Survey of Internet Users Regarding Cyber Security

Final Report

Prepared for Public Safety Canada

Supplier: EKOS RESEARCH ASSOCIATES INC.
Contract Number: OD160192340/001/CY
Contract Value: $122,983.55 including taxes
Award Date: August 13, 2018
Delivery Date: September 30, 2018

Registration Number: POR 032-18
For more information on this report, please contact Public Safety Canada at ps.communications-communications.sp@canada.ca

Ce rapport est aussi disponible en français

Survey of Internet Users Regarding Cyber Security

Final Report

Prepared for Public Safety Canada
Supplier name: EKOS RESEARCH ASSOCIATES INC.
Date: September 30, 2018

This public opinion research report presents the results of an online survey conducted by EKOS Research Associates Inc. on behalf of Public Safety Canada. The research study was conducted with 2,072 Canadians between August 21 and September 5, 2018.

Cette publication est aussi disponible en français sous le titre Sondage auprès des utilisateurs d'Internet au sujet de la cybersécurité.

Communications Branch
Public Safety Canada
269 Laurier Ave. W.
Ottawa ON K1A 0S5

Catalogue Number:
PS4-245/2018E-PDF
International Standard Book Number (ISBN):
978-0-660-27887-2

Related publications (registration number: POR 130-16):

Catalogue Number PS4-245/2018E-PDF (Final Report, English)
ISBN 978-0-660-27887-2

EKOS RESEARCH ASSOCIATES

Contact: Susan Galley

Ottawa Office
359 Kent Street, Suite 300
Ottawa, Ontario
K2P 0R6
Tel: (613) 235 7215
Fax: (613) 235 8498
E-mail: pobox@ekos.com

www.ekos.com

TABLE OF CONTENTS

LIST OF TABLES

LIST OF CHARTS

SUMMARY

The use of Internet-enabled computer technology is ubiquitous across Canada. A priority of Public Safety Canada is to make the public aware of issues of security and safety and help Canadians stay safe from cyber threats. This survey gathers quantitative data on the knowledge, attitudes, and behaviours of Canadians who use the Internet to inform future communications and policy development initiatives. Interviews were completed with 2,072 Canadian adults from across the country who use the Internet. The cases were drawn from a random selection of Prob*it* panel members, a randomly recruited panel of Canadian households assembled through random digit dialling (RDD) methodology used in standard telephone survey sampling techniques.

A series of eight focus group discussions were also held across the country to discuss awareness of online security risks, types of actions taken and need for information.

Usage of the Internet

Survey results confirm that Canadians are using a variety of Internet-enabled devices to access the web on a daily basis, including not only desktop and laptop computers (93 per cent), but smartphones (76 per cent), tablets/readers (58 per cent), smart TVs (27 per cent), streaming services (25 per cent), gaming systems (21 per cent), and other devices. Virtually everyone has access from home, and almost nine in ten are using secure Wi-Fi in their home. Canadians spend an average of five hours online per day.

Canadians use the Internet for a wide variety of activities, with almost everyone using the Internet for email and browsing websites. Canadians also commonly use the Internet to perform financial transactions, follow the news, view videos and movies, make purchases, use social networking sites such as Facebook or Twitter, and/or access government information services. Email is the most ubiquitous source of risk with 98 per cent of Canadians engaging in this online activity.

Level of Concern and Awareness

Canadians who are actively using the Internet are very concerned about having their personal information obtained and used without permission as a result of their online activities. In fact, half say they are very concerned and, by and large, the remainder are moderately concerned. The importance of taking steps to protect personal information online and home computers is also not lost on Canadians with more than eight in ten seeing this as important. A similar proportion recognizes the importance of protecting mobile devices from online threats.

Canadians perceive online threats to be fairly commonplace today; 43 per cent believe it is very common for Canadians to be affected, and more than four in ten feel it is moderately common. In terms of one's own personal online security, one in three think it very likely they will be affected by an online threat in the near future, and another one in three believe it to be moderately likely.

The majority of Canadians online are aware of the threats individuals can face when using the Internet. Similar to the awareness levels in 2016, nine out of ten Canadians are aware of spyware/ malware on computer devices, being a victim of an online scam or fraud, and identity theft. Eight in ten are also familiar with privacy violations, and loss. More Canadians (three in four) are now aware of personal data held for ransom (a 12-point increase from 2016), as well as the loss of files or information, or personal data erased, changed, or lost. Almost all Canadians also report being aware of precautions they can take to protect themselves online, such as not sharing passwords, not opening email attachments from people they do not know, and limiting the personal information they share online, and using anti-virus/anti-spyware software. Virtually everyone is also aware that their laptop or computer can be affected by an online threat, and eight in ten are aware of the same potential for a smartphone or tablet/reader. This drops considerably, however, when it comes to awareness of possible risks to voice activated devices, smart TVs, or wearable devices.

Results suggest that Canadians' familiarity with crypto currency is quite limited and that its use is rare. Just under half of Canadians would consider themselves at least moderately familiar with the alternative currency and of those who are familiar, just one in ten have used it.

Level of Protective Measures Taken

The vast majority of Canadians say they are just as cautious – or even more cautious – when protecting themselves against online threats as they are in response to real-world threats. They report a strong repertoire of precautions they take to protect their devices and personal information online, including two in three or more who say they download files only from trusted sources, keep anti-virus software up-to-date, lock devices with password protection, password-protect their Wi-Fi, and generally use caution with unknown sources.

About nine in ten Canadians say that they refrain from sharing passwords, while eight in ten use complex passwords or exercise caution when giving out information like their real name, address, or phone number and when responding to solicitations from strangers. Roughly nine in ten say that they have anti-virus software installed on their computers. Other precautions that are used less often include changing default passwords, checking privacy policies, using multiple email accounts under a pseudonym, not using an administrator account when accessing the web, and using encryption software. There is a fairly significant increase from one in four Canadians in 2016 to now one in three Canadians who report using two-step authentication or biometric protection.

Nevertheless, many risky forms of behaviour are prevalent. Nearly half of Canadians report using the same passwords for multiple accounts, and four in ten allow their browsers to store their passwords. Also, between three in ten and four in ten Canadians never change their passwords, or do so only every few years, for social media, shopping, and email accounts. Younger Canadians (25 or younger) are more likely than older Canadians to be prompted to change their social media account passwords when they hear about a breach.

Although one in ten Canadians say they are less likely to take precautions against online threats when compared to in-person threats, three in ten are more likely to exercise caution in the digital world than the real world (and six in ten say they exercise the same degree of precaution).

Incidence of Victimization

The incidence of victimization from online attacks appears to be on the rise. More than half of Canadians (56 per cent) report having been a victim of a virus, spyware, or malware attack on the device(s) they use to access the Internet for personal use. Results also indicate that there is at least a moderate impact from these attacks for more than half, with one in five reporting a significant impact. Between five and 12 per cent have experienced identity theft and financial loss as a result of online activity.

Need for Information

Canadians have looked for a range of information about online threats, including protecting devices with anti-virus software (48 per cent), how to secure home networks (38 per cent), and how to tell if an email is a scam (38 per cent). Three in ten looked for information about how to protect devices and computer files (30 per cent), while one-quarter researched steps towards safe social networking. Use of public Wi-Fi, general terms related to cyber security, and cyberbullying were also sought out by about one in six. Most looked for this information using a general search engine (two in three) or from a vendor website (four in ten). Government websites or friends and family were consulted about a third of the time. Results suggest that most are looking for information proactively rather than trying to fix a problem that has already occurred, highlighting a willingness to take steps provided they have access to the information they need. This was echoed in the focus group discussions where many expressed an interest in a website with centralized information about general, and new security risks, and considerations for protective behaviours.

Two-thirds of Canadians are confident that they can protect themselves online as long as they have the basic information on steps to take, suggesting a need for concrete information, particularly for those less knowledgeable and confident. Six in ten feel that they have enough information on how to take steps to protect themselves against online threats, although one in four Canadians do not feel this way. Canadians are similarly mixed about whether they feel they have enough information to know how new technologies might affect their personal privacy, with half agreeing that this is the case and one in three disagreeing.

Canadians are mixed in their trust of a variety of sources in terms of the technical reliability, currency, and neutrality of information about online threats. Around half of Canadians trust law enforcement organizations, governments, and security software companies. Slightly fewer trust Internet service providers for current and reliable information about online threats. When Canadians are asked to indicate their most trusted source for unbiased information about online threats, law enforcement agencies and governments again top the list, with half of Canadians expressing confidence in these groups. Not-for-profit organizations rank third, while financial institutions, friends and family, private vendors, and security software companies are each trusted by one in four Canadians.

Most Canadians think that the responsibility for ensuring that web-enabled personal devices are safe and secure rests with the individual owners of the devices, suggesting again that they are willing to take action, provided they have the information they need to do it.

Canadians have varying interpretations of what constitutes “fake news”. About four in ten interpret the term to mean information that is falsely used to shape opinion or facts, although three in ten feel that it refers to information that comes from a biased source. There is no consensus on who should take charge in helping Canadians recognizing fake news, although the plurality of Canadians believe that governments should play a key role.

Concern Among Parents

Results suggest that while many parents feel that they have the information they need to protect their children online, a significant minority do not feel this to be the case. For example, while more than half feel that they are confident they have the information to help their child navigate online, one in four say they do not. Four in ten also agree that they cannot keep up with the apps, games, and other technology that young people are using. More than half say that they are concerned for their children’s privacy and also about cyberbullying and online harassment. Fewer (one in five to four in ten) are concerned with the legal implications of image and file sharing. Those parents who are not concerned about their children’s exposure to these threats say they have already spoken with their children about these issues, their children are not online to an extensive degree (more often among parents with younger children), their child receives sufficient information at school, or they trust their child to act appropriately.

Concerns Among Businesses

Although a survey of the general public, the research took the opportunity to ask those who are self-employed or in a managerial position in a small- to medium-sized company (i.e., with fewer than 250 employees) about their IT practices and level of concern when it comes to online protection. A total of 533 businesses were represented. Although one in four say that they are very concerned, half rated themselves as moderately concerned, and one in five say that are not concerned with work disruptions and/or financial loss from online threats. Among those unconcerned, this is most often because they feel that the threat is very low or they feel that they have researched and taken appropriate steps to protect the business.

Results show that there is as much need for improvement in security protection from online threats to businesses as there is among members of the public in their personal space. Between half and seven in ten employers require employees to password protect devices, keep security software up to date, use password authentication, back up information, and set spam filters. About half of the time, employees are asked to download only from trusted sources, use complex passwords, and click with caution when opening attachments and responding to email invitations. Slightly fewer instruct employees to not give out passwords, use caution when responding to solicitations from strangers, and change default passwords. Results also show that there is a strong appetite for information on a range of topics to help businesses identify and manage their risks from online threats. These include having a list of threats to look for, procedures for dealing with a cyber attack, steps to protect mobile devices in a public setting, best practices for storage of data, guidelines for employees' use of personal devices for work, and guidelines to establish rules for safe email usage policies, each of interest to at least four in ten businesses.

Segments of the Population

There are a number of repeating patterns found in the survey results. Younger Canadians are more active online, and tend to be more knowledgeable about online threats and security. Older Canadians are less active, but more concerned about security, and typically more apt to be looking for information and advice on how to protect themselves online. The generational divide is typically found with the younger boomers (with results looking quite different for those under 45 to 55, and those 45 to 55 and older). Socioeconomic status also provides a key demarcation, with those reporting higher education often reporting more online activity and awareness of the issue. Residents of Quebec report lower awareness of online threats and security, less concern about potential threats, and fewer protective measures taken.

The contract value for the POR project is $122,983.55 (including HST).

Supplier Name: EKOS Research Associates
PWGSC Contract Number: OD160192340/001/CY
Contract Award Date: August 13, 2018
To obtain more information on this study, please email info@GetCyberSafe.gc.ca

POLITICAL NEUTRALITY CERTIFICATION

This certification is to be submitted with the final report submitted to the Project Authority.

I hereby certify as Senior Officer of EKOS Research Associates Inc. that the deliverables fully comply with the Government of Canada political neutrality requirements outlined in the Communications Policy of the Government of Canada and Procedures for Planning and Contracting Public Opinion Research.
Specifically, the deliverables do not include information on electoral voting intentions, political party preferences, standings with the electorate, or ratings of the performance of a political party or its leaders.

Signed by:

Susan Galley (Vice President)

1. INTRODUCTION

1.1 STUDY BACKGROUND AND OBJECTIVES

As the most frequent Internet users in the world, it is important for Canadians to have a strong understanding of – and dedication to – cyber security and safety. This includes knowing how to identify an online threat, knowing the actions that should be taken to combat these threats, knowing where to find reliable information about how to stay safe online, and a commitment to protecting identities and safeguarding Internet-enabled devices. It is for this reason that Canada's Cyber Security Strategy includes assessing public awareness and engagement with cyber security, as well as implementing the Get Cyber Safe public awareness campaign, which aims to boost general knowledge and understanding.

The objectives of the research were as follows:

- Assess performance of the public awareness campaign and help identify shifts in knowledge, behaviours, and attitudes.
- Track campaign target audience(s) for the public awareness campaign.
- Identify and track motivators and barriers to behaviour change (for those who have taken action, what prompted them to do so, for those who have not, why not?).
- Identify and track the best ways of communicating such information.
- Track public expectations in terms of the involvement of the federal, provincial, and municipal governments, as well as non-governmental agencies.

1.1 METHODOLOGY

a) Survey

The sample consists of 2,072 completed interviews with Canadians 18 years of age or older who use the Internet on a regular basis, including more than 300 interviews with youth between the ages of 16 and 24, and 300 with Canadians who own or act in a managerial position in a small- to medium-sized business employing between one and 100 individuals. The sample is based on a random selection of Prob*it* panel members from across the country. Prob*it* panellists were selected using a random-digit dial (RDD) landline-cell phone hybrid sample frame. This is the same sample frame and sampling process used to conduct telephone surveys, which are considered to be representative of the population. Once selected, they are contacted and recruited by telephone and asked to complete a basic profile (i.e. base survey instrument) including a range of demographic information about themselves. They are also asked if they would prefer to complete surveys online or by telephone. All sample members are eligible to participate, including those with cell phones only, those with no Internet access and those who simply prefer to respond by telephone rather than online. This panel represents a fully representative sample of Canadians, from which we can draw random samples and collect data in a more cost conscious and timely manner than would otherwise be possible in a traditional telephone survey. This panel of more than 95,000 individuals can be considered representative of the general public in Canada (meaning that the incidence of a given target population within our panel very closely resembles the public at large) and margins of error can be applied.

In this survey, a sample of 16,178 was drawn from the online only portion of the Prob*it* panel and survey cases completed online only, since this is the specific portion of the Canadian public that would be targeted by the communications campaign. The participation rate was 15 per cent[1]. The final survey sample of 2,072 yields a level of precision of +/-2.2 per cent for the sample overall and +/-3 to 6 per cent for most sub-groups that could be isolated in the analysis (including all regions, age, education, and income segments).

Prior to conducting the survey, the instrument was tested with 16 cases in English and 10 cases in French. Additional questions were placed on the pretest version of the questionnaire asking about length, flow, clarity of wording and so on to elicit feedback from respondents. Minimal changes were made as a result of the testing, although a few questions were removed in order to reduce the survey length.

The survey was administered between August 21 and September 5, 2018, using a bilingual questionnaire, installed on a secure web-server controlled by EKOS. The email invitation included a description and purpose of the survey (in both languages) along with a link to the survey website. The survey database was mounted using a Personalized Identification Number (PIN), so only individuals with a PIN were allowed access to the survey (the PIN was included in the email invitation). The questionnaire was prefaced with a brief introduction to the study and rationale for the research. The voluntary and confidential nature of the survey was also emphasized. Survey data collection adhered to all applicable industry standards. All invited panel members were informed of their rights under current Privacy legislation, as well as how to obtain a copy of their response and results of the survey.

[1] Among the sample of 16,178 cases, 596 bounced as undeliverable (15,582 valid sample) and 260 were screened out as out of scope.

The database was reviewed following data collection for data quality, outliers, coding requirements, weighting and construction of independent variables, and was used to explore sub-group patterns (e.g., by age, gender and so on) in the analysis. Weighting of the sample was based on population parameters according to the latest Census on age, gender and region of the country.

The following table presents a profile for the sample. This includes the unweighted distribution of demographic characteristics related to region, gender, and age (used in weighting the data), and weighted distribution for presence of children in the home, and ages of children, whether they were born in Canada, current household composition, level of education and annual household income, as well as mother tongue.

Table 1: Demographic Table

Table 1a: Province / Territory (unweighted)

--	Total
n=	*2072*
British Columbia and Yukon	13%
Alberta and Northwest Territories	10%
Saskatchewan and Manitoba	6%
Ontario	33%
Quebec and Nunavut	23%
Atlantic	10%

Table 1b: Gender (unweighted)

--	Total
Male	48%
Female	52%

Table 1c: Age (unweighted)

--	Total
16-24	15%
25-34	11%
35-44	17%
45-54	20%
55-64	20%
65 up	15%

Table 1d: Children under the age of 18 in the home

--	Total
n=	*2072*
Yes	26%
No	74%
Prefer not to say	0%

Table 1e: Age of children in the home

--	Total
n=	*2072*
Under 6	22%
6 to 11	23%
11 to 15	27%
16 or older	17%
Prefer not to say	11%

Table 1f: Born in Canada

--	Total
n=	2072
Yes	86%
No	13%
Prefer not to say	1%

Table 1g: Level of education completed

--	Total
n=	2072
High school or less	12%
Some post secondary	12%
College, vocational or trade certificate or diploma	27%
Undergraduate university degree	29%
Graduate or professional degree	19%
Prefer not to say	1%

Table 1h: Annual household income

--	Total
n=	2072
<$20,000	6%
$20,000-$39,999	11%
$40,000-$59,999	14%
$60,000-$79,999	13%
$80,000-$99,999	13%
$100,000-$149,999	17%
$150,000 or more	12%
Don't know/No response	14%

Table 1i: Mother Tongue

--	Total
n=	2072
English	73%
French	20%
Other	7%
Prefer not to say	1%

A comparison of each unweighted sample with 2016 Census figures from Statistics Canada suggests there are similar sources of systematic sample bias in each survey, following patterns typically found in most general public surveys. There is a more educated sample in each survey than found in the population with 48 per cent reporting university degrees in the survey compared with 25 per cent in the population. Households with children under the age of 18 are also under represented in each sample (26 per cent compared with 35 per cent in the population). There is also an under representation of Canadians born outside of Canada in each survey (13 per cent in both the baseline and post-campaign versus 27 per cent in the population). As previously described, each sample was weighted by age, gender, and region.

b) Focus Groups

In order to add further context and understanding to the survey results, as well as gather reaction to the Get Cyber Safe website, eight focus groups were held in four Canadian cities (Montreal (2), Toronto (2), Calgary, (2), and Halifax (2). In each centre one session was held with the general public, across all age cohorts. In Montreal and Toronto the other session was held with those under 30 years of age. In Calgary and Halifax, the other session was held with small and medium business owners or employees (i.e., in organizations with fewer than 100 employees). Both groups in Montreal were conducted in French. All others were conducted in English. A recruitment screener can be found in Appendix A. Groups were stratified to ensure a balance of males and females, and mix across age cohorts. In total, 67 individuals participated in the discussions. A focus group guide (provided in Appendix B) was developed by EKOS in consultation with the client. The discussions explored awareness, concerns and steps taken regarding mitigation of risk of online threats, as well as information sources used, and need for information on the topic. Reaction was also gathered to the main page of the website as well as an infographic and a Facebook ad.

