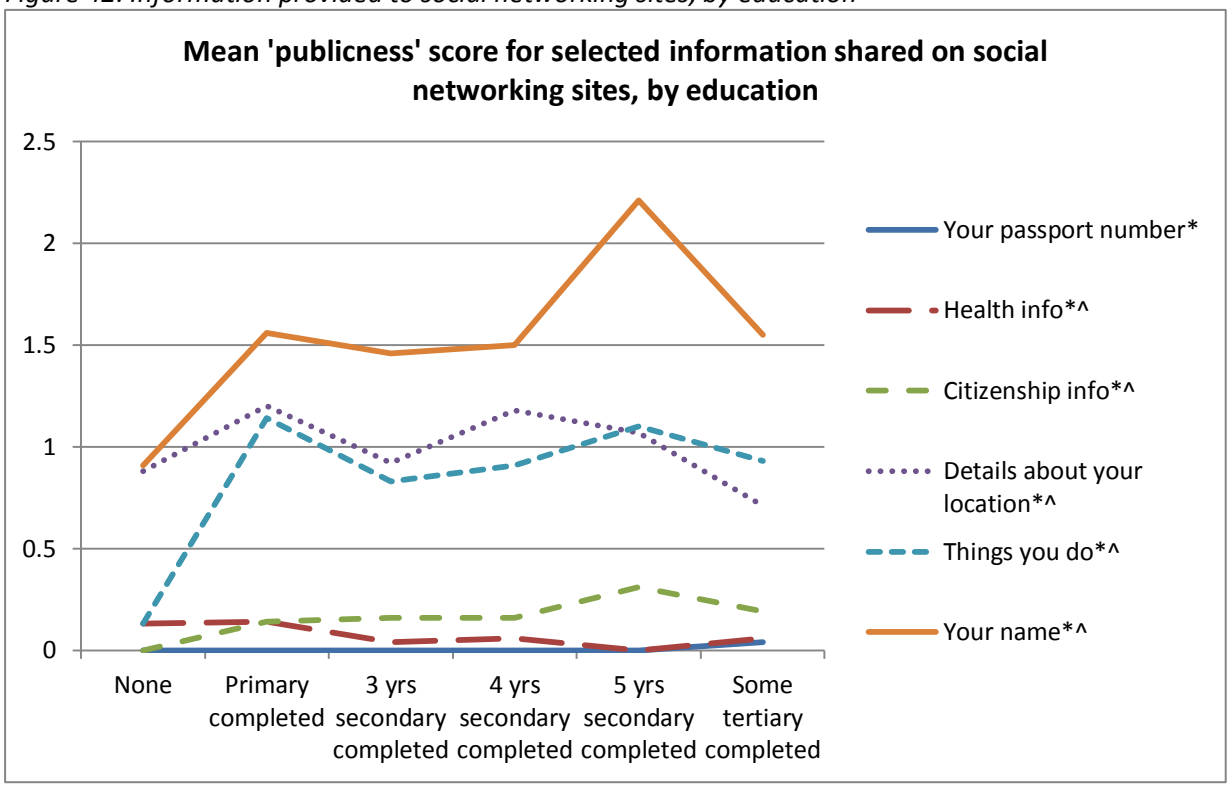
[64] *p=.033: ^confidence intervals: none: 2.3%-78 %; primary: no data; 3yrs secondary:2.9%-42%; 4yrs secondary: no data; 5yrs secondary: 3.6%-50%*

Sharing identity information as part of social networking

People from varying educational backgrounds demonstrate different identity information behaviours as part of social networking (see Figure 42). In particular, different behaviours could be observed between people with no education^ and people with some form of educational achievement^:

- Name*^: Respondents with no education^ were the most private of all educational groups about providing their name on SNSs (means score: .91).
- Things you do*: Respondents with no education (means score: .13) were more private than others on SNSs about the things they do.
- Personal opinions*^: People with no education^ (means score: .26), but also those who have completed primary education^ (means score: .39), were more private about their personal opinions on SNSs, than people with higher levels of educational achievement^.
- Information about NZ citizenship, residency or visa status*^: People with no education did not provide any information at all on SNSs about their New Zealand citizenship, residency or visa status. Respondents who had completed 5 years of secondary schooling^ were slightly less private with information about their New Zealand citizenship, residency or visa status on SNSs (means score: .31) compared to people with other levels of educational achievement.
- Current location*^: Respondents with some form of tertiary education (means score: .71), those with no education (means score: .88) and those who had completed 3 years of secondary schooling^ (means score: .92) were the most private about disclosing their current location on SNSs.
- SNS account details*^: People with no education^ (means score: 1.34) and those with primary schooling^ (means score: .55) were less private about their SNS account details on SNSs than people with higher levels of educational achievement.
- LinkedIn profile*^: People with no education^ (means score: 1.02), those with a primary education background^(means score: .63) and those with a tertiary education background (means score: .45) were less private about their LinkedIn profile on SNSs, compared with other respondents.
- Health information*: Respondents with no education (means score: .13) and those with primary education (means score: .14) were slightly less private about their personal health information on SNSs compared to other respondents.
- Passport number*: Only respondents with a tertiary education background disclosed their passport number to close friends, if anybody, on SNSs (means score: .04).

Figure 42: Information provided to social networking sites, by education



Name (p=.042: ^confidence intervals: none: 0.1-1.80; primary: 1.05-2.07; 3yrs secondary: 1.09-1.82; 4yrs secondary: 1.11-1.89; 5yrs secondary: 1.79-2.63); current location (p=.044: ^confidence intervals: primary: .75-1.65; 3yrs secondary: .54-1.31; 4yrs secondary: .75-1.60; 5yrs secondary: .77-1.38); health information (p=.011); information about NZ citizenship, residency or visa status (p=.000: ^confidence intervals: 5yrs secondary: -.23-.84); passport number (p=.04); things you do (p=.000: ^confidence intervals: primary: .29-1.99; 3yrs secondary: .47-1.20; 4yrs secondary: .53-1.30; 5yrs secondary: .84-1.37); personal opinions (p=.002: confidence intervals: none: -.08-.61; primary: .06-.71; 3yrs secondary: .29-1.16; 4yrs secondary: .39-1.16; 5yrs secondary: .85-1.51); SNS account details (p=.038: confidence intervals: none: .24-2.44; primary: -.04-1.15; 4yrs secondary: .09-.63); LinkedIn profile (p=.000: confidence intervals: none: -.35-2.39; primary: -.02-1.27).

Why identity information is provided on Social Networking Sites

People with lower levels of educational achievement^ and those with no education^ indicate different reasons for sharing identity information on SNSs^[65], compared to people with higher levels of educational achievement^:

Particularly people with a primary education background^ (48%), but also those with 3 years of secondary schooling^ (16%), those with no education^ (13%) and those with 4 years of secondary schooling^ (12%), reported convenience^ as an important reason to provide identity information on SNSs.

[65] *Convenience (p=.000: ^confidence intervals: none: 1.6%-59%; primary: 20%-77%; 3yrs secondary: 6.7%-34%; 4yrs secondary:4.7%-26%); to get a discount (p=.000: ^confidence intervals: none: 1.6%-59%; primary: no data; 3yrs secondary: no data; 4yrs secondary: no data; 5yrs secondary: no data); to ask a question (p=.000: ^confidence intervals: none: 9.5%-84%; primary:4.7%-56%; 4yrs secondary: 0.2%-11%; 5yrs secondary: 1.3%-19%).*

Particularly respondents with no education^ (13%), but also some respondents with a tertiary education background (0.2%) indicated getting a discount^ as an important reason to provide their identity information on SNSs.

People with no education^ (43%), but also those who have completed primary education^ (20.1%), reported an important reason for them to provide identity information to SNSs is to ask a question^.

Trust in organisations to protect identity information

People with varying educational backgrounds demonstrate different levels of trust in organisations to protect their identity information (see Figure 43).

People with no education^ trusted insurance companies^ much more to protect their identity information, compared to respondents with some level of educational achievement^.

People with no education^ tended to have slightly more trust in overseas online dating sites^ to protect their identity information, than people with other educational backgrounds.