Each focus group was 90 minutes in duration. Groups were held in professional focus group facilities. Refreshments were provided and participants were provided $85 for their attendance. Video or audio recordings, researchers' notes and observations from the focus groups formed the basis for analysis and reporting of results.

It should be kept in mind when reading this report that findings from the focus groups are qualitative in nature, designed to provide a richer context rather than to measure percentages of the target population. These results are not intended to be used to estimate the numeric proportion or number of individuals in the population who hold a particular opinion as they are not statistically projectable.

2. Use of Devices and the Internet

Chapter 2 establishes the level of use and general sophistication of Canadians who are online, including their use of computer and other devices to access the Internet, their frequency of use and proficiency with computers and other technology, as well as their level of online activity. Canadians are very active online, using an increasing variety of devices and generally at a high level of sophistication regarding use of technology.

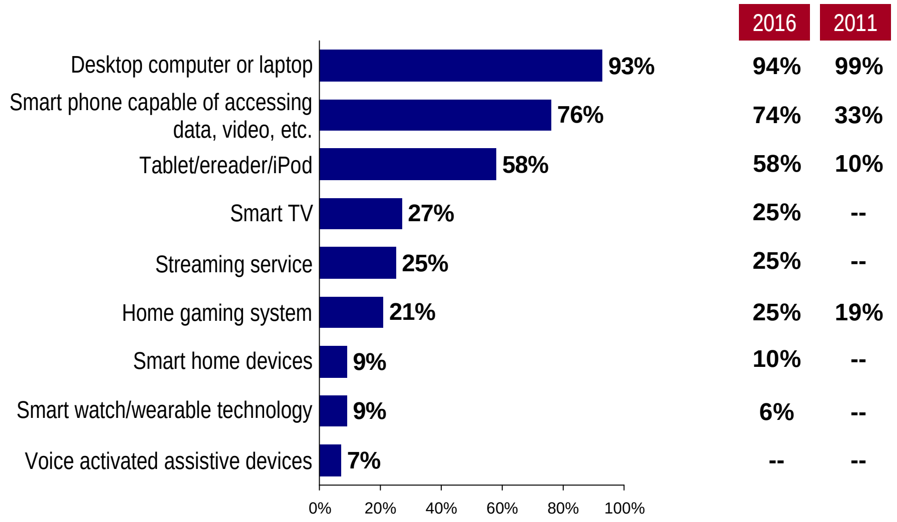
2.1 Internet-Enabled Devices Used

Consistent with 2016 results, desktop or laptop computers are used for accessing the Internet for personal use by nearly all Canadians who are online (93 per cent). Three-quarters of Canadians online (76 per cent) use a smartphone capable of accessing data. This finding is consistent with 2016, but represents is a vast increase from the 2011 results where only one-third (33 per cent) indicated they use a smartphone such as an iPhone or BlackBerry to access the Internet for personal use[2]. Over half of Canadians (58 per cent) use tablets (including iPods and e-readers) to access the Internet (consistent with 2016, but more than a five-fold increase over 2011). One-quarter use a smart TV (27 per cent), a streaming service (25 per cent), or a home gaming systems such as Sony Playstation or Microsoft Xbox (21 per cent, a slight decrease from 25 per cent in 2011). One in ten use smart home devices (nine per cent) or a smart watch or other wearable technology (nine per cent). Seven per cent use voice activated assistive devices to access the Internet.

[2] An additional 10 per cent said they use a mobile phone with basic Internet access in 2011; a category not offered in 2016.

Chart 1: Internet-Enabled Devices Used

"What kinds of devices do you use to access the internet for personal use?"



EKOS Research Associates Inc.

n=2072

PS Cyber Security Survey, 2018

- Those under 25 are less apt than older cohorts to report using desktop computers or laptops, as well as tablets, e-readers, or iPods. Younger Canadians (under 55) are more likely to use smartphones and home gaming systems to access the Internet. Canadians ages 25 to 44 are more likely than other age groups to use streaming services and those ages 35 to 54 are more likely to use smart TVs.

- Those in British Columbia and the prairies are more apt than Canadians in other regions to use smartphones to access the Internet for personal use. Residents of Quebec are less likely to access the Internet through smart TVs, streaming services, or home gaming systems.

- Men are more likely than women to report using smart TVs, streaming services, and home gaming systems to access the Internet.

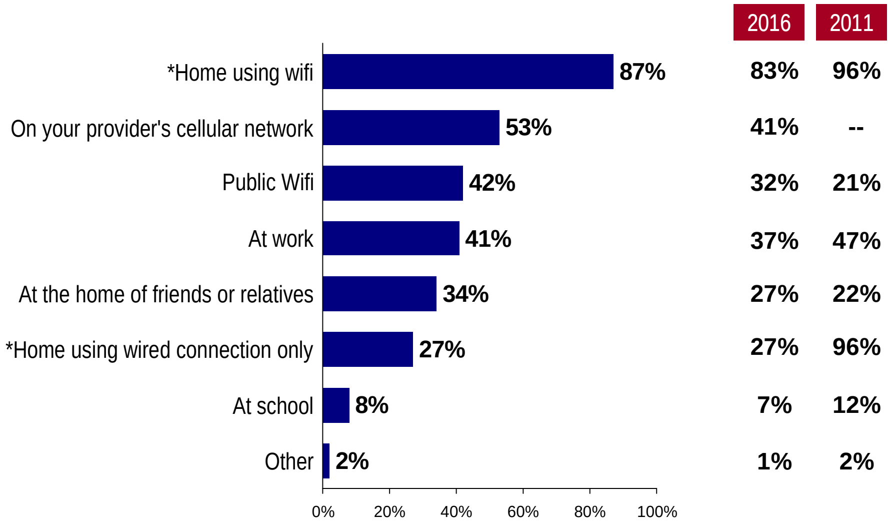
- The university-educated and those with higher income are generally more likely to report use of all devices.

2.2 PLACES TO ACCESS THE INTERNET

The vast majority households in the sample with Internet at home rely on a Wi-Fi network (87 per cent, up slightly from 83 per cent in 2016), while one-quarter (27 per cent) access the Internet from home using a wired connection only (unchanged from 2016). Canadians access the Internet through other means such as on their cellular network (53 per cent, up from 41 per cent), public Wi-Fi (42 per cent, up from 32 per cent), or at work (41 per cent, up slightly from 37 per cent). One-third (34 per cent, up from 27 per cent) access the Internet at the home of friends or relatives. One in ten Canadians (eight per cent) report accessing the Internet at school, but this figure rises to 54 per cent among those under 25 (up from 39 per cent in 2016).

Chart 2: Places to Access the Internet

“Where do you typically access the internet?”



* Both items were in same category in 2011

EKOS Research Associates Inc.

n=2072

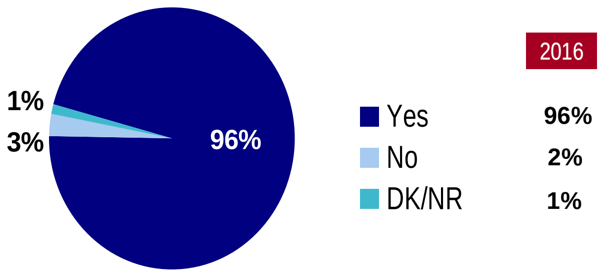
PS Cyber Security Survey, 2018

- Older Canadians (age 65 or older) are more likely than younger Canadians to rely primarily on a wired connection. Those ages 25 to 54 are more apt to access the Internet at home using Wi-Fi or at work. Those under 45 are most likely to use their provider's cellular network, public Wi-Fi, or a connection owned by a friend or family member.
- Men are more apt than women to access the Internet through a wired home connection, at work, or on their cellular network.
- Canadians reporting higher levels of education and income are more apt to access the Internet from home using Wi-Fi, from work, or on their provider's cellular network.

Canadians appear to be taking precautions to secure their home networks. Among Canadians with home Wi-Fi, nearly all (96 per cent) secure their network with a password, compared to just three per cent who do not. These results are consistent with those found in 2016.

Chart 3: Securing Home Wi-Fi

"Do you secure your home wifi with a password?"



EKOS Research Associates Inc. n=1801 PS Cyber Security Survey, 2018

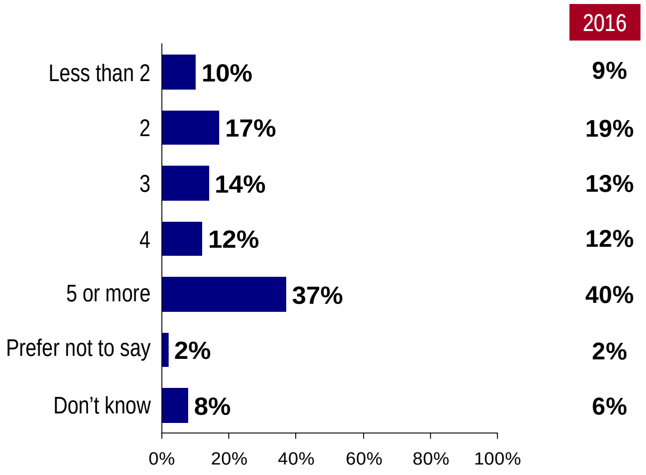
- Those over age 65 and over have a slightly lower propensity to use a password (seven per cent do not use a password).

2.3 USE OF COMPUTERS

Canadians spend an average of 4.9 hours online each day. Roughly two in five (37 per cent) report spending at least five hours online each day. Only one in ten Canadians (10 per cent) spend fewer than two hours online each day. One in six (17 per cent) spend two hours, 14 per cent indicate they spend three hours, and 12 per cent spend four hours online every day.

Chart 4: Extent of Online Activity

"How many hours do you spend online each day?"



EKOS Research Associates Inc.

n=2072

PS Cyber Security Survey, 2018

- Younger Canadians spend much more time online than older Canadians. Those under age 25 spend an average of 7.2 hours each day online, and those aged 25-34 spend 6.5 hours online. Canadians aged 55-64 spend 4.1 hours online, while those 65 and over report spending the least amount of time at 3.3 hours on average.

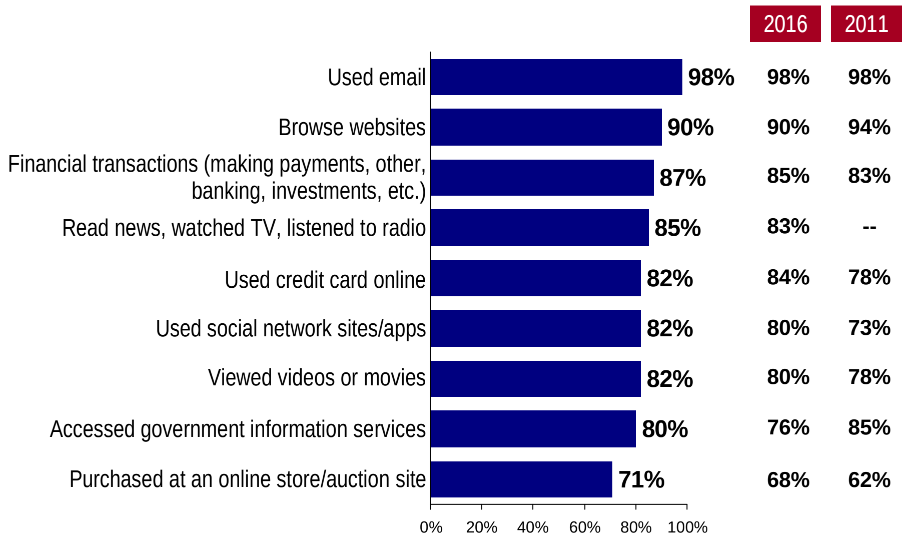
2.4 ONLINE ACTIVITIES

Although the means of accessing the Internet has changed somewhat over the past two years, online activities remain relatively similar. Canadians use the Internet for a wide variety of activities, with many citing five to six activities that they are involved in online. Email is the most common use of the Internet for Canadians, with 98 per cent saying they use the Internet for email. Nine in ten (90 per cent) Canadians cite browsing websites and generally surfing the Internet. More than eight in ten Canadians conduct financial transactions (87 per cent), consume news, television, or radio (85 per cent), use a credit card online (82 per cent), access social media (82 per cent), or view videos or movies (82 per cent) online. Eight in ten (80 per cent) have accessed government information services over the Internet (a slight increase from 76 per cent in 2016), while seven in ten (71 per cent) have conducted online shopping.

Six in ten Canadians have downloaded software (62 per cent), streamed or downloaded music or podcasts (61 per cent, a 10-point increase over 2016), or conducted telephone or video calls (58 per cent). About half have engaged in online gaming (51 per cent) or participated in online contests (47 per cent). Roughly four in ten have submitted applications (40 per cent), participated in blogs or online discussions (38 per cent), consumed an online training course (36 per cent), or used app-based services (35 per cent, up from 27 per cent in 2016).

Chart 5a: Online Activities

"Which of the following activities have you done over the Internet in the past year?"



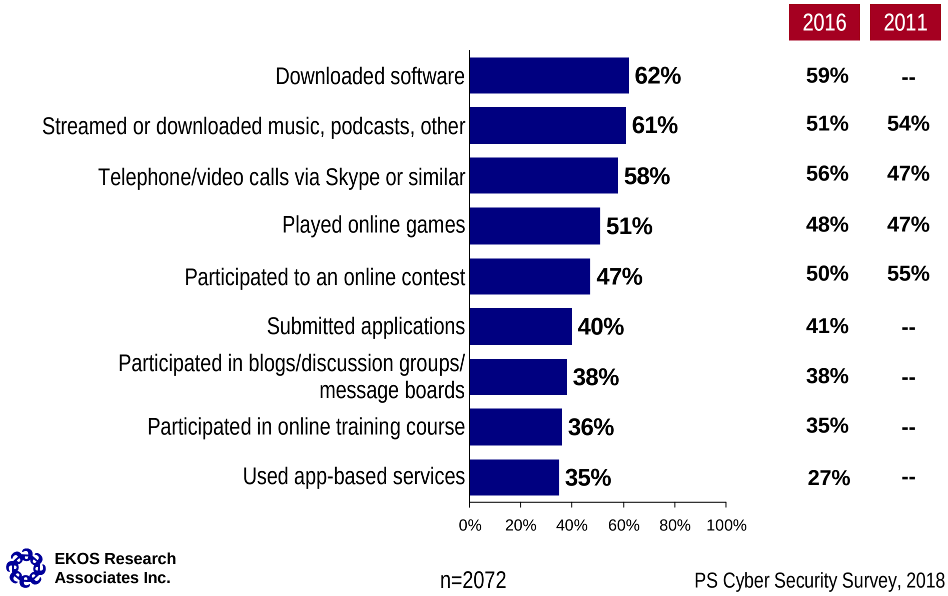
EKOS Research Associates Inc.

n=2072

PS Cyber Security Survey, 2018

Chart 5b: Online Activities

"Which of the following activities have you done over the Internet in the past year?"



n=2072

PS Cyber Security Survey, 2018

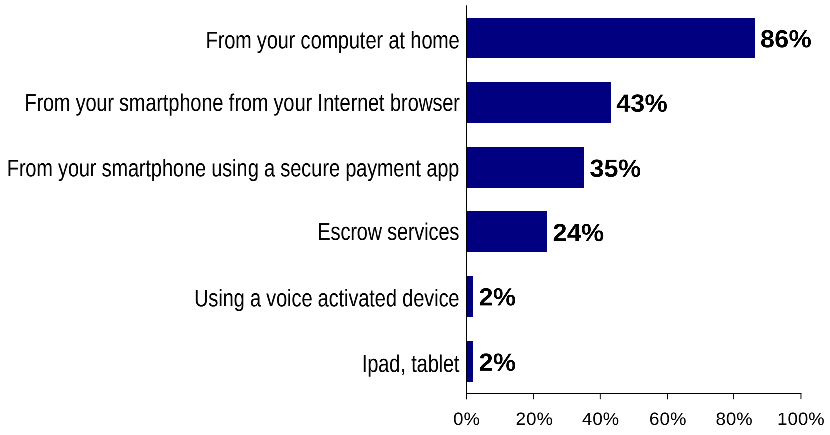
- There is a distinct generational divide between those who are more likely to use the Internet for these activities and those who do not. Canadians aged 55 and older are less likely to use the Internet for most of these activities, with the exception of email. Use of the Internet for most activities is more prevalent among Canadians under the age of 55. Those under the age of 25 are less likely to have used the Internet for commercial purposes (such as banking, using a credit card, or shopping), browsing websites, accessing government services, or reading news, watching television, and listening to radio.
- Men have a greater propensity to shop online, watch videos online, download software, stream or download music, use app-based services, participate in online discussions, or participate in online courses. Women are slightly more apt to use social networking sites.
- Those with higher incomes and higher education levels tend to use the Internet for most of these activities, with the exception of using email, online gaming, and online contests.
- Those in Quebec are more likely to participate in online contests, but they are less likely to engage in most of the other activities tested, with the exception of using email, financial transactions, social media, playing online games, and submitting applications.

2.5 Means Used to Conduct Transactions Online

Those respondents who indicated that they have engaged in financial matters online in the past year were asked to identify the means through which they conduct these transactions. The vast majority of these respondents (86 per cent) carry out these actions from a home computer. Roughly four in ten use their smartphone, either through a browser (43 per cent) or a secure payment app (35 per cent). One-quarter (24 per cent) rely on escrow services such as PayPal. A handful also use a voice-activated device (two per cent) or an iPad or tablet (two per cent).

Chart 6: Means Used to Conduct Transactions Online

"How do you usually do these transactions?"



EKOS Research Associates Inc.

n=1775; engage in financial transactions

PS Cyber Security Survey, 2018

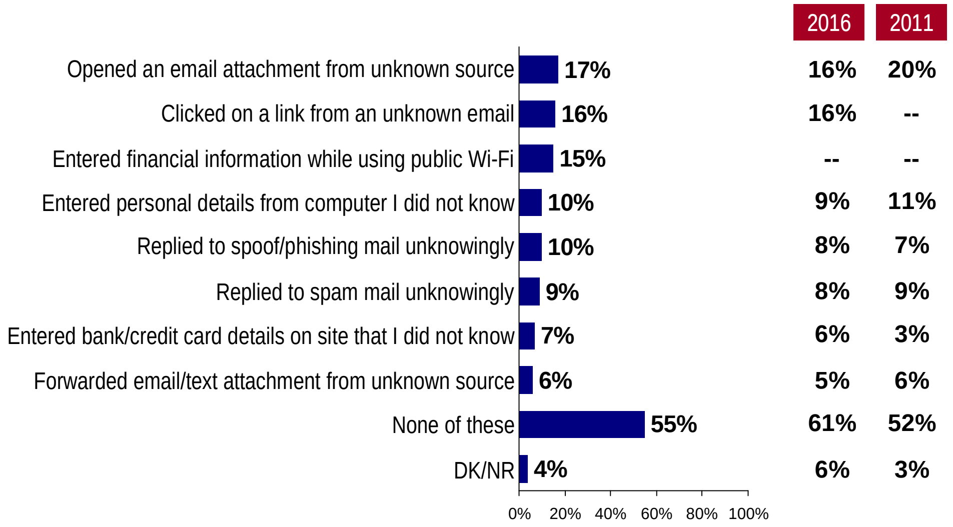
- Those ages 65 and over are more likely to conduct their transactions from a home computer. Those under the age of 45 are much more likely to rely on smartphones or escrow services.
- Men are slightly more likely to have used each of the media tested.
- University educated are somewhat more likely to use a home computer or a secure smartphone app, while high school educated are discernibly less likely to use a smartphone altogether. Those with higher income are more likely to use a smartphone.

2.6 Incidence of Risky Online Activities

Results suggest that a significant minority of Canadians participate in risky behaviour online. Just over half of Canadians (55 per cent) report that they have conducted none of the risky activities identified; a slight decrease from 61 per cent in 2016. One in six Canadians have opened an email attachment from an unknown source (17 per cent), clicked on a link from an unknown email (16 per cent), or entered financial information while using public Wi-Fi (15 per cent). About one in ten have entered personal details from a computer they did not know (10 per cent), replied to a phishing email unknowingly (10 per cent), replied to spam email unknowingly (nine per cent), entered bank details on an unfamiliar site (seven per cent), or forwarded an email attachment from an unknown source (six per cent). These results are generally consistent with those found in 2016.

Chart 7: Incidence of Risky Online Activities

"To your knowledge, have you ever done any of these things?"



EKOS Research Associates Inc.

n=2072

PS Cyber Security Survey, 2018

- Those under age 25 are more likely to have opened an email attachment from an unknown source, clicked on a link from an unknown email, or forwarded an email or text from an unknown source. Those under 35 are more apt to have entered personal details on a computer they did not know or entered banking information on a site they did not know was secure. Those under 45 are more likely to have entered financial information while using public Wi-Fi.

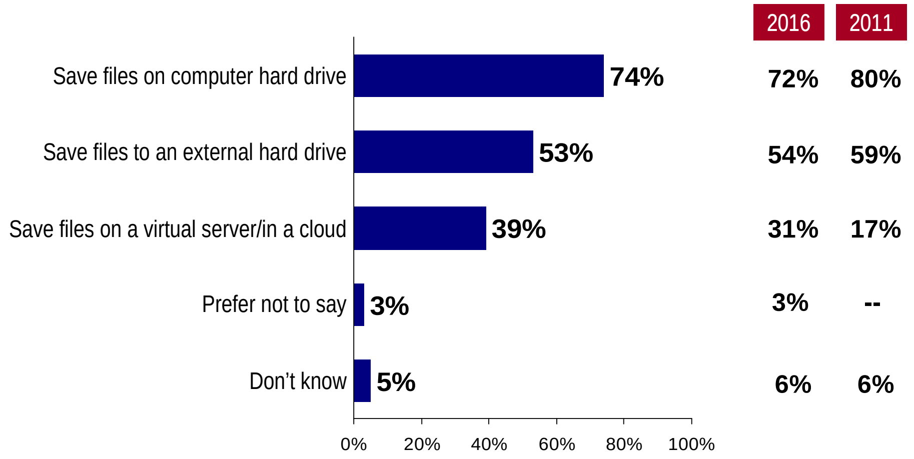
- Canadians with a university degree are more likely to have entered financial information while using public Wi-Fi or entered personal details on an unfamiliar computer. Those with a household income of $80,000 or more are more apt to have conducted entered financial information while using public Wi-Fi.

2.7 Data Storage

Most Canadians who are online (74 per cent, consistent with 2016 results) still use a computer hard drive to store information for personal use. About half (53 per cent) save files to an external hard drive. Four in ten (39 per cent) save files on a virtual server, an eight-point increase over 2016. Five per cent do not know how they save their data and three per cent prefer not to say.

Chart 8: Data Storage

"Thinking about data storage of information for personal use, do you save information on your computer hard drive, an external hard drive or on a "virtual server"?"



EKOS Research Associates Inc.   n=2072   PS Cyber Security Survey, 2018

- Education, age, income, and gender are strong predictors of whether any type of the above data storage options is used. Canadians in the 25 to 54 age cohort are more likely than other age groups to use any form of data storage. Men are more apt than women to use computer hard drives or external hard drives. Those with university education and those with at least $80,000 in annual household income are more likely to use each data storage method.

3. Level of Concern/ Importance

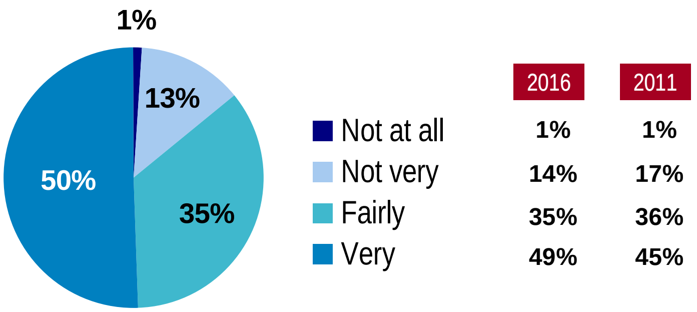
This chapter explores the perception of the problem of online threats among Canadians online. It examines the degree of threat they perceive, including the severity of consequences and their overall concern with online threats. Results show that Canadians who are engaged in online activities appreciate the threat that comes with use of the Internet, understand the issue and see the need for protective measures to address online security. That said, there is some evidence of distancing that takes place with some Canadians considering this as something that will not affect their own family.

3.1 Level of Concern Re: Online Threats

Canadians who are actively using the Internet are still very concerned about having their personal information obtained and used without permission as a result of their online activities. Half of respondents (50 per cent) are very concerned about online threats. An additional one-third (35 per cent) are fairly concerned about online threats. Very few (one per cent) would say they are not at all concerned about their personal information being fraudulently obtained online.

Chart 9: Level of Concern Regarding Online Threats

“Canadians have expressed a wide range of views regarding their ability to protect their personal information when going online. Some are quite concerned and others are not concerned. How concerned would you say that you are personally about your personal information being fraudulently obtained online and used for purposes of illegal activities?”



	2016	2011
■ Not at all	1%	1%
■ Not very	14%	17%
■ Fairly	35%	36%
■ Very	49%	45%

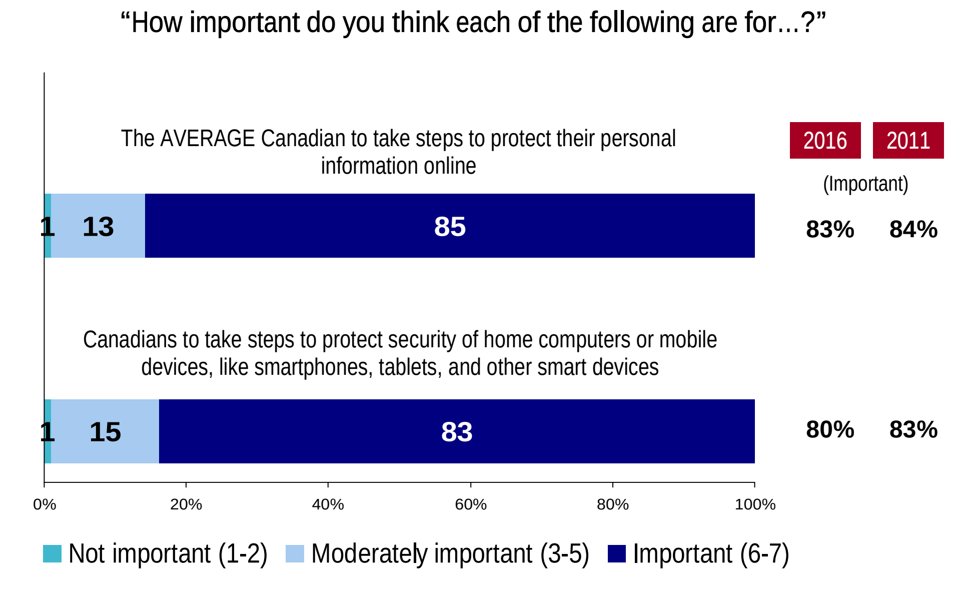
EKOS Research Associates Inc. n=2072 PS Cyber Security Survey, 2018

- Older Canadians (aged 55 and over) are more apt to be very concerned about online threats.
- Residents of Quebec and the Prairies are comparatively less likely to say they are very concerned.

3.2 Importance of Protecting Against Online Threats

Canadians continue to feel it is important to protect themselves against online threats. Mirroring the levels of concern found in 2011 and 2016, more than eight in ten state that it is important for the average Canadian to take steps to protect their personal information online (85 per cent) or to protect the security of home computers and mobile devices (83 per cent).

Chart 10: Importance of Protecting Against Online Threats



EKOS Research Associates Inc.

n=2072

PS Cyber Security Survey, 2018

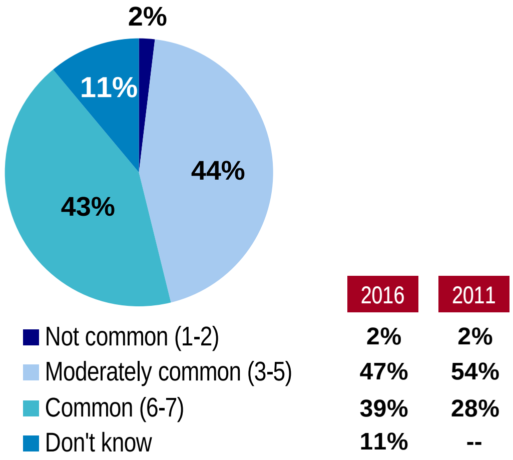
- The perceived importance of taking steps to protect the security of home computers or mobile devices is greatest among Canadians aged 45 and older. Those under 25 are less likely to say it is very important that average Canadians take steps to protect their personal information.

3.3 PERCEIVED PERVASIVENESS OF ONLINE THREATS

Canadians increasingly perceive online threats to be fairly pervasive. Roughly four in ten (43 per cent) feel that it is common for Canadians to be affected by online threats, which is a steady increase from 28 per cent reported in 2011. Roughly the same proportion (44 per cent) indicated that online threats are moderately common. Two per cent believe that online threats are not common.

Chart 11: Perceived Pervasiveness of Online Threats

"How common is it for Canadians to be affected by online threats?"



	2016	2011
■ Not common (1-2)	**2%**	**2%**
■ Moderately common (3-5)	**47%**	**54%**
■ Common (6-7)	**39%**	**28%**
■ Don't know	**11%**	**--**

EKOS Research Associates Inc. n=2072 PS Cyber Security Survey, 2018

- Those ages 45 to 64 are somewhat more likely to say that online threats are very common.

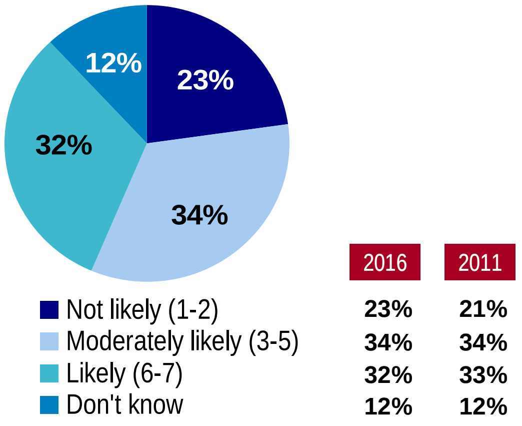
3.4 PERCEIVED LIKELIHOOD OF AN ONLINE THREAT

In comparison with the perceived pervasiveness of online threats overall, Canadians are less apt to think that they or anyone in their family will be affected by an online threat. As was the case in 2016, one in three (34 per cent) believe that they are likely to be personally affected by an online threat in the next year. Another one-third (33 per cent) feel that the likelihood of personally experiencing an online threat in the next two years is moderate, and one-quarter (23 per cent) believe that it is not likely that they will be affected by an online threat.

Of those who feel that the online threat is unlikely, most said that this is because they take steps to protect themselves online (73 per cent) or that they feel they do not participate in risky behaviour online (67 per cent), and two in five (42 per cent) think that the chances are just very small. A small proportion (six per cent) believe that online threats only apply to businesses and people with a lot of money.

Chart 12: Perceived Likelihood of Threat

"How likely is it that you or a family member will be affected by an online threat in the next 2 years?"

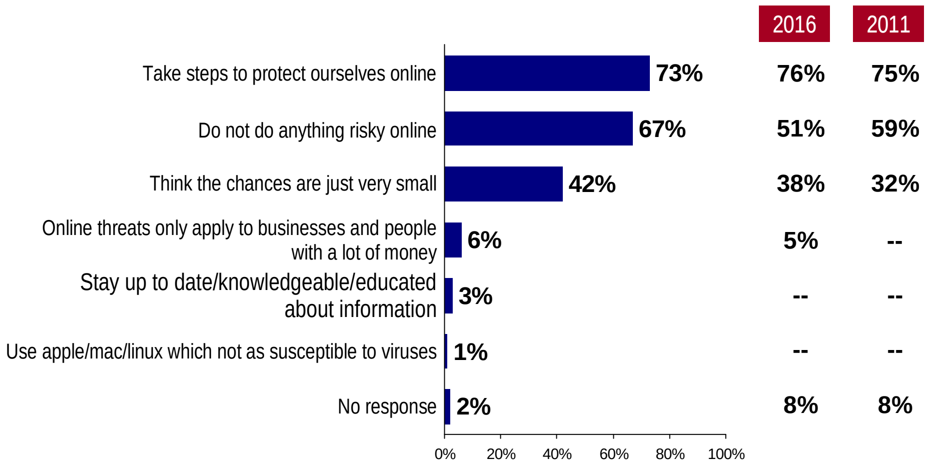


	2016	2011
Not likely (1-2)	23%	21%
Moderately likely (3-5)	34%	34%
Likely (6-7)	32%	33%
Don't know	12%	12%

EKOS Research Associates Inc. n=2072 PS Cyber Security Survey, 2018

Chart 13: Reasons for Dismissing Possibility of Online Threat

"Why don't you think that it is likely that you or your family will be affected by an online threat?"



EKOS Research Associates Inc.

n=492 (unlikely)

PS Cyber Security Survey, 2018

- Those under age 35 are more apt to see themselves or a family member being affected by an online threat as an unlikely occurrence.
- Men are somewhat more likely to see themselves or a family member being targeted in the next two years.

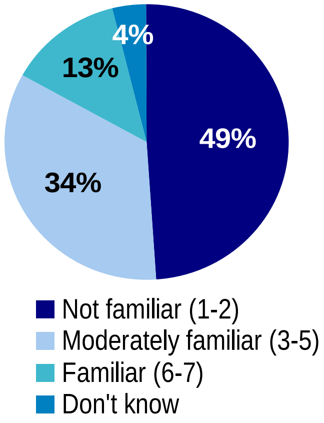
3.5 Crypto Currency

Results suggest fairly limited familiarity with crypto currency. Half of respondents (49 per cent) say they are not familiar with this medium of exchange, while one-third (34 per cent) are moderately familiarity. Just one in eight (13 per cent) would rate their familiarity as high.

Of those who are at least moderately familiar with crypto currency, relatively just one in ten (12 per cent) have made use of one. The vast majority of these respondents (86 per cent) have never purchased, traded, or used crypto currency.

Chart 14: Familiarity with Crypto Currency

"How familiar are you with the practice of purchasing crypto currency that can be used for online purchasing or trading?"



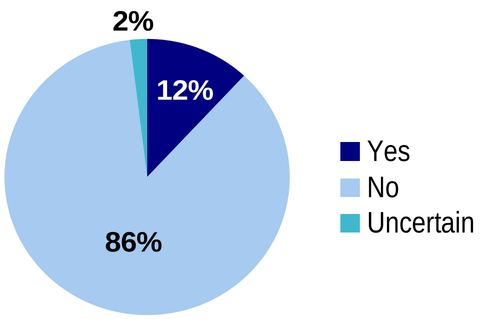
EKOS Research Associates Inc.

n=1036; half sample

PS Cyber Security Survey, 2018

Chart 15: Use of Crypto Currency

"Have you ever purchased, traded or used crypto currency for online purchases/activities?"



EKOS Research Associates Inc.

n=502; familiar with crypto currency (half sample)

PS Cyber Security Survey, 2018

- Self-rated familiarity with crypto currency declines steadily with age. Use of crypto currency is significantly higher among those under the age of 35, while it is virtually unheard of among those ages 55 and over.
- Compared to women, men are more likely to say they are very or moderately familiar with crypto currencies.
- University educated are more likely to see themselves as at least moderately familiar.
- Familiarity with crypto currency rises progressively with household income.