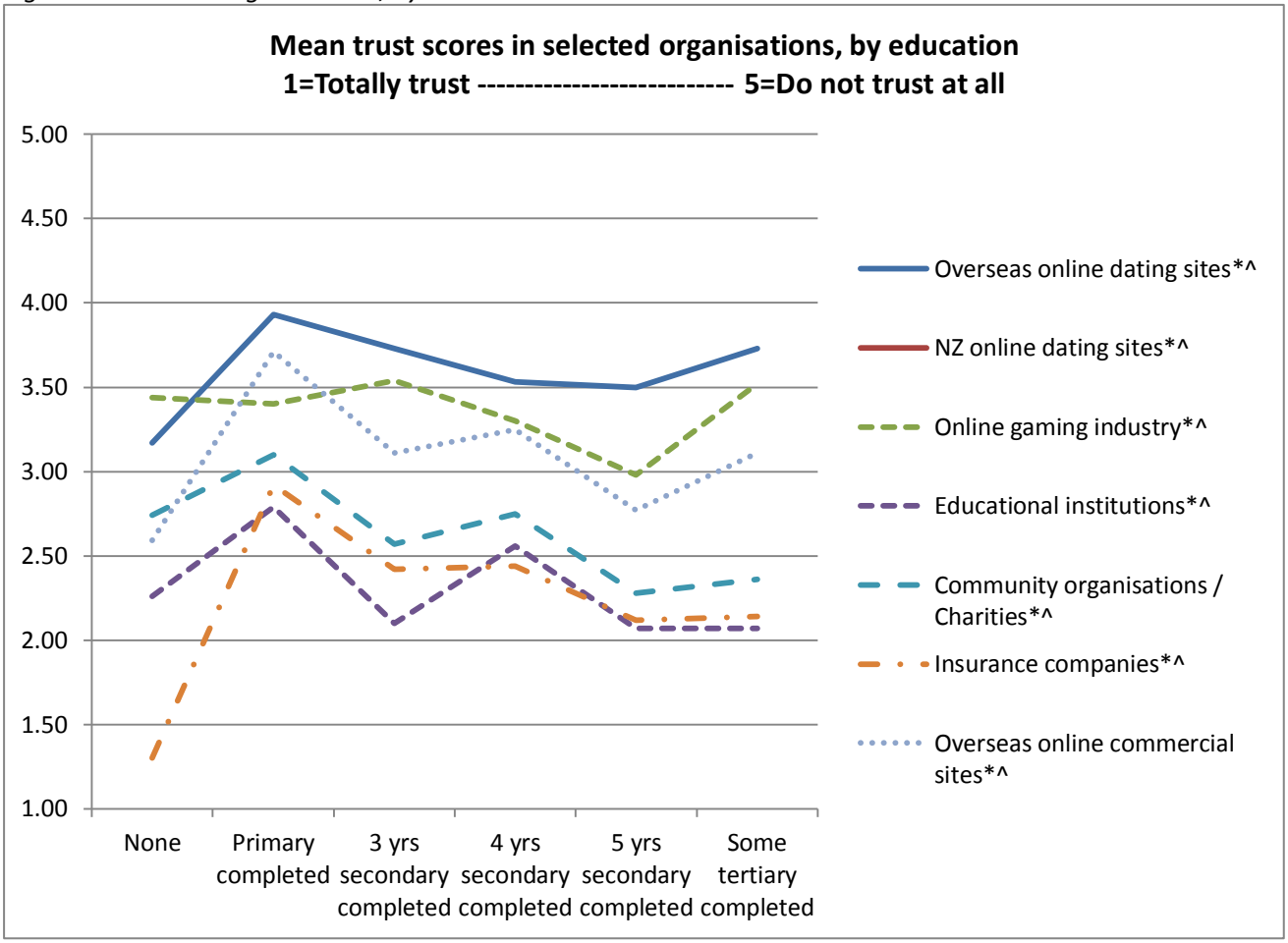
Respondents with no education^ and those with 5 years of secondary schooling^ tended to have more trust in overseas-based online commercial sites^ to protect their identity information, than people with other educational backgrounds^.

People with 5 years of secondary schooling^ and those with a tertiary education background tended to have slightly more trust in educational institutions^ to protect their identity information, than others.

People with 5 years of secondary schooling and those with a tertiary education background tended to have more trust in community organisations and non-government organisations^ to protect their identity information, than other respondents^.

People with 5 years of secondary schooling^ tended to have more trust in the online gaming industry^ to protect their identity information, compared with others^.

Figure 43: Trust in organisations, by education



Insurance companies (p=.000: ^confidence intervals: none: .90-1.70; primary: 2.24-3.60; 3yrs secondary: 2.12-2.72; 4yrs secondary: 2.14-2.73*); online commercial sites overseas (p=.000:* ^confidence intervals: none: 1.25-3.93; primary: 3.42-3.99; 3yrs secondary: 2.81-3.41; 5yrs secondary: 2.49-3.06*); online gaming industry (p=.011:* ^confidence intervals: none: 3.33-4.21; primary: 2.83-3.97; 3yrs secondary: 3.22-3.86; 4yrs secondary: 3.02-3.59; 5yrs secondary: 2.69-3.26*); online dating sites overseas (p=.008:* ^confidence intervals: none: 2.15-4.19*); educational institutions (p=.004:* ^confidence intervals: none: .70-3.82; primary: 2.33-3.25; 3yrs secondary: 1.79-2.41; 5yrs secondary: 1.79-2.36*); community organisations (p=.005:* ^confidence intervals: none: 1.65-3.83; primary: 2.62-3.59; 3yrs secondary: 2.25-2.90; 4yrs secondary: 2.47-3.03*).*

Steps taken to protect online identity information

22% of the respondents who have completed primary school, 6.1% of those with 5 years of secondary schooling and 1.4% of those with a tertiary education background used a personal information vault to protect their identity information.