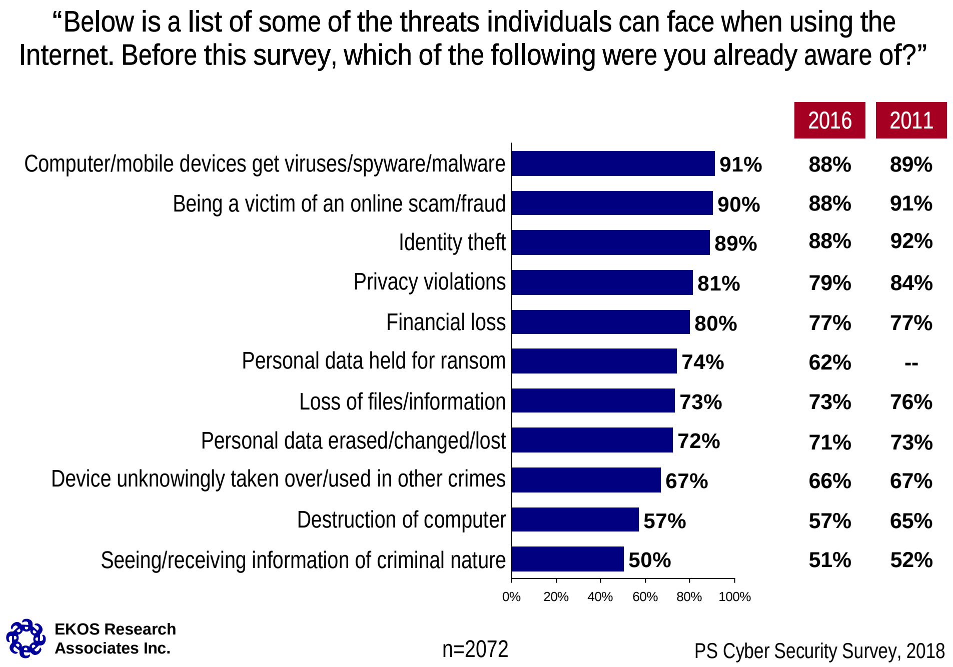
4. Familiarity

This chapter explores the level of knowledge that Canadians who are on the Internet have about online threats and steps to protect themselves from harm. Canadians are acutely aware of the multitude of online threats and precautions that can be taken. There is a relatively lower awareness of the means of determining if a website is secure.

4.1 Awareness of Online Threats

The majority of Canadians online are aware of the threats individuals can face when using the Internet. Similar to the awareness levels in 2016, nine out of ten Canadians are aware of spyware or malware on computer devices (91 per cent), being a victim of an online scam or fraud (90 per cent), and identity theft (89 per cent). Eight in ten are also familiar with privacy violations (81 per cent) and financial loss (80 per cent), while roughly three-quarters are familiar with personal data held for ransom (74 per cent, a 12-point increase over 2016), the loss of files or information (73 per cent), or personal data erased, changed, or lost (72 per cent). Two-thirds are aware of a device unknowingly being taken over or used in other crimes (67 per cent), while about six in ten are aware of the destruction of a computer (57 per cent). Half (50 per cent) are familiar with seeing and receiving information of a criminal nature.

Chart 16: Awareness of Online Threats



n=2072

PS Cyber Security Survey, 2018

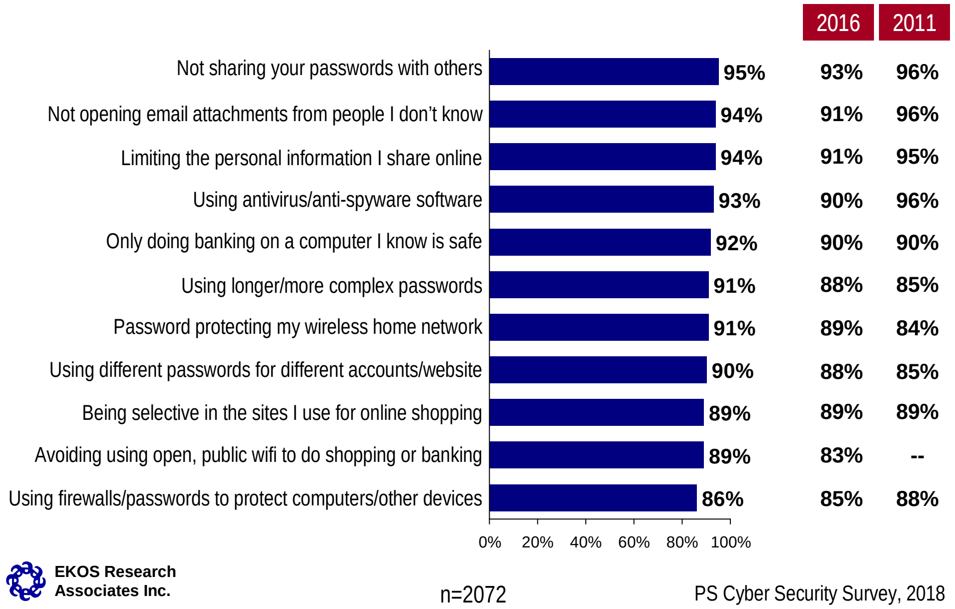
- Canadians aged 25 – 54 are more likely than others to say they are aware of each of these online threats.
- Residents of Quebec are consistently less likely to say they are familiar with these risks.
- Men are consistently as likely or more likely to say they are familiar with these threats.
- Those with higher income or education are consistently more likely to indicate they are already aware of each the online threats presented.

4.2 Awareness of Precautions

Results highlight a strong level of awareness regarding ways to reduce the chances of experiencing an online threat. More than nine in ten said that are aware of precautions that can be taken such as not sharing passwords (95 per cent), not opening email attachments from people they do not know (94 per cent), limiting the personal information they share online (94 per cent), and using anti-virus/anti-spyware software (93 per cent). Nine in ten say they know to do their banking on a computer they know is safe (92 per cent), use longer and more complex passwords (91 per cent), password protect their wireless home networks (91 per cent), use different passwords for different accounts and websites (90 per cent), choose online shopping sites carefully (89 per cent), and avoid using public Wi-Fi when conducting shopping and banking (89 per cent, up slightly from 83 per cent in 2016). Slightly fewer (86 per cent) say are familiar with using firewalls and passwords to protect their devices. Awareness is fairly consistent with results from 2016 and 2011, although use of longer/more complex passwords, password protecting home wireless network and use of different passwords for different accounts or websites seems to be steadily increasing since 2011. Avoidance of open, public wifi when conducting online shopping and banking is up since it was first asked in 2016.

Chart 17: Awareness of Precautions

"Below is a list of steps to reduce the chances of experiencing an online threat. Some people are aware of these threats, while others are not. Which of the following were you already aware of?"



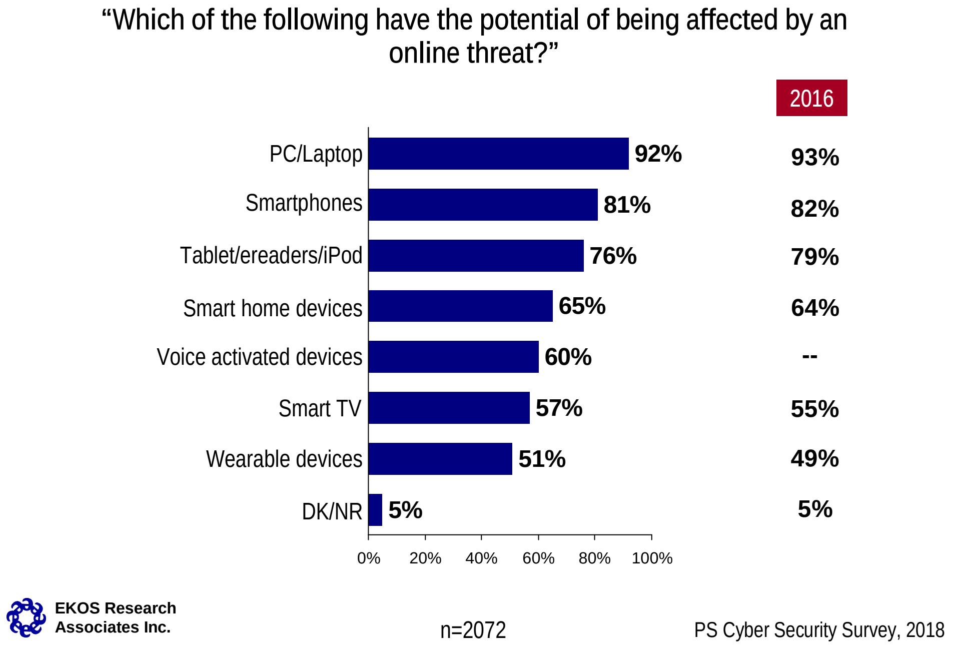
n=2072

PS Cyber Security Survey, 2018

- Canadians under the age of 25 are consistently less likely to say they are familiar with these precautions.
- Awareness of these precautions consistently increases with income and education.

Canadians are aware that the security of most devices can be threatened. Nine in ten respondents (92 per cent) believe that personal computers and laptops have the potential of being affected by an online threat. Roughly eight in ten see smartphones (81 per cent) and tablets or e-readers (76 per cent) as having the potential of being affected. Two-thirds (65 per cent) believe that smart home devices can also be affected, while about six in ten believe that voice activated devices (60 per cent) and smart TVs (57 per cent) can be targeted. Half (51 per cent) are aware of the potential threat to wearable devices. These results are consistent with those found in 2016.

Chart 18: Possible Devices Threatened


“Which of the following have the potential of being affected by an online threat?”

n=2072

PS Cyber Security Survey, 2018

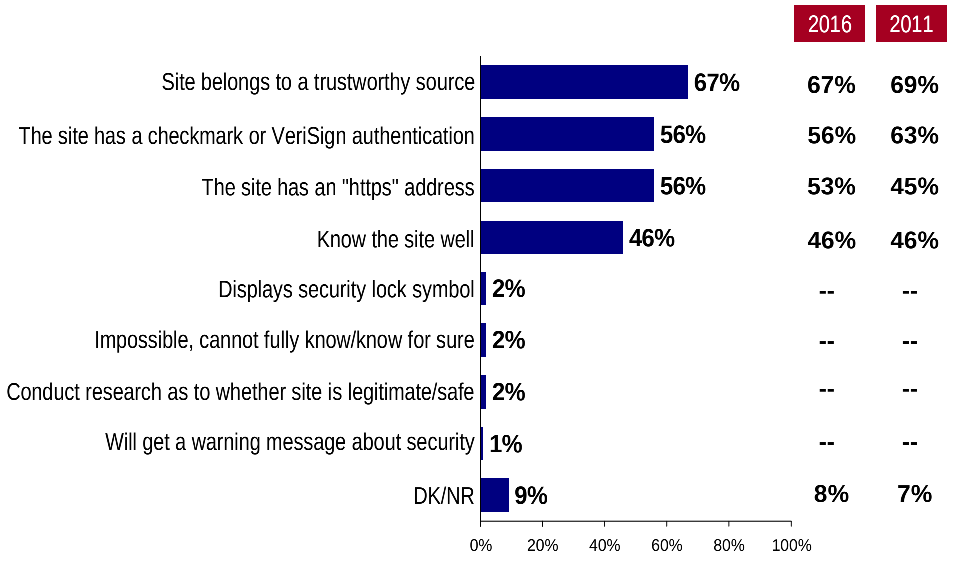
- Canadians aged 25 to 54, along with those with higher income and education, are more likely to be aware that most devices have the potential of being affected.
- Canadians perceive a threat for computers, tablets, and smartphones in fairly equal measure across regions. However, residents of Quebec are less likely to perceive smart home devices, voice activated devices, smart TVs, and wearable devices as at-risk.

4.3 Determining Secure Websites

Among those indicating that they do online banking, two-thirds of Canadians (67 per cent) say they can tell a website is secure when they know it belongs to a trustworthy source (such as a well-known service provider, software provider, government website, etc.). More than half determine that a website is secure if it has a checkmark or VeriSign authentication (56 per cent; 58 per cent including those describing a lock symbol, unprompted[3]) or has an "https" address (56 per cent). Just under half (46 per cent) determine that the website is secure if they know the site well. These results are consistent with those found in 2016.

Chart 19: Determining Secure Websites

"How can you tell if a website is secure?"



EKOS Research Associates Inc.

n=1880 (do online banking)

PS Cyber Security Survey, 2018

[3] The lock symbol described by a small number of individuals was not included in the initial list of response categories shown to respondents but coded from open responses following survey collection.

- Younger Canadians (under age 35) are more apt to feel a website is secure if it belongs to a trustworthy source. Those aged 25 to 44 are more apt than other age cohorts to feel a site with an “https” address or a checkmark or VeriSign authentication is secure.
- Regionally, residents of Quebec are less likely to identify a checkmark or VeriSign authentication or their personal familiarity with the website as signs as the website is secure.
- Those with a university education are more likely to cite an “https” address or a checkmark or VeriSign authentication.

5. Attitudes

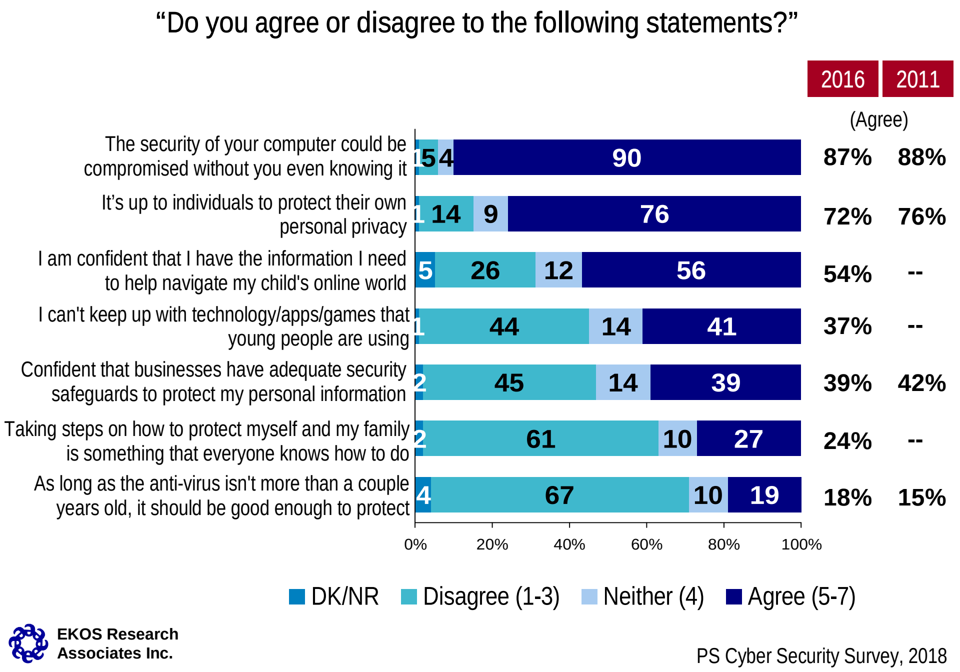
This chapter provides a picture of the attitudes of Canadians who are online with regard to online threats and the need to protect themselves. These results are an extension of Chapter 3, indicating that most Canadians are very aware of the threat and firmly believe that individuals need to take steps to ensure online security, though there are still some specific gaps in awareness.

5.1 Attitudes Regarding Online Threats

Similar to 2016 results, nine in ten Canadians (90 per cent) are aware that a computer can be compromised without an owner even knowing it. Canadians tend to feel that it is up to individuals to protect their own personal privacy, with three in four (76 per cent) agreeing with this statement (up slightly from 72 per cent in 2016 and consistent with 76 per cent in 2011).

Canadians have relatively low confidence regarding their ability to protect themselves from most online threats. Just over half of parents (56 percent) agree that they have the information they need to navigate their child's online world. Four in ten parents feel that they cannot keep up with technology that young people are using (41 per cent, a slight increase from 37 per cent in 2016). Four in ten Canadians agree that businesses have adequate security to safeguard their personal information (39 per cent). Canadians continue to feel more pessimistic about their ability to protect themselves online, with only 27 per cent agreeing that steps on how to protect themselves is something everyone knows how to do; 61 per cent disagree. One in five Canadians (19 per cent) incorrectly agree that as long as their anti-virus software is not more than a couple years old it should protect their computer.

Chart 20: Attitudes Regarding Online Threats



PS Cyber Security Survey, 2018

- Younger Canadians (under 25) are less likely to agree that the security of your computer can be compromised without you even knowing it. They are also more likely to agree that taking steps on how to protect from online threats is something that everyone knows how to do.

- Canadians with a university education are more apt to disagree that it is up to individuals to protect their own personal privacy.

- Younger Canadians, along with those with lower income, or living in Quebec, are more likely to be confident that businesses have adequate security safeguards to protect their personal information.

- Younger parents are more likely to disagree that they can't keep up with technology that young people are using.

- Younger Canadians are nearly twice as likely to agree that as long as the anti-virus software is up to date they are protected. Men are more apt than women to disagree.

6. PRECAUTIONS

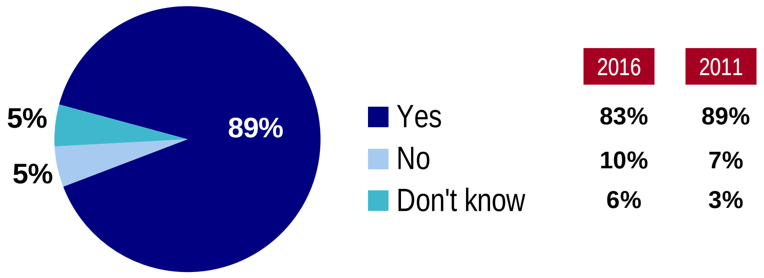
The current chapter focuses on the actual behaviour that Canadians online engage in to protect themselves from online threats. The survey results assist in understanding which segments of the online population are taking protective measures and which are not, and which are taking measures that are adequate.

6.1 REPORTED INCIDENCE OF PRECAUTIONS

Nine in ten Canadians (89 per cent) say that they are taking precautions to protect their computer and other devices they use to access the Internet, a six-point increase over 2016. Five per cent say they do not take any precautions to protect their device and five per cent are not sure.

Chart 21: Reported Incidence of Precautions

"Some people take precautions to protect their computer and other devices they use to access the Internet, while others do not. Do you take precautions to protect your devices?"



EKOS Research Associates Inc.

n=2072

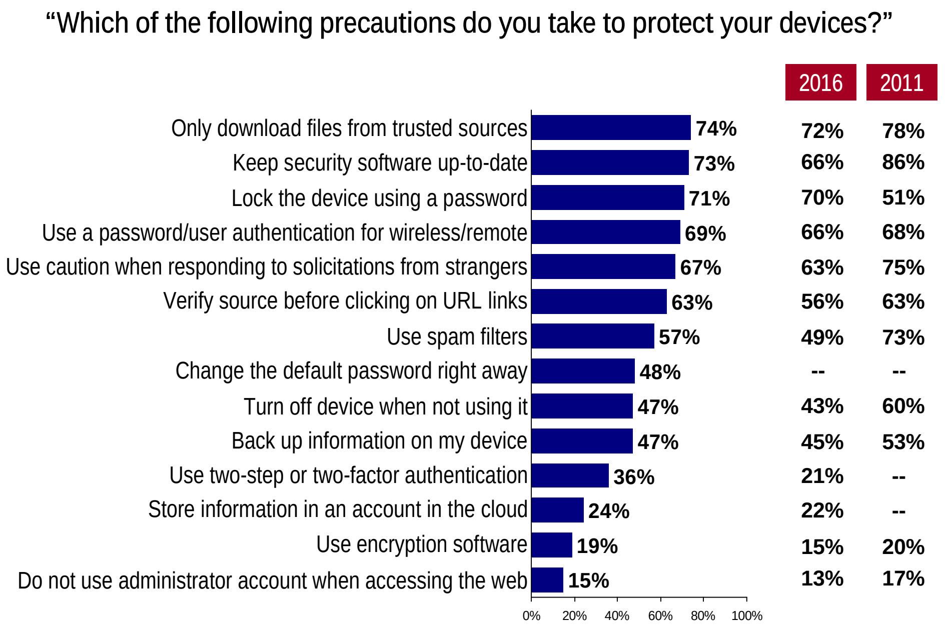
PS Cyber Security Survey, 2018

- Those under the age of 35 are most apt to say they do not take precautions.

6.2 Types of Precautions Taken (Device Protection)

Canadians also report a vast repertoire of precautions they take to protect their devices. Three-quarters report downloading only from trusted sources (74 per cent) and keeping security software up to date (73 per cent, up from 66 per cent in 2016). About seven in ten say they lock their devices using a password (71 per cent), password-protect their Wi-Fi (69 per cent), and use caution when responding to solicitation from strangers (67 per cent, up from 63 per cent in 2016). Roughly six in ten verify a URL link's source before clicking on it (63 per cent, up from 56 per cent) and use spam filters (57 per cent, up from 49 per cent). About half report changing default passwords right away (48 per cent), turning off devices when not in use (47 per cent, up from 43 per cent), and backing up information in their devices (47 per cent). One-third use two-step authentication (36 per cent, a 15-point jump over 2016), while one-quarter (24 per cent) store information in a cloud service. One in five report using encryption software (19 per cent, up from 15 per cent) and 15 per cent do not use an administrator account when accessing the web.

Chart 22: Types of Precautions Taken (Device Protection)



EKOS Research Associates Inc.

n=2072

PS Cyber Security Survey, 2018

- Older Canadians ages 55 and over are more likely to keep their security software up-to-date and turn off their devices when not in use. Those who are 25 to 44 are more apt to use most of the other tactics tested.
- Those who reside in British Columbia are more likely to change their default passwords immediately and use two-step authentication. Those who live in Quebec are less likely to download files exclusively from a trusted source, use spam filters, back up information on their devices, use two-step authentication, or change their default passwords immediately.
- Men are more likely than women to report keeping their security software up-to-date, backing up information on their devices, using two-step authentication, and using encryption software.
- Overall, those with higher income and education tend to be more likely to take precautions to protect their computer and other devices.

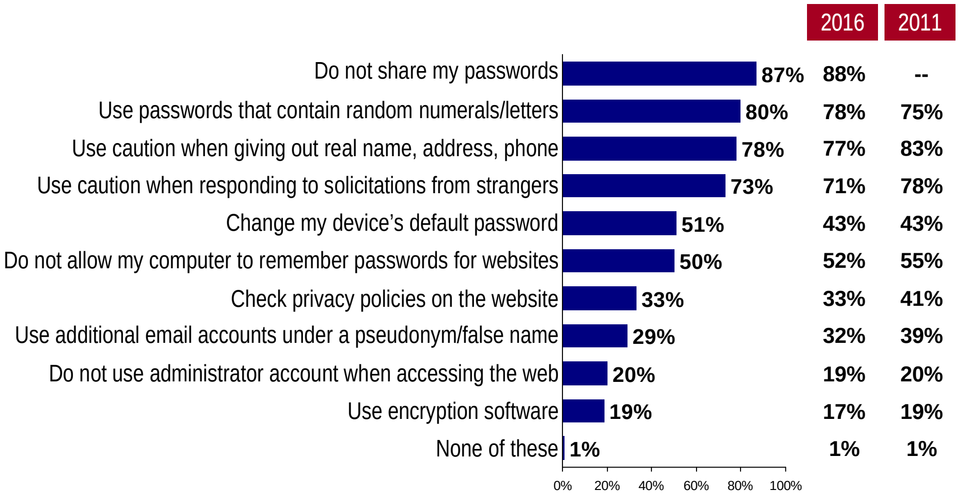
6.3 TYPES OF PRECAUTIONS TAKEN (ONLINE THREATS)

Most Canadians take some sort of precaution to protect their personal information from online threats. Results are largely consistent with those found in 2016. Roughly nine in ten (87 per cent) say they do not share their passwords. Eight in ten use passwords that contain random numbers and letters (80 per cent) or use caution when giving out information like their real name, address, or phone number (78 per cent). About seven in ten (73 per cent) use caution when responding to solicitations from strangers. Half change their default passwords (51 per cent, up from 43 per cent in 2016) or do not allow their computer to remember passwords for websites (50 per cent).

About three in ten check privacy policies on the website (33 per cent) or use additional email accounts under a pseudonym (29 per cent). Precautions used least often include not using an administrator account when accessing the web (20 per cent) and using encryption software (19 per cent).

Chart 23: Types of Precautions Taken (Online Threats)

"Which of the following precautions do you take to protect yourself against online threats and to protect your personal information?"



EKOS Research Associates Inc.

n=2072

PS Cyber Security Survey, 2018

- Canadians between the ages 25 to 44 are more apt to change their default passwords, use additional email account under a pseudonym, and use encryption software. Those ages 55 to 64 are more likely to refrain from using administrator accounts when accessing the web. Those under the age of 25 are consistently less likely to take most of the precautions examined. Those ages 55 and up are also comparatively less likely to chance their default passwords or use additional email accounts under a pseudonym.

- Regionally, Quebec residents are more likely to say they do not allow their browser to remember passwords.

- Compared to women, men are more likely to change their default passwords, use additional email accounts under a pseudonym, and use encryption software. In contrast, women are more apt to refrain from storing passwords in their browser.

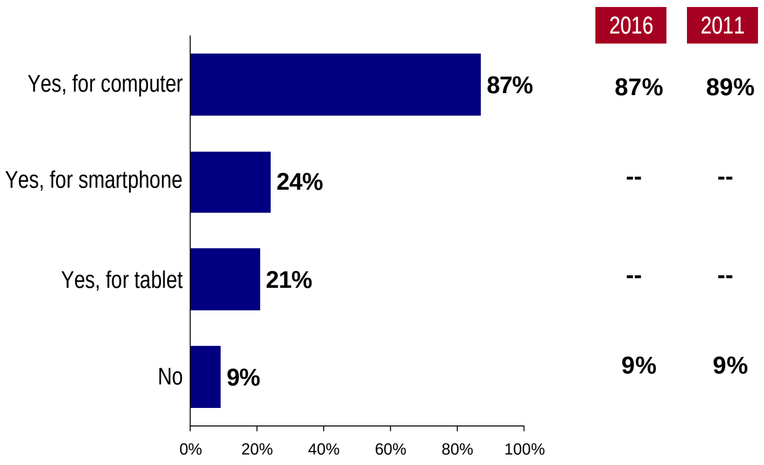
- Those with a university degree and those with higher income levels are more apt to report using most of these precautions.

6.4 USE OF ANTI-VIRUS SOFTWARE

Consistent with findings from previous iterations of the survey, the vast majority of respondents (87 per cent) have anti-virus software on their computer. Respondents appear take a less cautious approach with their mobile devices, however. Just one-quarter (24 per cent) have anti-virus software for their smartphone and one-fifth (21 per cent) have it for their tablet.

Chart 24: Use of Anti-Virus Software

"Do you have anti-virus software on your computer, smartphone or tablet?"



EKOS Research Associates Inc.

n=1907

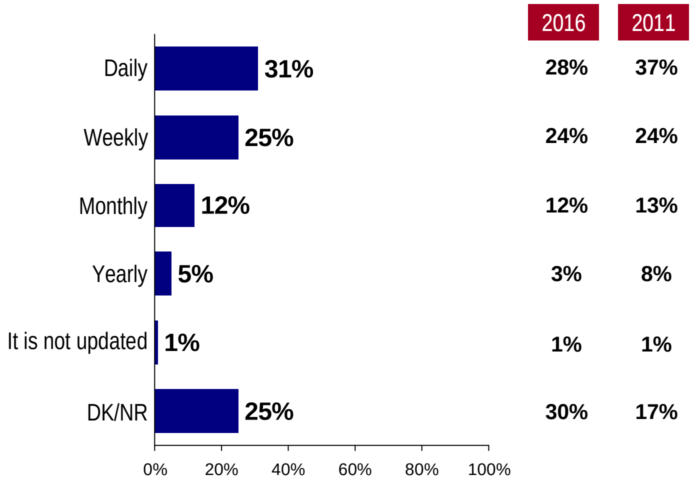
PS Cyber Security Survey, 2018

- Canadians under 45 are less apt to have anti-virus software on their computer, while older Canadians report this much more frequently.

Results suggest that three in ten Canadians (31 per cent) update their anti-virus software on a daily basis (either manually or automatically), while one-quarter (25 per cent) do so weekly. One in eight (12 per cent) update their software on a monthly basis, while one in twenty (five per cent) do so on an annual basis. One-quarter (25 per cent) are not sure how frequently their anti-virus software is updated. These results are consistent with those from 2016.

Chart 25: Timing of Updates

[IF YES] "How often is the anti-virus software on your computer, smartphone or tablet updated (by you or automatically) to the latest version?"



n=1653 (have anti-virus software on computer)

EKOS Research Associates Inc.

PS Cyber Security Survey, 2018

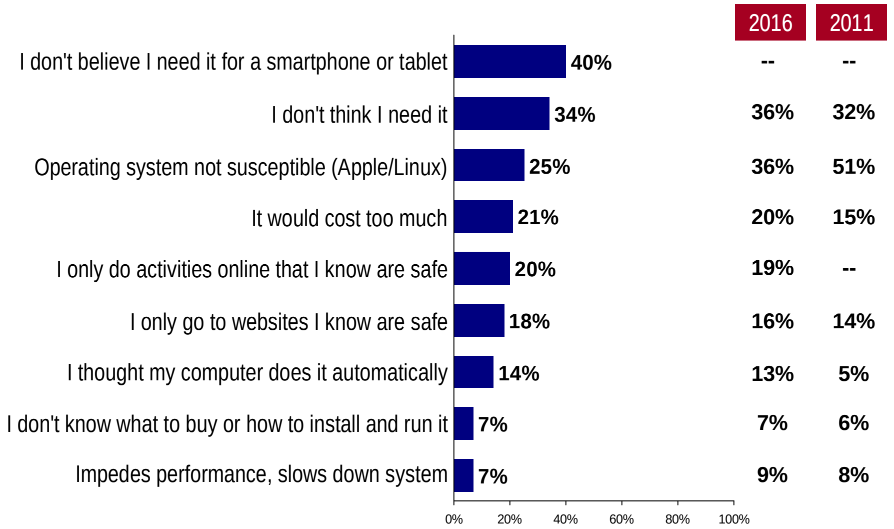
- Those under the age of 25 tend to wait longer to update their anti-virus software, while those ages 45 to 64 are more likely to update their software on a daily basis.
- Men are significantly more likely to say they update their anti-virus software on a daily basis, while women are more apt to say they do not know how often their software is updated.

6.5 Reasons for Lack of Anti-Virus Software

Canadians who do not have anti-virus software on their computer were asked to identify the reasons from a list of options. Results are largely consistent with those found in 2016. Four in ten (40 per cent) say they do not believe they need anti-virus software for a smartphone or tablet, while one in three feel they do not need it in general (34 per cent). One-quarter (25 per cent) say their operating system is not susceptible to viruses, an 11-point decrease from 2016. One in five feel it would cost too much (21 per cent), that they only do activities online that are safe (20 per cent), or only go to websites that are safe (18 per cent). One in seven believe that their computer checks for viruses automatically (14 per cent). A number of respondents also indicated that they do not know what to buy and install (seven per cent), they are concerned that anti-virus software will impede the performance of their device (seven per cent), or they believe anti-virus software is ineffective (five per cent).

Chart 26a: Reasons for Lack of Anti-Virus Software

[IF NO] "People have a number of different reasons for not having anti-virus software. What is the reason that you don't have anti-virus software?"



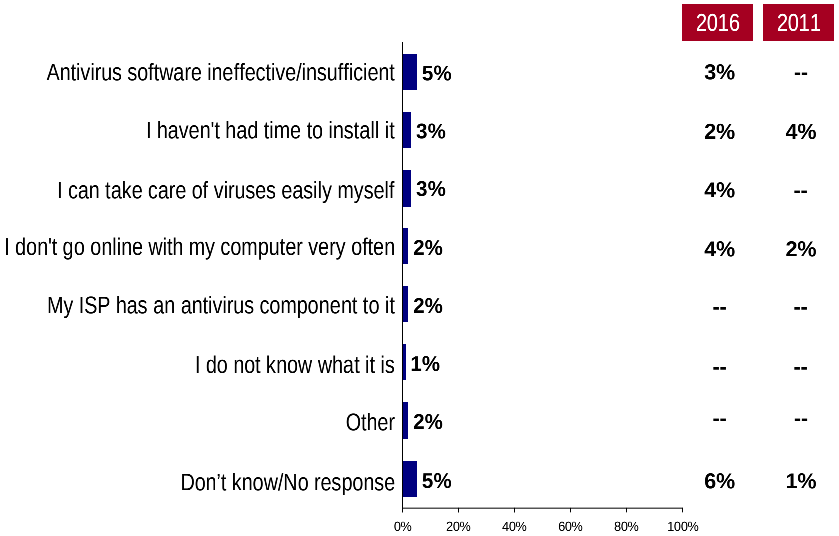
EKOS Research Associates Inc.

n=176; no anti-virus software

PS Cyber Security Survey, 2018

Chart 26b: Reasons for Lack of Anti-Virus Software

[IF NO] “People have a number of different reasons for not having anti-virus software. What is the reason that you don't have anti-virus software?”



EKOS Research Associates Inc.

n=176; no anti-virus software

PS Cyber Security Survey, 2018

6.6 Frequency of Changing Passwords Online

When asked about frequency of changing password on various types of accounts roughly one in six Canadians (15 to 18 per cent) said they never update any of their online accounts, and roughly the same proportion (14 to 23 per cent) update these accounts every few years. Roughly one in ten update passwords for their online accounts once a year (11 to 12 per cent) or a few times a year (10 to 12 per cent). Just six to seven per cent update their passwords more often than a few times per year. About one in ten report updating their passwords when prompted (eight to 10 per cent) or whenever they think of it (eight to nine per cent). Six to seven per cent update their passwords only when they learn about security breach.

It is more common for Canadians to say it is not applicable for social media accounts (13 per cent) or online shopping accounts (15 per cent) than it is for email accounts (one per cent).

Table 2: Frequency of Changing Passwords

Many people use the same passwords for different accounts and devices, and many keep the same passwords over time. How often would you say you change a password in each of the following? (n=1050)

	Social media accounts	Online shopping accounts	Email accounts
Never	18%	15%	18%
Every few years	17%	14%	23%
Once a year	11%	12%	11%
A few times a year	10%	10%	12%
More often than a few times a year	6%	7%	7%
Whenever I am prompted to	8%	10%	10%
Whenever I think of it /no set pattern	8%	9%	9%
When I learn about a security breach	6%	6%	7%
Not applicable (don't have any)	13%	15%	1%
No response	3%	3%	2%

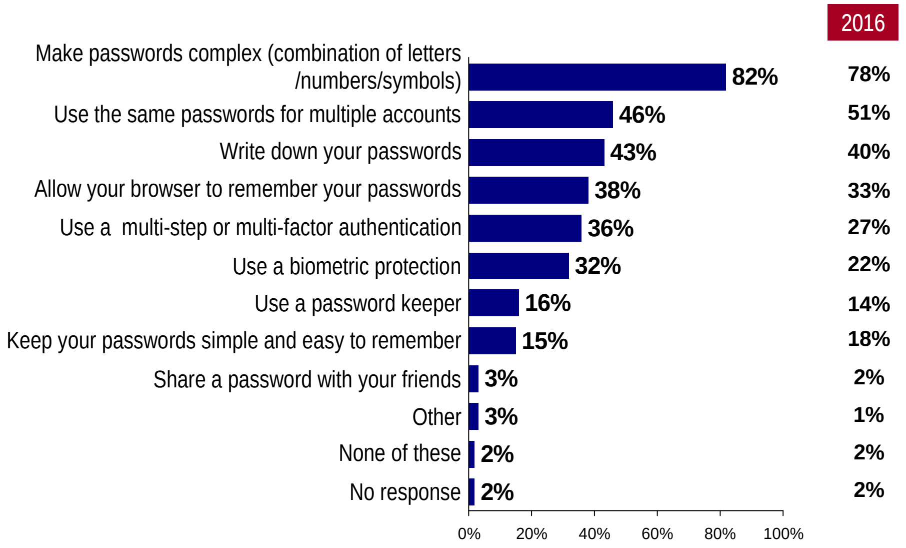
- Younger Canadians (under 25) are more likely to update passwords only when they hear of a security breach.

Canadians practice a variety of behaviours to safeguard their passwords. Eight in Canadians (82 per cent, up slightly from 78 per cent in 2016) attempt to make their passwords complex, and about one in three Canadians report using security practices such as two-step authentication (36 per cent, up from 27 per cent) or biometric protection (32 per cent, up from 22 per cent).

To help remember passwords, Canadians use the same password for multiple accounts (46 per cent, down slightly from 51 per cent), write down passwords (43 per cent), or allow a browser to remember their password (38 per cent, up from 33 per cent). Just one in six report using a password keeper (16 per cent) or using simple passwords (15 per cent). Only a small segment of the population share passwords with friends (three per cent).

Chart 27: Security Practices

"Which of the following do you do, if any?"