Personal information vault (p=.000: confidence intervals: none: no data; primary: 6.5%-54%; 3yrs secondary: no data; 4yrs secondary: no data; 5yrs secondary: 1.9%-18%).

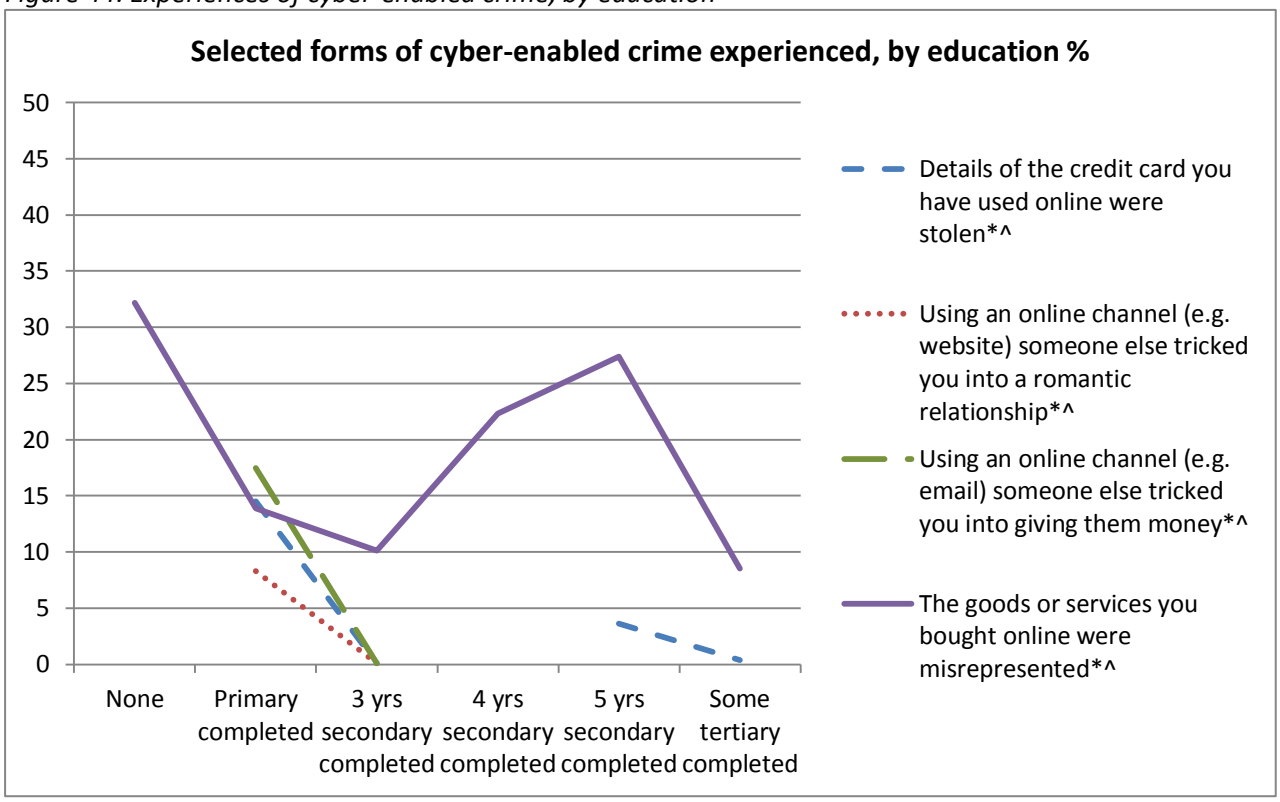
User experiences with forms of cybercrime or cyber-enabled crime

People who have completed primary education are significantly more likely to have had an experience online with stolen credit card details, being tricked into giving money, being tricked into a romantic relationship, or with misrepresented goods or services bought online, compared to people with other levels of educational achievement (see Figure 44):

- Credit card details stolen*^[66]: 15% of respondents with a primary school background^, 3.6% of people with 5 years of secondary education^, 0.4% of people with a tertiary education background and 0.1% of people with 3 years of secondary education, reported the personal experience of stolen credit card details;
- Someone else tricked you into giving them money*^[67]: 18% of respondents with a primary school background^, 0.7% of respondents with a tertiary education background and 0.1% of respondents with 3 years of secondary education, reported the personal experience online of someone else tricking them into giving money;
- Someone else tricked you into a romantic relationship*^[68]: 8.3% of respondents with a primary school background^, 0.4% of the people with a tertiary education background and 0.1% of people with 3 years of secondary education, reported the personal experience of having been tricked into a romantic relationship online;
- Goods or services bought online were misrepresented*^: 32% of respondents with no education^, 14% of respondents with a primary education background^, 10% of respondents with 3 years of secondary education^, 22% of respondents with 4 years of secondary education^, 27% of respondents with 5 years of secondary education and 8.5% of respondents with a tertiary education background reported the personal experience of misrepresented goods or services bought online.