EKOS Research Associates Inc.

n=2072

PS Cyber Security Survey, 2018

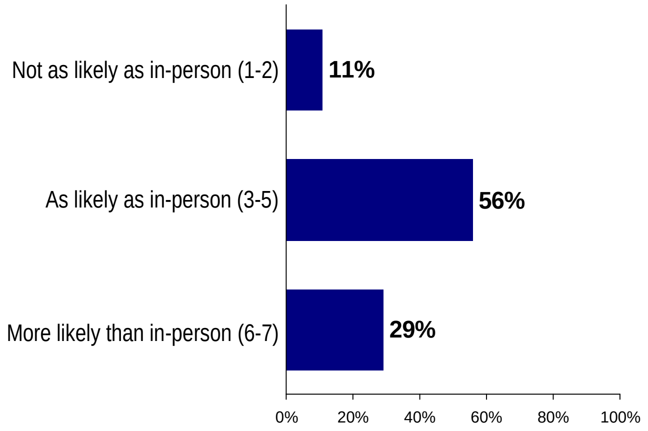
- Older Canadians (over 55) are more likely to write passwords down in order to remember them, while those ages 25 to 44 are more likely engage in each of the other behaviours tested.
- Quebec residents are more likely to write down passwords and less likely to use the same password for multiple accounts or allow a browser to remember their passwords.

- Those with a university education are more likely to practice each of the security procedures tested (i.e., complex passwords, two-step authentication, and biometric information). They are also more likely to use the same password for multiple accounts and allow their browser to save passwords.
- Those with lower household income levels are more likely to write down their passwords. Those with higher levels of income are more likely to report most of the behaviours examined including both beneficial and possibly detrimental behaviours.

Respondents were asked whether they apply the same level of caution against online threats as they do against in-person threats. One in ten (11 per cent) say they are less likely to take precautions against online threats when compared to in-person threats, while three in ten (29 per cent) are more likely to exercise caution in the digital world than the real world. Just over half (56 per cent) would exercise the same degree of care against both types of threats.

Chart 28: Likelihood of Taking Precautions against Online Threats vs. In-person Threats

"How likely are you to take precautions against online threats as you are to take precautions against "in-person" threats?



EKOS Research Associates Inc.

n=1036 (half sample)

PS Cyber Security Survey, 2018

- Those ages 55 and over are more likely to say they take more precautions online than in the real world.

7. Incidence of Victimization

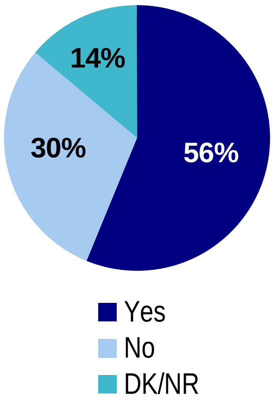
This chapter provides some evidence of the level of incidence of online threats. Perhaps more importantly, it also provides some understanding of the degree to which previous experience does (or does not) have an impact on changes in views about the likelihood of being affected or results in a change of protective behaviour.

7.1 Incidence and Impact of Computer Attack

Over half of Canadians (56 per cent) report having an incident of a virus, spyware or malware on their computer. Nearly one in three (30 per cent) did not have a computer attack, and 14 per cent say they are not sure.

Chart 29: Incidence of Computer Attack

"Have you ever had a virus, spyware or malware on your computer?"

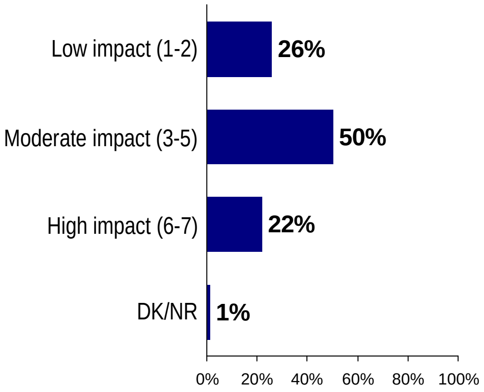


EKOS Research Associates Inc. n=1672 PS Cyber Security Survey, 2018

Of the 56 per cent who reported having a virus, spyware, or malware on their computer, one in five (22 per cent) indicate that the attack had a high impact. Half (50 per cent, compared to 57 per cent in 2016) say the impact was moderate, and one-quarter (26 per cent, compared to 20 per cent in 2016) indicate there was a low impact.

Chart 30: Impact of Computer Attack

[IF YES] "How much of an impact did this virus, spyware or malware have on you or your family?"



EKOS Research Associates Inc.

n=944

PS Cyber Security Survey, 2018

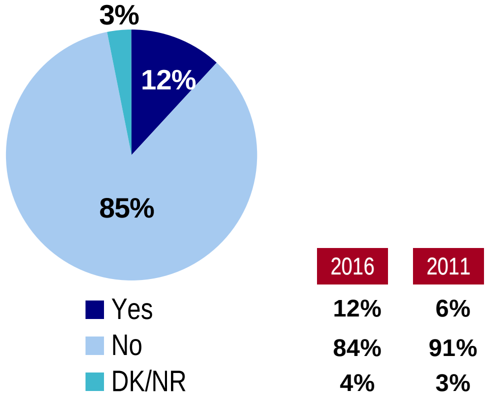
- Men are more likely than women to say they had a virus, spyware, or malware on their devices.
- Canadians on the prairies are more likely than those in other regions to say they had an attack, while also more likely to say the incident left little impact. Conversely, those in Quebec are least likely to report having an incident, but more likely to state that it had a large impact.
- Those with lower income ($40,000 or less) are more likely to say the attack had a large impact.

7.2 INCIDENCE AND IMPACT OF FINANCIAL LOSS

The portion of Canadians experiencing financial loss as a result of online activity has increased from six per cent in 2011 to 12 per cent in 2016 and 2018. Still, the majority, 85 per cent, state they have not had an incident of financial loss or fraud.

Chart 31: Incidence of Financial Loss

"Have you ever suffered financial loss or been the victim of financial fraud as a result of your online activity?"



EKOS Research Associates Inc.

n=2072

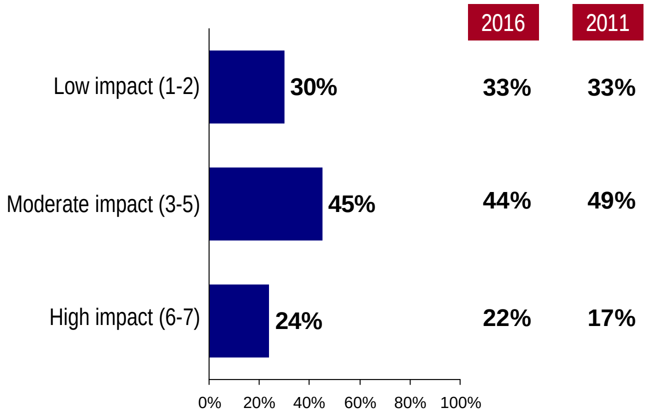
PS Cyber Security Survey, 2018

- Younger Canadians (ages 18 to 25) and those with lower income report experiencing financial loss more often than other Canadians.

One-quarter of respondents (24 per cent, up from 22 per cent in 2016 and 17 per cent in 2011) of those who experienced financial loss say that the fraud had a high impact. Less than half (45 per cent) indicate there was a moderate impact, and three in ten (30 per cent) say the impact was low.

Chart 32: Impact of Financial Loss

[IF YES] "How much of an impact did the financial fraud as a result of your online activity have on you or your family?"



EKOS Research Associates Inc.

n=274

PS Cyber Security Survey, 2018

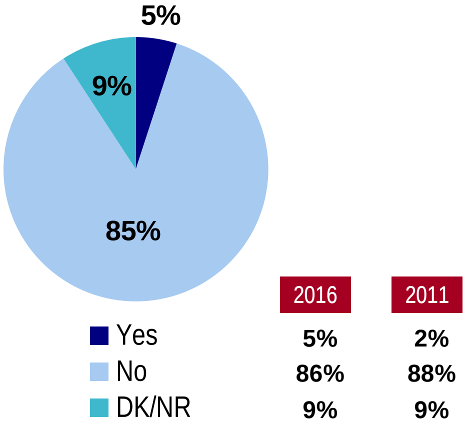
- Canadians with lower income ($40,000 and under) are more apt to say the financial fraud had a large impact.

7.3 Incidence and Impact of Identity Theft

A small minority of Canadians (five per cent) report being the victim of identity theft as a result of their online activity. Most (85 per cent) have never had an incidence of identity theft, although nine per cent say they are not sure.

Chart 33: Incidence of Identity Theft

"Have you ever been a victim of identity theft a result of online activity?"



EKOS Research Associates Inc.

n=2072

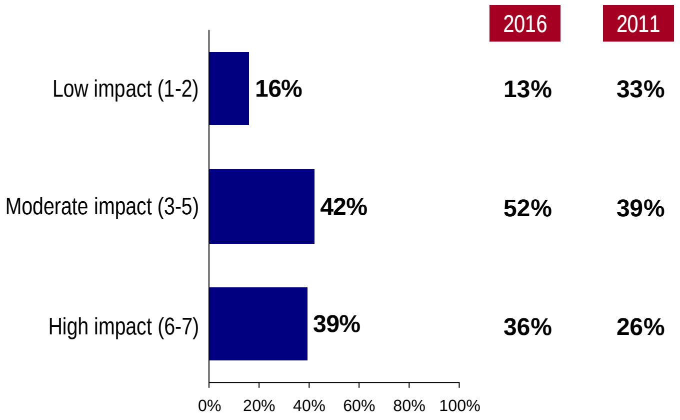
PS Cyber Security Survey, 2018

- Younger Canadians (ages 18 to 25) are more likely to say they have experienced identity theft.

Among the small percentage of Canadians reporting identity theft, nearly four in ten (39 per cent) reported a large impact. A similar proportion describes the impact as moderate (42 per cent), and sixteen per say the impact was low. Caution should be used in comparing results to previous periods due to the relatively low sample size.

Chart 34: Impact of Identity Theft

[IF YES] "How much of an impact did your identity theft have on you or your family?"



EKOS Research Associates Inc.

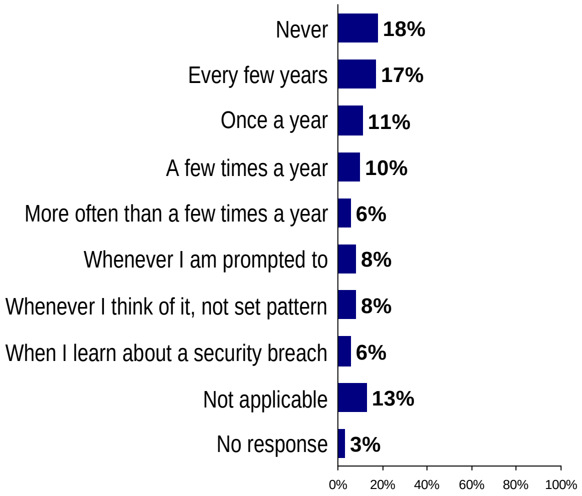
n=118

PS Cyber Security Survey, 2018

Respondents were prompted to consider that many people use the same passwords for different accounts and devices, and many keep the same passwords over time. When considering their own social media accounts, just under one in five say that they change their password never (18 per cent) or every few years (17 per cent). One in ten more diligently change their password once a year (11 per cent) or a few times a year (10 per cent). Less than one in ten change their pass word more than a few times of year (six per cent), whenever prompted (eight per cent), whenever they think of it (eight per cent), or when they learn about a security breach (six per cent).

Chart 35: Password Changes – Social Media

"Many people use the same passwords for different accounts and devices, and many keep the same passwords over time. How often would you say you change the password in your social media accounts?"



EKOS Research Associates Inc.

n=1050 (half sample)

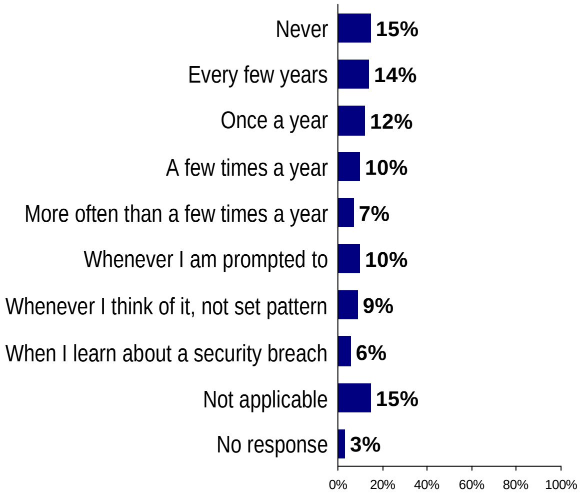
PS Cyber Security Survey, 2018

- Younger Canadians are more likely than those aged 25 and over to say they change their password to social media accounts whenever they hear about a security breach.
- Those with a high school education or less tend to say they change the passwords on their social media accounts a few times a year, or more often than a few times a year.

When considering online shopping accounts, less than one in five say that they never change their password (15 per cent) or do so every few years (14 per cent). One in ten change their password once a year (12 per cent) or a few times a year (10 per cent). A small proportion changes their password more than a few times of year (seven per cent). One in ten or less do not follow a timeline when changing passwords for online shopping, and do so whenever prompted (10 per cent), whenever they think of it (nine per cent), or when they learn about a security breach (six per cent).

Chart 36: Password Changes – Online Shopping

"Many people use the same passwords for different accounts and devices, and many keep the same passwords over time. How often would you say you change the password in your online shopping accounts?"



EKOS Research Associates Inc.

n=1050 (half sample)

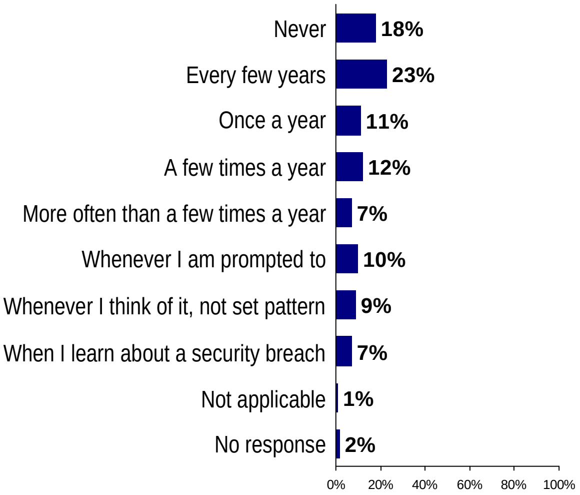
PS Cyber Security Survey, 2018

- Similar to password changes for social media accounts, younger Canadians are more likely to say they change their password to online shopping accounts whenever they hear about a security breach.
- Those with a high school education or less tend to say they change the password for online shopping accounts a few times a year, or more often than a few times a year.

One in five Canadians (18 per cent) say they never change email account passwords. One-quarter (23 per cent) change their password every few years, while one in ten do so once a year (11 per cent) or a few times a year (12 per cent). Seven per cent change their email account password more often than a few times a year. As with other password change patterns, one in ten, or less, do not follow a timeline when changing passwords for email accounts, and do so whenever prompted (10 per cent), whenever they think of it (nine per cent), or when they learn about a security breach (seven per cent).

Chart 37: Password Changes – E-mail Accounts

"Many people use the same passwords for different accounts and devices, and many keep the same passwords over time. How often would you say you change the password in your email accounts?"



EKOS Research Associates Inc.

n=1050 (half sample)

PS Cyber Security Survey, 2018

- Similar to password changes for social media and online shopping accounts, younger Canadians are more likely to say they change their password whenever they hear about a security breach. Those 55 and over are more apt to never change their password on email accounts.
- Those with a high school education or less are more likely to change the password for email accounts a few times a year, or more often than a few times a year.

8. INFORMATION AND RESPONSIBILITIES

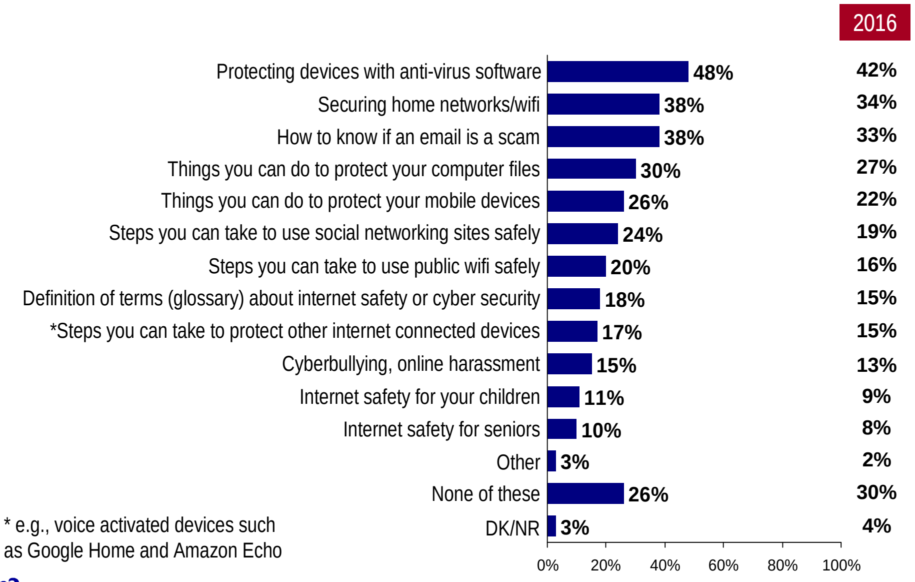
This chapter presents a continuing demand for information, as well as an understanding of who Canadians trust to provide unbiased and reliable up to date information. Canadians continue to look for information on online threats. A majority of Canadians continue to agree that information can help protect themselves online. Canadians consider the security of online personal devices the responsibility of individual owners. They also continue to look to law enforcement organizations and government for the necessary information to take on this responsibility.

8.1 INFORMATION SOUGHT

Most Canadians have searched for information on types of online threats, with only three in ten (26 per cent, down slightly from 30 per cent in 2016) indicating that they have not looked for information. Nearly half (48 per cent) have searched for information on protecting devices with anti-virus software. Four in ten have looked for information on securing home networks and Wi-Fi (38 per cent), or how to know if an email is a scam (38 per cent). Three in ten (30 per cent) have searched for actions to take to protect computer files. One-quarter have searched for information on ways to protect mobile devices (26 per cent) or steps to take to use social networking sites safely (24 per cent). One in five or less have looked for information on using public Wi-Fi safely (20 per cent), definition of terms (18 per cent), steps to protect other connected devices (17 percent), or cyberbullying and online harassment (15 per cent). One in ten have searched for Internet safety for children (11 per cent) or seniors (10 per cent). For each type of online threat, more Canadians have searched for information than in 2016.

Chart 38: Information Sought

"Which of the following types of online threats have you looked for information on, if any?"



* e.g., voice activated devices such as Google Home and Amazon Echo

EKOS Research Associates Inc.

n=2072

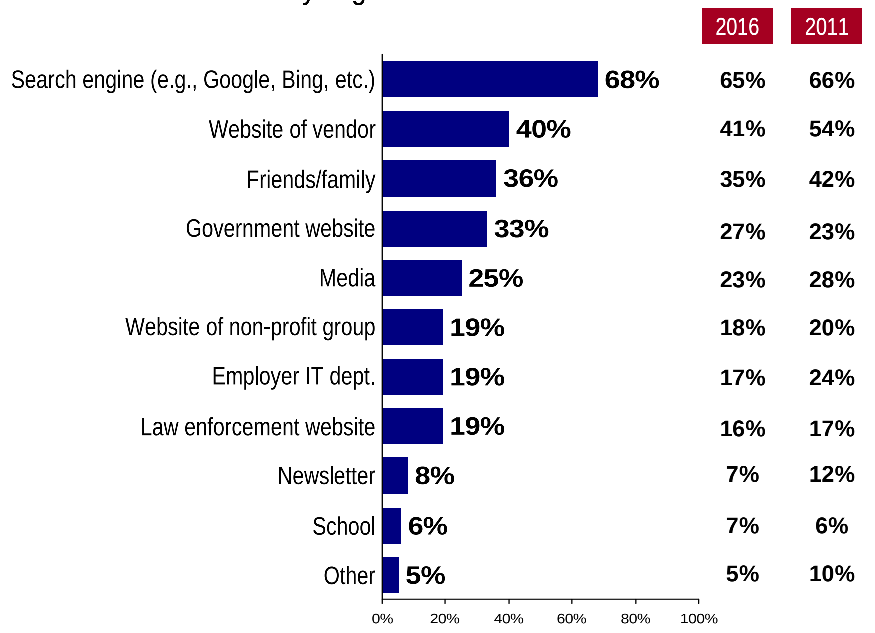
PS Cyber Security Survey, 2018

- Younger Canadians are more likely than older Canadians to have searched for information on steps to use public Wi-Fi safely, safe use of social media sites, protecting mobile devices, and cyberbullying. Older Canadians, ages 65 and over, are more likely to have searched for information on Internet safety for seniors.
- Men are more likely than women to report searching for information on most areas.
- Quebec residents are less apt to have looked for information in most areas than other Canadians.
- The propensity to search for information increases with education level.

Consistent with previous measurement periods, Canadians who sought information are most likely to use search engines when looking for information about online threats (68 per cent). Four in ten go to the website of a vendor for information (40 per cent, similar to 41 per cent in 2016 and down from 54 per cent in 2011). Friends and family are cited as a source of information for 36 per cent. The use of government websites appears to be increasing as a source of information, as one-third (33 per cent) identified that they would go to a government website, higher than reported in 2016 (27 per cent) or 2011 (23 per cent). One-quarter (25 per cent) report using the traditional media as a source of information. One in five say they use the website of a non-profit group (19 per cent), an employer's IT department (19 per cent), or a law enforcement website (19 per cent).

Chart 39: Sources of Information

"Where did you go for that information?"



EKOS Research Associates Inc.

n=1038 (sought information)

PS Cyber Security Survey, 2018

- Those under age 25 are much more likely to say they obtained information from school (24 per cent, compared to six per cent overall).

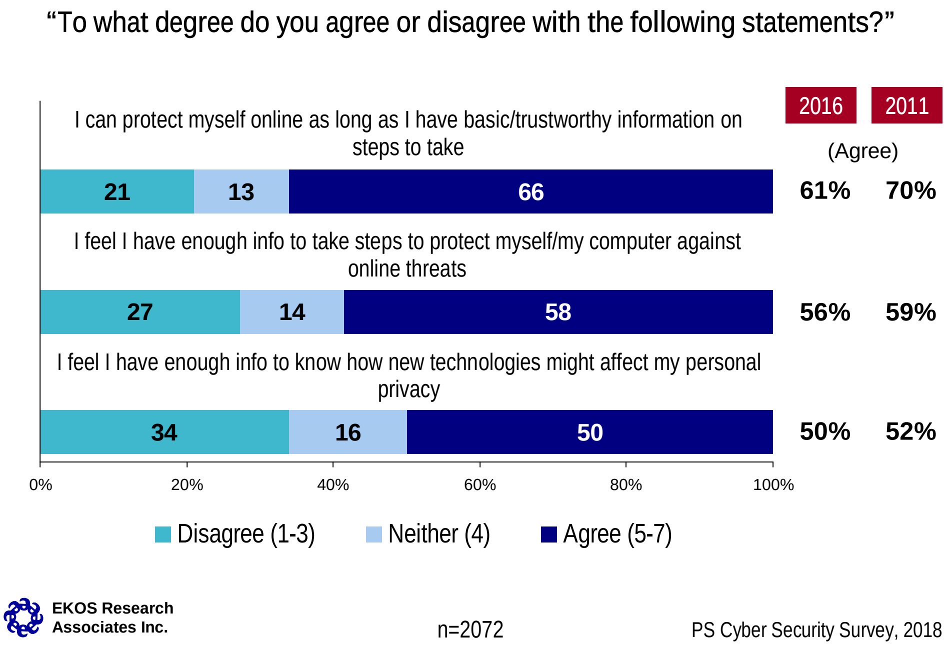
- Men are more likely than women to have found information through a search engine, a website of a vendor, the media, a website of non-profit group, or a newsletter. Women are more apt then men to say they obtained information from friends and family.

- Those with higher education and income are more likely to have used an employer IT department for information. Those with a university education are also more likely to have used a search engine or the website of a non-profit group.

8.2 Attitudes re: Protection from Online Threats

Two in three Canadians (66 per cent) are confident that they can protect themselves online as long as they have the basic and trustworthy information on steps to take. This is higher than the 61 per cent reported in 2016 and remains below the 70 per cent confidence reported in 2011. Over half (58 per cent, similar to 56 per cent reported in 2016 and 59 per cent in 2011) agree that they have enough information on how to take steps to protect themselves, although one-quarter (27 per cent) feel that they do not. Similarly, the proportions of Canadians agreeing that they have enough information to know how new technologies might affect their personal privacy have remained virtually the same as in 2016 with 50 per cent agreeing, and a notable 34 per cent disagreeing.

Chart 40: Attitudes Regarding Protection from Online Threats



- Canadians ages 44 and under, and men are generally more apt to agree with all three factors.
- Those with higher income are more apt to agree they have enough information on how technology might affect personal privacy and how to protect against online threats.

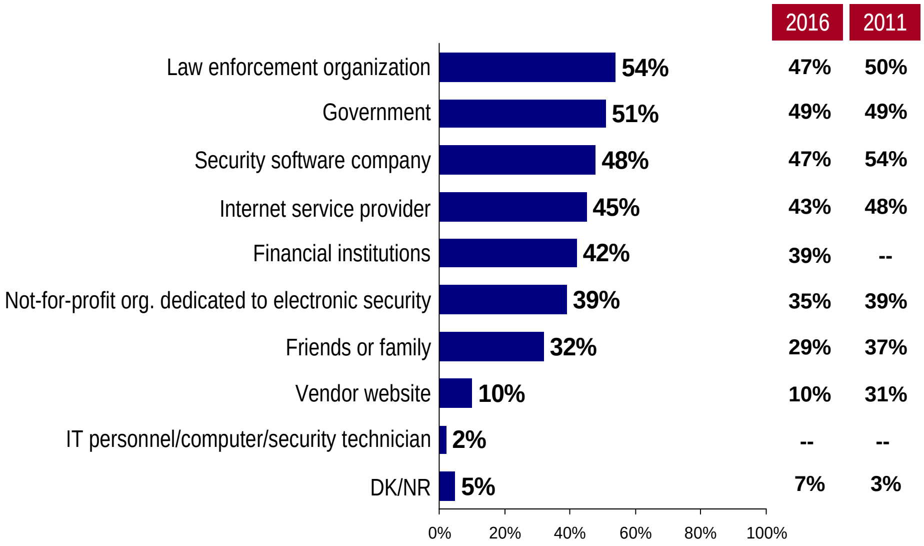
8.3 Trustworthy Organizations for Information

Just over half of Canadians say they trust law enforcement organizations (54 per cent, an increase from 47 per cent in 2016) or the Government (51 per cent) to provide the best technically reliable and up-to-date information about online threats and the steps to take to protect themselves. Fewer than half trust a security software company (48 per cent), Internet service providers (45 per cent), or financial institutions (42 per cent). Four in ten (39 per cent) trust not-for-profit organizations dedicated to electronic security. Friends or family are trusted by one-third (32 per cent), while a vendor website is trusted by one in ten (10 per cent). Two per cent trust an IT or security technician (not noted in previous measurement periods).

This is the first time law enforcement organizations have reached the top of the rankings, while trust in a security software company dropped from first place in 2011 to third place in 2018.

Chart 41: Trustworthy Organizations for Information

"Who would you trust to give you the best technically reliable and up-to-date information about online threats and steps you can take to protect yourself?"



EKOS Research Associates Inc.

n=2072

PS Cyber Security Survey, 2018

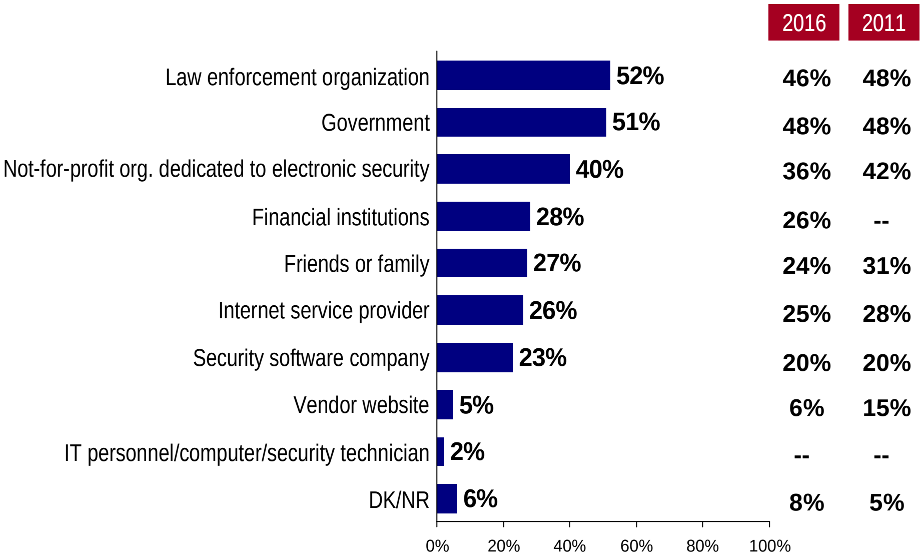
- Age is a factor in deciding trustworthy sources. Older Canadians (age 65 or older) are more likely to trust friends or family, their Internet service provider, and financial institutions. Those age 25 to 54 are more likely to trust not-for-profit organizations than other age groups. Younger Canadians (under 24) are more likely to trust a vendor website such as the online store.
- Men are more likely than women to trust a security software company, not-for-profit organization, or vendor website. Women are more apt to trust law enforcement agencies, the government, or friends and family.
- Those with higher education and income are more apt to trust not-for-profit organizations.

8.4 UNBIASED ORGANIZATIONS FOR INFORMATION

Public services remain the top two organizations identified in terms of being trusted to provide unbiased information about online threats and steps to take for individual protection. Roughly half of respondents trust law enforcement organizations (52 per cent, up from 56 per cent in 2016) or the government (51 per cent) to provide unbiased information. Not-for-profit organizations are trusted by four in ten (40 per cent, up slightly from 36 per cent in 2016). Roughly one-quarter trust financial institutions (28 per cent), friends or family (27 per cent), Internet service providers (26 per cent), or security software companies (32 per cent).

Chart 42: Unbiased Organizations for Information

"And who would you trust to give you the most unbiased information about online threats and steps you can take to protect yourself?"



EKOS Research Associates Inc.

n=2072

PS Cyber Security Survey, 2018

- As with sources considered trustworthy, age is a factor in deciding unbiased sources. Older Canadians (ages 65 or older) are more likely to identify friends or family, their Internet service provider, financial institutions, and software security companies as unbiased sources. Those ages 25 to 54 are more likely to say not-for-profit organizations are unbiased than other age groups. Younger Canadians (under 25) are more likely to state a vendor website is an unbiased source.

- Men are more likely than women to trust a financial institution, an Internet service provider, a security software company, or a not-for-profit organization. Women are more apt to trust law enforcement agencies or friends and family.

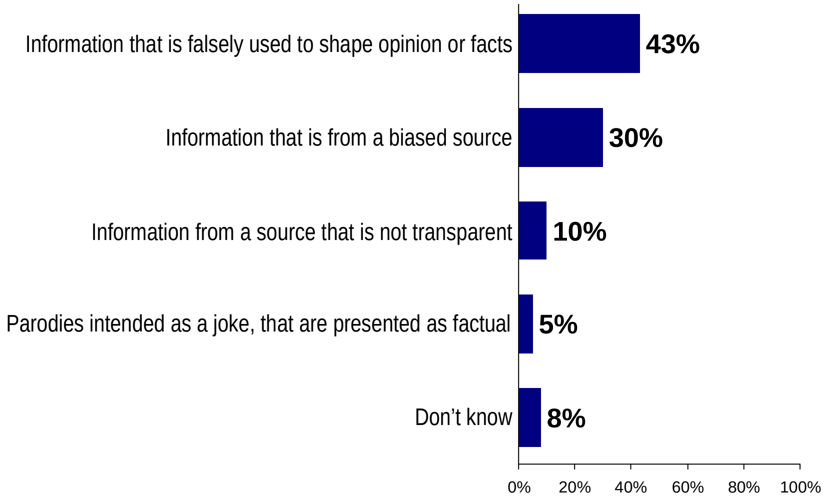
- Those with higher education and income are more apt to trust governments and not-for-profit organizations. University graduates are also more likely to trust law enforcement agencies.

8.5 UNDERSTANDING "FAKE NEWS"

When someone talks about "fake news" in connection with information that individuals need to protect themselves, roughly four in ten Canadians (43 per cent) feel that this refers to information that is falsely used to shape opinion or facts. Three in ten (30 per cent) feel that "fake news" is information that is produced by a biased source, while one in ten (10 per cent) state that it is information from a source that is not transparent. Few (five per cent) state that they consider "fake news" to be parodies intended as a joke that are presented as factual. Eight per cent are not sure.

Chart 43: Fake News

"When someone talks about "fake news" in connection with information that people/consumers need to protect themselves, do you think that this typically refers to...?"



EKOS Research Associates Inc.

n=2072

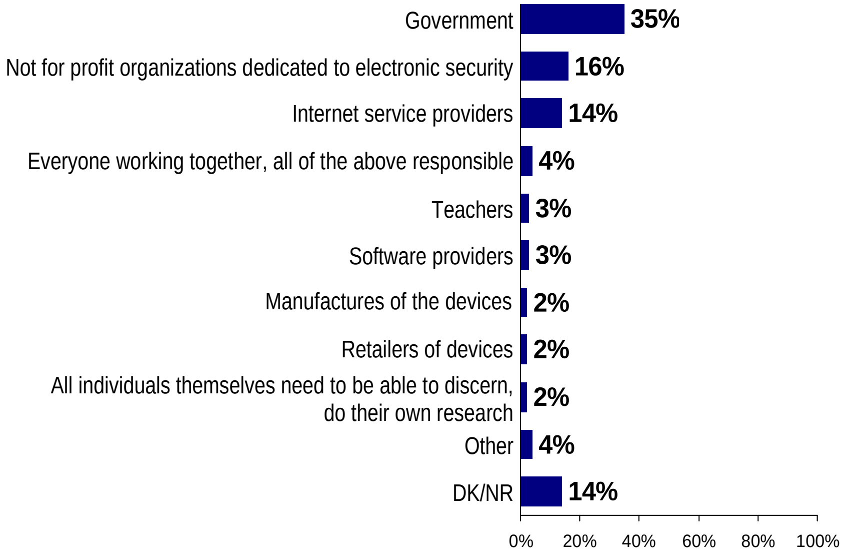
PS Cyber Security Survey, 2018

- Younger Canadians (under age 24), along residents of Quebec, are more apt to state that "fake news" means the information is from a source that is not transparent, or that it is a parody.

One-third of Canadians (35 per cent) feel that the government should play a role in helping Canadians recognize what is “fake news” when it comes to information about online threats and consumer protection. Over one in ten say that not-for-profit organizations dedicated to electronic security (16 per cent) or Internet service providers (14 per cent) should have a role. A variety of other sources are mentioned including everyone working together (four per cent), teachers (three per cent), software providers (three per cent), device manufacturers (two per cent), retailers of devices (two per cent), or that individuals should discern and do their own research (two per cent). Fourteen per cent are not sure who should play a role.

Chart 44: Sources to Help Recognize Fake News

“Who should play a role in helping Canadians recognize what is "fake news" when it comes to information about online threats and consumer protection?”



EKOS Research Associates Inc. n=1050 (half sample) PS Cyber Security Survey, 2018

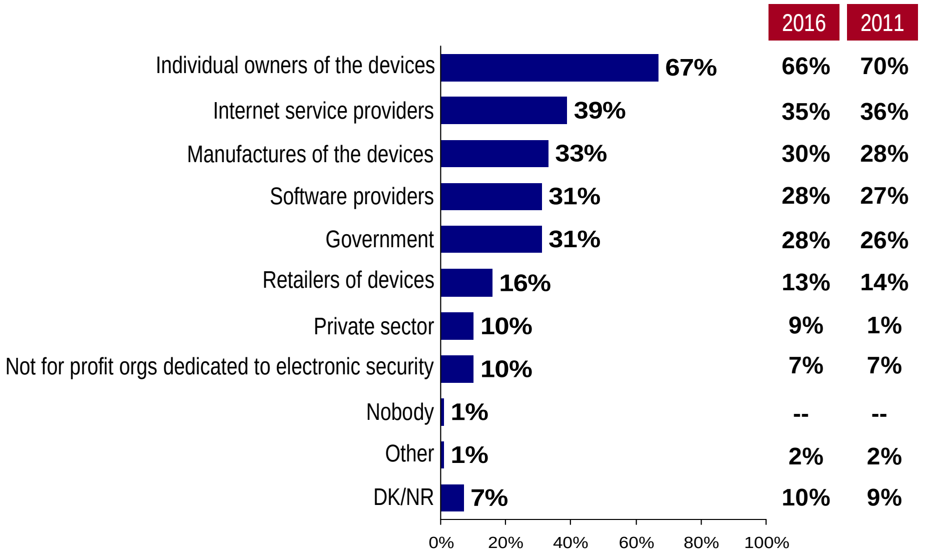
- Older Canadians (age 55 and over) are more likely to say that Internet services providers should play a role. Younger Canadians are more apt to state the government should play a role.
- Those in Quebec are more likely than those in any other region to say the government should play a role.