[66] No education: no data; 4yrs secondary school: no data
[67] No education: no data; 4yrs secondary school: no data; 5yrs secondary school: no data
[68] No education: no data; 4yrs secondary school: no data; 5yrs secondary school: no data

Figure 44: Experiences of cyber-enabled crime, by education



Credit card details stolen (p=.002: ^confidence intervals: none: no data; primary: 2.1%-57%; 4yrs secondary: no data; 5yrs secondary: 0.5%-22%); someone else tricked you into a romantic relationship (p=.011: ^confidence intervals: none: no data; primary: 1.1%-42%; 4yrs secondary: no data; 5yrs secondary: no data); goods or services bought online were misrepresented (p=.012: ^confidence intervals: none: 4.8%-82%; primary: 2.0%-56%; 3yrs secondary:3.6%-25%; 4yrs secondary: 12%-38%; 5yrs secondary: 15%-46%); someone else tricked you into giving them money (p=.001: ^confidence intervals: none: no data; primary: 3.9%-53%; 4yrs secondary: no data; 5yrs secondary: no data).

References

European Commission (2012) *Cyber Security*, Special Eurobarometer 390, Survey undertaken by the European Commission

European Commission (2011) *Attitudes on Data Protection and Electronic Identity in the European Union* , Special Eurobarometer 359, Survey undertaken by the European Commission

Fox, S. (2000). *Trust and Privacy Online: Why Americans Want to Rewrite the Rules.* Retrieved from: www.pewinternet.ort/Reports/2000/Trust-and-Privacy-Online.aspx

Halperin, R., & Backhouse, J. (2008). *A roadmap for research on identity in the information society. Identity in the Information Society, 1.* Retrieved from: http://www.springer.com/computer/journal/12394

Lips, A.M.B., Eppel, E., Cunningham, A. & Hopkins-Burns, V. (2010) *Public attitudes to the sharing of personal information in the course of online public service provision.* Wellington: Victoria University of Wellington

Lohr, S. (2010). *Sampling Design and Analysis*, (2nd ed.), Brooks/ Cole.

Nissenbaum, H. (2010). *Privacy In Context: Technology, Policy and the Integrity of Social Life.* California: Stanford University Press.

Olson, J. S., Grudin, J., & Horvitz, E. (2005). *A Study of Preferences for Sharing and Privacy.* Paper presented at the CHI'05 Extended Abstracts on ACM SIGCHI Conference on Human Factors in Computing Systems, Portland, OR, April 2-7 New York.

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

Annex 1 – Survey Questionnaire

Q1 **In the last 12 months, which of the following devices have you used to go on to the Internet? Please tick all that apply.**

- ☐ PC or desktop computer
- ☐ Laptop, notebook or netbook
- ☐ Tablet (e.g. iPad, PDA)
- ☐ Mobile phone
- ☐ Internet enabled television
- ☐ Games console (e.g. Xbox, Playstation)
- ☐ E-book reader
- ☐ Kiosks
- ☐ I don't go on to the internet. Please explain why: _____

  _____

  _____

- ☐ Other. Please specify:_____

If you ticked the option 'I don't go on to the Internet', please skip to question Q11.

Q2 **How often do you use the Internet, and at which location? Please circle the number which best represents your answer.**

		Everyday / Almost everyday	Two or three times a week	About once a week	Two or three times a month	Less often	Never
1	I use the Internet at home	1	2	3	4	5	6
2	I use the Internet at work	1	2	3	4	5	6
3	I use the Internet on a mobile device	1	2	3	4	5	6
4	I use the Internet at school	1	2	3	4	5	6
5	I use the Internet at a public library	1	2	3	4	5	6
6	I use the Internet at an Internet café	1	2	3	4	5	6

Q3 What activities have you done in the last 12 months? Please circle the number that <u>best</u> represents your answer.

		Yes	No	Don't Know
1	Went online to search for information, news, etc.	1	2	3
2	Used a social networking site	1	2	3
3	Purchased something online (e.g. clothes, books, tickets, insurance, films, music, software, food, travel, accommodation)	1	2	3
4	Transacted with government agencies online (e.g. submitted your tax form, applied for a benefit , registered your vehicle, managed a student loan)	1	2	3
5	Participated in online public consultations from government agencies	1	2	3
6	Used the iGovt or RealMe[1] service	1	2	3
7	Did personal banking online	1	2	3
8	Traded online (e.g. using TradeMe)	1	2	3
9	Participated in online discussion groups	1	2	3
10	Dated online	1	2	3
11	Participated in online games	1	2	3
12	Communicated online (e.g. used email, text, Skype)	1	2	3
13	Participated in education online	1	2	3
14	Created content online (e.g. photos, blogs, YouTube video)	1	2	3
15	Participated in entertainment online (e.g. watched videos online, watched television on demand, listened or downloaded music, read e-book)	1	2	3
16	Stored information online (e.g. used Dropbox, backups)	1	2	3
17	Conducted my business online (e.g. running my own website)	1	2	3
18	Hacked[2] into another person's online system or device	1	2	3
19	Pretended to be someone else	1	2	3
20	Other. Please specify:			

[1] **RealMe** (previously iGovt) = *a way of verifying your identity, so you can use the same log-in for communications with several government departments.*

[2] **Hacked** = A*ttempted to gain unauthorised access to another person or organisation's computer systems.*

Q4A **In the last 12 months when you have PURCHASED GOODS OR SERVICES over the Internet, which of the following types of information have you provided? Please circle the number which <u>best</u> represents your answer.**

	Yes	No	Don't Know
Credit card or debit card details	1	2	3
Bank details	1	2	3
Your name	1	2	3
Your home address	1	2	3
Your billing address	1	2	3
Your mobile phone number	1	2	3
Your email address	1	2	3
Information about your insurance	1	2	3
Health information	1	2	3
Employment details	1	2	3
Information about your educational background	1	2	3
Information about your New Zealand citizenship, residence or visa status	1	2	3
Your Facebook log-in details	1	2	3
Things you do (e.g. hobbies, sports, places you go)	1	2	3
Your personal opinions and tastes	1	2	3
Who your friends are	1	2	3
Information about your relationship status	1	2	3
Information about whether or not you have any criminal convictions (e.g. speeding, drunk driving)	1	2	3
Other. Please specify:			

Q4B What are the most important reasons why you provided such information when PURCHASING GOODS AND SERVICES online? Please circle the numbers of the top <u>three</u> reasons for you.

To access further information about the service	1
To get a product or service	2
To complete the transaction	3
I was asked to do so	4
Convenience (e.g. to save time, to have 24/7 service access, expediency)	5
To get a financial discount	6
To get a personalised service	7
To benefit from personalised commercial offers in the future	8
For fun	9
To connect with others	10
To ask a question	11
It doesn't bother me	12
Other. Please specify:	13
Don't Know	14

Q5A **Thinking of the occasions when you have transacted with New Zealand GOVERNMENT AGENCIES online via the Internet over the last 12 months, which of the following types of information have you provided? Please circle the number which best represents your answer.**

	Yes	No	Don't Know
Financial information (e.g. credit card details, bank details)	1	2	3
Your name	1	2	3
Your home address	1	2	3
Your mobile phone number	1	2	3
Your email address	1	2	3
Information about your insurance	1	2	3
Your IRD number	1	2	3
Health information	1	2	3
Employment details	1	2	3
Information about your educational background	1	2	3
Information about your New Zealand citizenship, residence or visa status	1	2	3
Things you do (e.g. life style, hobbies, sports, places you go)	1	2	3
Social welfare number	1	2	3
Community services card number	1	2	3
Student number	1	2	3
Health services number	1	2	3
Your RealMe[3] (previously known as iGovt) logon details	1	2	3
Your driver's licence number	1	2	3
Your passport number	1	3	3
Information about whether or not you have any criminal convictions (e.g. speeding, drunk driving)	1	2	3
Your personal opinions	1	2	3
Other. Please specify:			

[3] **RealMe (previously iGovt)** = *Way of verifying your identity, so you can use the same log-in for communications with several government departments.*

Q5B What are the most important reasons why you provided such information in online New Zealand GOVERNMENT transactions? Please circle the numbers of the top <u>three</u> reasons for you.

To access information about the service	1
To get the service I want / need	2
Convenience (e.g. to save time, to have 24/7 service access)	3
I was asked to do so	4
To receive a price reduction	5
To benefit from personalised service	6
To pay (or receive) tax, ACC levies, fines	7
To engage with government	8
To comply with the law (e.g. file a return)	9
To be a good New Zealander	10
To get a service adapted to your personal needs	11
To organise a meeting appointment	12
To ask a question	13
It doesn't bother me	14
Other. Please specify:	15
Don't Know	16

Q6A **Thinking of your usage of SOCIAL NETWORKING SITES and sharing sites over the last 12 months, which of the following types of information have you already provided, and to whom? Please circle the number which <u>best</u> represents your answer.**

	Close friends	Friends of friends	Public	No-one	Don't know
Your name	1	2	3	4	5
Your home address	1	3	3	4	5
Details about your location	1	2	3	4	5
Your mobile phone number	1	2	3	4	5
Your email-address	1	2	3	4	5
Financial information (e.g. credit card details, bank details)	1	2	3	4	5
Health information	1	2	3	4	5
Employment details	1	2	3	4	5
Educational background information	1	2	3	4	5
Information about your New Zealand citizenship, residence or visa status	1	2	3	4	5
Your passport number	1	2	3	4	5
Things you do (e.g. hobbies, sports, places you go)	1	2	3	4	5
Your personal tastes and opinions	1	2	3	4	5
Photos of you	1	2	3	4	5
Who your friends are	1	2	3	4	5
Information about your relationship status	1	2	3	4	5
Information about whether or not you have any criminal convictions (e.g. speeding, drunk driving)	1	2	3	4	5
Your social networking service account details (e.g. Facebook or Twitter account details)	1	2	3	4	5
Your LinkedIn profile	1	2	3	4	5
Your user name	1	2	3	4	5
Your password	1	2	3	4	5
Websites you visit	1	2	3	4	5
Other. Please specify:	1	2	3	4	5

Q6B What are the most important reasons why you provided such information on SOCIAL NETWORKING SITES and/or sharing sites? Please circle the numbers of the top <u>three</u> reasons for you.

To access the social networking site / sharing site	1
To get information (e.g. news, updates from friends/family, product information)	2
To get a product or service adapted to your needs	3
Convenience (e.g. to save time, 24/7 access)	4
I was asked to do so	5
To get a discount	6
To benefit from personalised commercial offers	7
For fun	8
To connect with people	9
To share information with people	10
To meet people	11
To ask a question	12
It doesn't bother me	13
Other: Please specify	14
Don't Know	15

Q7 **Different authorities (government departments, local authorities, agencies) and private companies collect and store personal information. To what extent do you trust the following institutions to protect your personal information? Please circle the number which best represents your answer.**

		Totally trust	Tend to trust	Tend not to trust	Do not trust at all	Don't Know
1	New Zealand central government agencies (e.g. IRD, Work & Income, Internal Affairs, Police)	1	2	3	4	5
2	New Zealand local government	1	2	3	4	5
3	Banks and financial institutions	1	2	3	4	5
4	Insurance companies	1	2	3	4	5
5	Health and medical institutions (e.g. GP, hospital, dentist)	1	2	3	4	5
6	Online commercial sites in New Zealand (e.g. online shops)	1	2	3	4	5
7	Online commercial sites overseas	1	2	3	4	5
8	Social Networking service companies (e.g. Facebook, Google, Twitter)	1	2	3	4	5
9	Online trading sites in New Zealand (e.g. Trademe)	1	2	3	4	5
10	Online trading sites overseas (e.g. eBay)	1	2	3	4	5
11	Sharing sites (e.g. films, music)	1	2	3	4	5
12	Online gaming industry	1	2	3	4	5
13	Online dating sites in New Zealand	1	2	3	4	5
14	Online dating sites overseas	1	2	3	4	5
15	Phone companies and Internet Service Providers	1	2	3	4	5
16	Media organisations	1	2	3	4	5
17	Educational institutions	1	2	3	4	5
18	Community organisations / non-government organisations / charities	1	2	3	4	5

Q8 When you are on the Internet, what do you do to protect your identity? Please circle the number which best represents your answer.

	Yes	No	Don't Know
Change your privacy settings	1	2	3
Use security-protected WiFi or other networks	1	2	3
Use a dummy email account	1	2	3
Use antivirus software	1	2	3
Use a firewall[4]	1	2	3
Delete cookies[5]	1	2	3
Delete your online search history	1	2	3
Use a pseudonym[6]	1	2	3
Use tools and strategies to limit unsolicited emails (e.g. spam)	1	2	3
Check that the transaction is protected (e.g. only using Paypal for transacting money online)	1	3	3
Check the privacy policy of a website	1	2	3
Check that the website has a safety logo or label	1	2	3
Avoid providing the same information to different sites (e.g. using the same password for different sites)	1	2	3
Change your social networking site profile	1	2	3
Disclose minimal information about yourself	1	2	3
Use a search engine (e.g. Google, Bing, Yahoo) to maintain awareness of what information circulates about you on the Internet	1	2	3
Ask organisations to update or delete the online information they hold about you	1	2	3
Use a filter (e.g. on your email)	1	2	3
Use proxies (e.g. Tor)[7]	1	2	3
Use a password generator (e.g. Lastpass, PWGen)	1	2	3
Use iGovt or RealMe[8]	1	2	3
Use a personal information vault[9]	1	2	3
Don't provide any personal information via online channels	1	2	3
Other. Please specify			

[4]**Firewall** = *Software that helps screen out hackers, viruses, and destructive programs that try to reach your device over the Internet.*
[5]**Cookies** = *Small amount of data generated by the website you are visiting and saved on your web browser. Preferences and settings for that website can be stored this way.*
[6]**Pseudonym** = A *name you have made up*.
[7]**Proxies** = *Prevents others, especially sites you visit, learning about your online behaviour and location by 'bouncing' your communications around other networks.*
[8]**RealMe (previously iGovt)** = *Way of verifying your identity, so you can use the same log-in for communications with several government departments.*
[9]**Personal data vault** = *Service which stores and protects your personal data, loaning it only to Internet companies and advertisers that you trust and approve of, sometimes in exchange for discounts or rebates.*

Q9 **Thinking about <u>privacy statements</u> on the Internet, which one of the following sentences <u>best</u> describes what you usually or most often do?**

You usually read and understand them	1
You usually read them, but do not fully understand them	2
You usually do not read them	3
You do not know where to find them	4
You ignore them	5
Other. Please specify:	6

Q10 **In the last 12 months, have you <u>personally experienced</u> any of the following events? Please circle the number which <u>best</u> represents your answer.**

	Yes	No	Don't Know
etails of the credit card you have used online were stolen	1	2	3
ıe goods or services you bought online were misrepresented	1	2	3
ıe goods or services you ordered online were not delivered	1	2	3
sing an online channel someone else asked for your bank details	1	2	3
meone else misrepresented themselves to you online (providing incorrect name/ age/ gender/ photo)	1	2	3
meone else pretended to be you online without your permission	1	2	3
alware[10] was downloaded onto your device over the internet	1	2	3
sing an online channel (e.g. email) someone else tricked you into giving them money	1	2	3
meone else hacked[11] into your online device	1	2	3
Someone else used your name to set up a social media account (e.g. Facebook, LinkedIn)	1	2	3
Someone else sent out emails under your name without your permission	1	2	3
Using an online channel (e.g. website) someone else tricked you into a romantic relationship	1	2	3
Someone else uploaded pictures of you into an online public space, without your permission.	1	2	3

[10]**Malware** = *Computer viruses, Trojan horse, keylogger and other software which you are tricked in to downloading or download by mistake, and which can disrupt your online device, or gather information about you or your online device. Choose Yes if you KNOW this has happened to you.*

[11] **Hacked** = A*ttempted to gain unauthorised access to another person or organisation's computer systems.*

Finally, please tell us something about yourself. Please tick the box that <u>best</u> applies to your personal circumstances

Q11 Your age:

- ☐ Under 18 years
- ☐ 18 – 24 years
- ☐ 25 – 34 years
- ☐ 35 – 44 years
- ☐ 45 – 54 years
- ☐ 55 – 64 years
- ☐ 65 – 74 years
- ☐ 75 years and over

Q12 Your gender: ☐ Male ☐ Female

Q13 Where do you currently live?

- ☐ Auckland
- ☐ Christchurch
- ☐ Wellington
- ☐ Hamilton
- ☐ Dunedin
- ☐ Tauranga
- ☐ Other city
- ☐ Rural area

Q14 Which ethnic group do you belong to? Please tick <u>all</u> that apply.

- ☐ NZ European
- ☐ Māori
- ☐ Samoan
- ☐ Cook Island Māori
- ☐ Tongan
- ☐ Niuean
- ☐ Chinese
- ☐ Indian
- ☐ Other. Please specify_____

Q15 What is your <u>personal</u> income from all sources, before tax or anything else is taken out?

- ☐ $0 (no income)
- ☐ $1 - $10,000
- ☐ $10,001 - $20,000
- ☐ $20,001 - $30,000
- ☐ $30,001 - $50,000
- ☐ $50,001 - $70,000
- ☐ $70,001 - $100,000
- ☐ $100,001 - $150,000
- ☐ $150,001 or more
- ☐ I don't know
- ☐ I don't wish to answer

Q16 **Do you know roughly how much your household spends each month on all telecommunications (internet connection, phone, TV)?**

☐ No ☐ Yes roughly $_____ per month

Q17 **Do you know roughly your monthly data allowance (internet data cap)?**

☐ No ☐ Yes roughly _____GB per month

Q18 **What is your highest level of achievement at school?**

☐ None

☐ Completed primary school

☐ Completed 3 years at secondary school

☐ Completed 4 years at secondary school

☐ Completed 5 years at secondary school

☐ Completed some form of tertiary education (e.g. at a technical institute, polytech, wananga, university)

Q19 **Is there anything else you would like to tell us relating to the survey topics?**

_____

_____

_____

_____

Thank you for completing our survey.

Annex 2 - Definitions of terms used

Cookies	Small amount of data generated by a website visited which allows personal preferences and settings for that website to be stored on the user's computer
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
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
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
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