8.6 Responsibility for the Security of Devices

Most Canadians (67 per cent) think the responsibility for ensuring that web-enabled personal devices are safe and secure rests with the individual owners of the devices, down marginally from 2011 (70 per cent), but in line with 2016 (66 per cent). Other sources are mentioned slightly more often than previous measurement periods, including Internet service providers (30 per cent), manufacturers of the devices (33 per cent), software providers (31 per cent), and the government (31 per cent). Sixteen per cent feel that the retailers of devices have a responsibility for the security of the devices. One in ten say the private sector (10 per cent) or not-for-profit organizations dedicated to electronic security (10 per cent) should be responsible.

Chart 45: Responsibility for the Security of Devices

"As far as you know, who is primarily responsible for ensuring that personal devices that Canadians use to access the Internet with are safe and secure?"



EKOS Research Associates Inc.

n=2072

PS Cyber Security Survey, 2018

- As in 2016, residents of Quebec are less likely than other Canadians to say that it is the responsibility of individual owners to ensure their devices are secure, but Quebecers are much more likely to say that each of the other parties (with the exception of the private sector) – particularly governments – have primary responsibility.
- The perception that ISPs have primary responsibility for ensuring the safety and security of these devices continues to be much more common among older Canadians (55 or older).
- Interestingly, 25-34 year olds in 2011 were reported to be more likely to identify individual owners as responsible for the security of devices. In 2016 and 2018, 35-44 year old Canadians are statistically more likely to agree with this as opposed to 25-34 year olds and those under 25. This could point to a generational shift as members of the 25-34 age group of 2011 turn into the current 35-44 group. The youngest age group (18-24) are least likely to feel that individual owners of devices should be primarily responsible.
- As in previous measurement periods, those reporting the highest income more likely than others to think that individual owners are primarily responsible for the security of their devices.

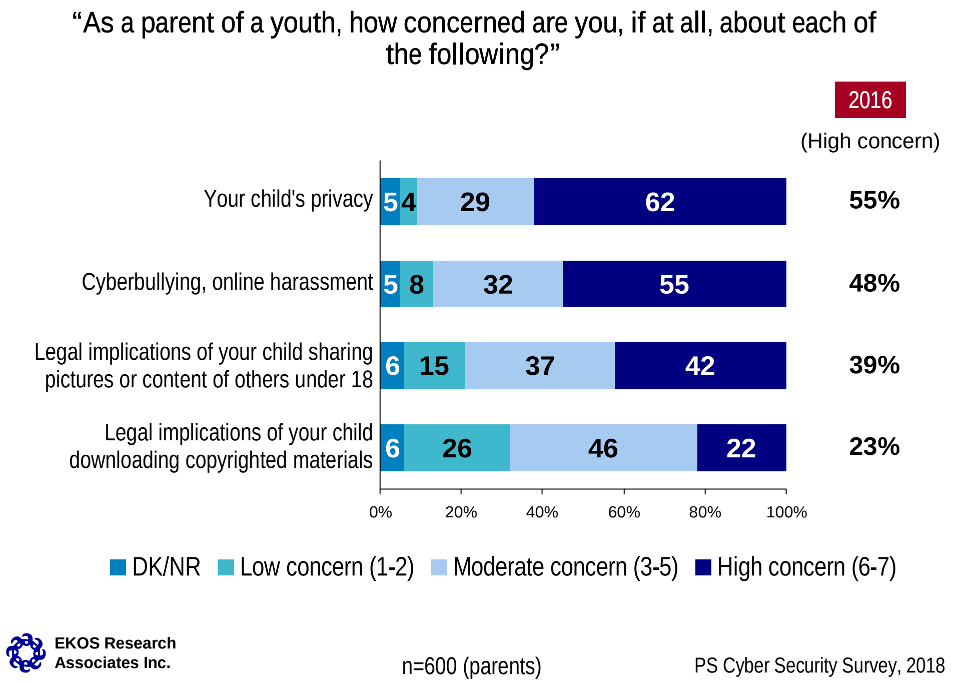
9. Concerns of Parents

This chapter highlights specific concerns that Canadian parents have when considering their children's online access. The results show that parents are more concerned with their children's privacy and welfare than the legal implications of their activities. Among those parents that are not concerned there is a divide between those that take action to inform themselves and their children and those that trust their children to monitor themselves to avoid specific threats online.

9.1 Concern among parents

Six in ten Canadian parents (62 per cent) are concerned about their children's online privacy. Just over half are concerned about cyberbullying and online harassment (55 per cent). About four in ten are also concerned with the implications of sharing pictures of others under 18 (42 per cent), although considerably fewer are concerned about the legal implications of children downloading copyrighted material (22 per cent).

Chart 46: Concern Among Parents



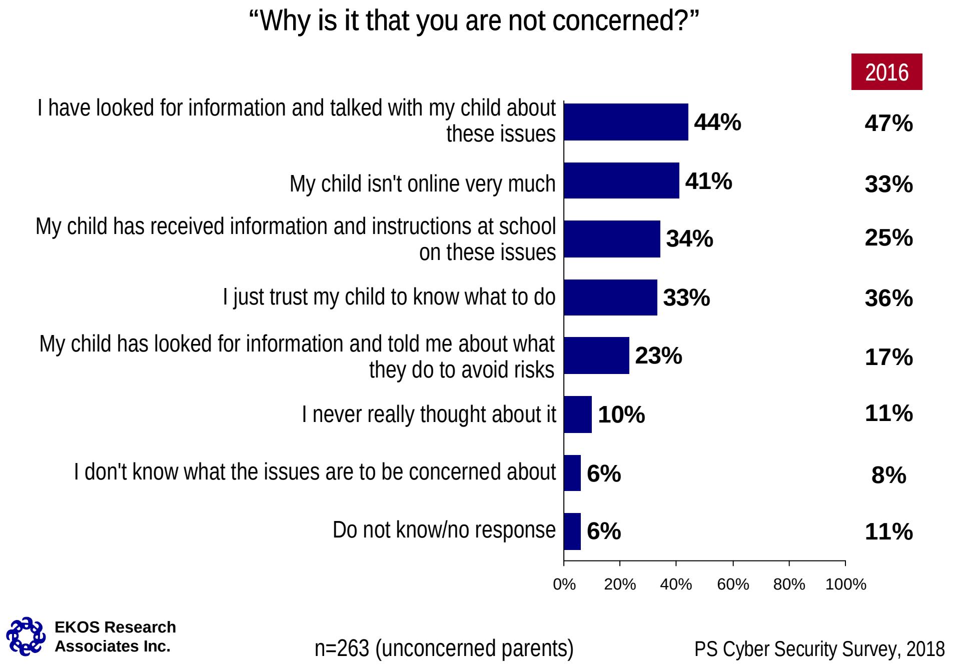
- Parents with a college degree are typically more concerned than other parents about the legal implications of sharing pictures.
- There are regional patterns to how parents perceive online threats. Parents in British Columbia are more likely to be concerned about cyberbullying and online harassment.
- Although there are few gender differences, mothers are somewhat more concerned than fathers about cyberbullying and their children's privacy.

9.2 REASONS FOR NON-CONCERN

Among those parents that were not concerned about their children's exposure to the specific online threats, more than four in ten (44 per cent) said this is because of having sought out information and talked to their children about the issues. Other slightly overlapping consisted of parents who said their children have received instruction and information on these issues (34 per cent), and/or they trust their children to know what to do (33 per cent). A third segment responded that their child is not online very much (41 per cent); this option was most likely to be selected by parents of children under 10. The large majority of parents choose to look for information themselves to teach their own children, have schools inform their children, or trust their child to inform themselves.

Compared with 2016, there is a notable increase in the proportion of parents indicating that their child has received information and instructions in school, from 25 per cent in 2016 to 34 per cent.

Chart 47: Reasons for Non-Concern



n=263 (unconcerned parents)

PS Cyber Security Survey, 2018

- The age of the child has a noticeable effect on why parents chose not to be concerned. Half or more of those with children under six (75 per cent) and those six to ten (58 per cent) respond that they are not concerned as their children are not online very much. This drops precipitously for children 11 to 15 (19 per cent) and those 16 or more (12 per cent). Parents of children 11 or older are more likely to have acted in looking for information to educate their children or trusting their children to know what to do, or that their child has looked for or received information in school.

- College-educated parents are more likely to say they have looked for information to teach their children.

- Parents in Quebec are more likely than others across the country to say that they have not thought about these issues, or do not know what the issues are.

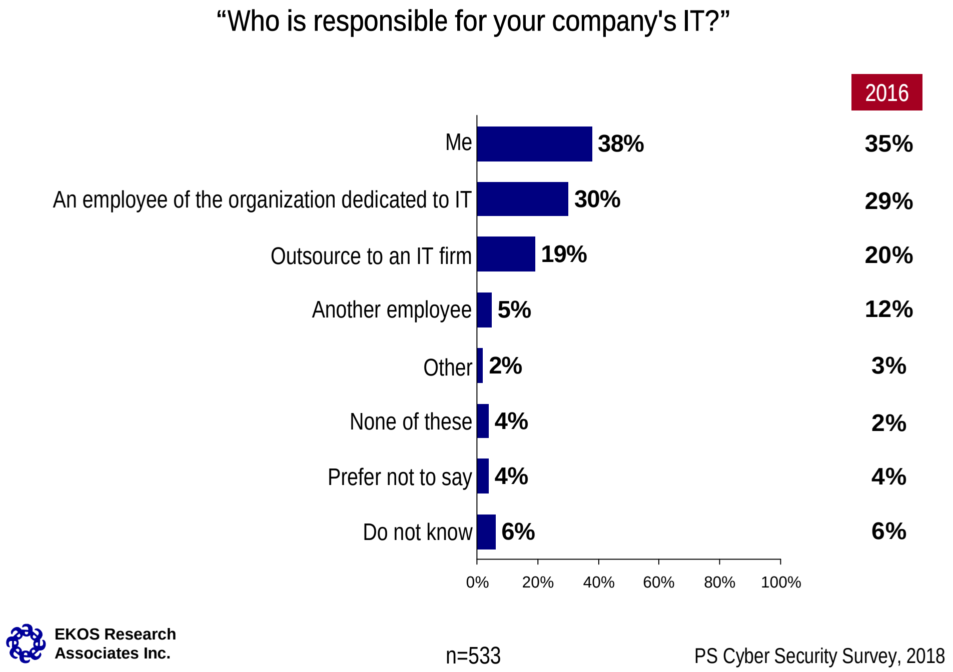
10. BUSINESS EXPERIENCE

Exclusive to business managers or owners, this section presents the concerns and perception of online threats within this segment of Canadians. The results show that a sizeable proportion of Canadian businesses worry about work disruptions and financial losses due to online threats. Although a majority of these businesses take precautions to protect themselves from threats, there is a high percentage that perceives it would benefit from knowing particularly what threats exist and guidelines for how to react to them.

10.1 IT RESPONSIBILITIES

Not surprisingly, the person responsible for a company's IT depends on the size of the company. Similar to results from 2016, in 38 per cent of companies in the sample, the respondent indicated that they are the person in charge of IT, reflecting the high concentration of smaller companies in the sample. In fact, 67 per cent of companies with one to ten employees had the respondent as the person in charge of IT. On the other hand, 69 to 73 per cent of those companies with more than 50 employees have a separate employee dedicated to IT. In 19 per cent of cases, the respondent indicated that IT is outsourced.

Chart 48: Survey Respondent



n=533

PS Cyber Security Survey, 2018

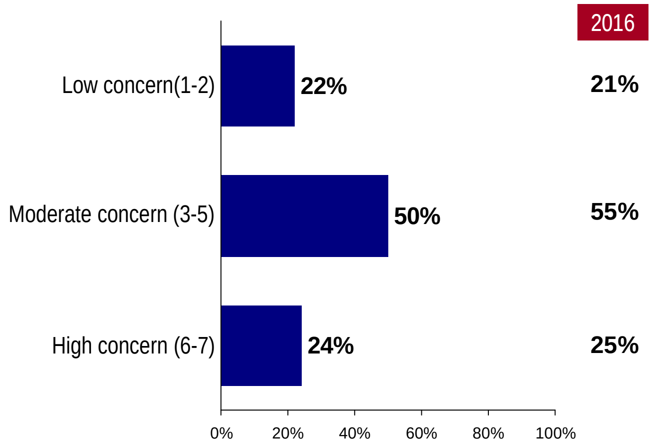
10.2 Concerns Over Disruption

While half of businesses expressed moderate levels of concern (50 per cent), there is a balance of roughly one in four to one in five who are either unconcerned or very concerned, as was also the case in 2016. Organizations with 11 to 20 employees reported the highest concern with 37 per cent indicating that they are concerned about disruptions or loss as a result of online threats (i.e., six or seven on seven-point scale).

Among those organizations not concerned, just under half consider the threat of an online incident to be very low (43 per cent) which seems an increase from 2016 when it was 33 per cent. Another three in ten feel confident in their research and preparedness for such an event (30 per cent). There are no discernible differences between companies of different sizes in terms of the nature of concern due, in part, to the small sample size.

Chart 49: Level of Concern Among Businesses

“Thinking about the various concerns of daily operations of your organization, how worried would you say you are about work disruptions or financial loss as a result of online threats?”

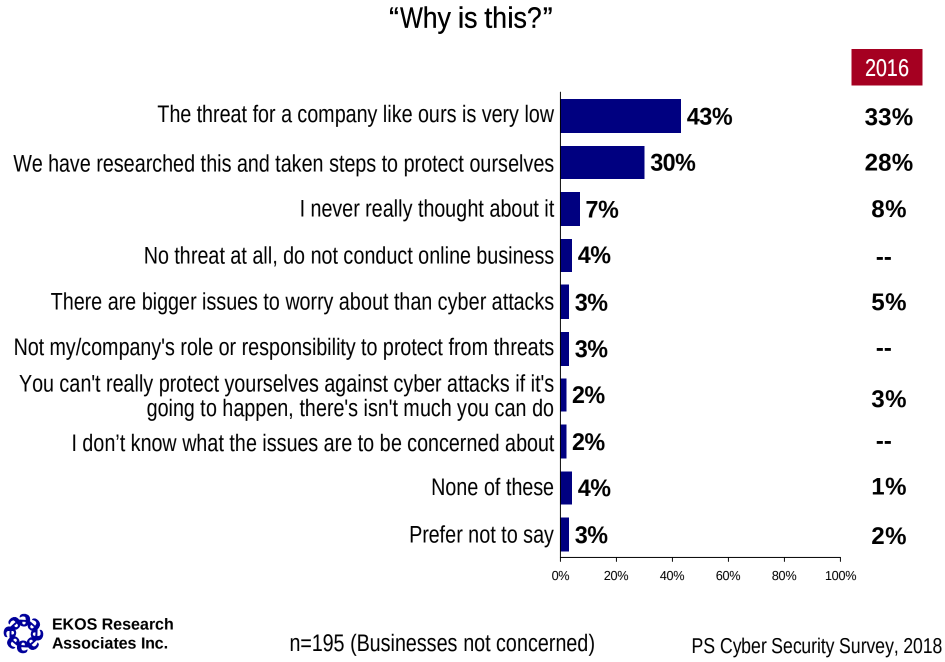


EKOS Research Associates Inc.

n=533

PS Cyber Security Survey, 2018

Chart 50: Reason for Lack of Concern

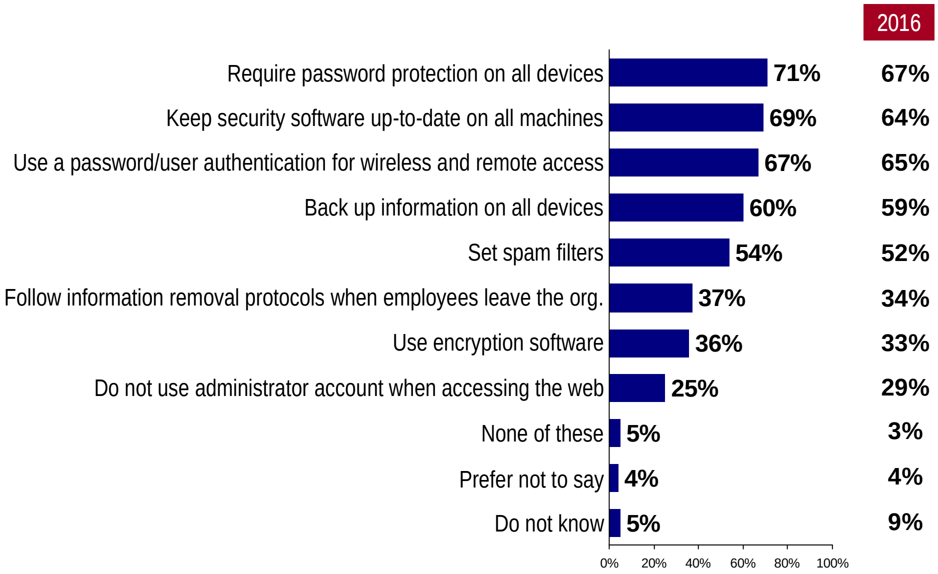


10.3 Steps to Protect Against Online Threats

Most Canadian businesses have taken basic steps to protect themselves against online threats. About seven in ten require password protection on all devices (71 per cent), keep security software up to date (69 per cent, up from 64 per cent in 2016), and/or use password authentication for remote access (67 per cent). As in 2016, more than half back up information (60 per cent) and set spam filters (54 per cent). When it comes to more demanding initiatives, fewer businesses take such measures. Just over a third follow information removal protocols when employees leave the organization (37 per cent) of use encryption software (36 per cent). Another one in four (25 per cent) avoid using administrator accounts to access the web. Only five per cent explicitly say that they do not take any of the presented precautions.

Chart 51: Steps Taken by Businesses

"Turning to your work as a business owner/manager, which of the following steps has your business taken to protect itself against online threats?"



EKOS Research Associates Inc.

n=533

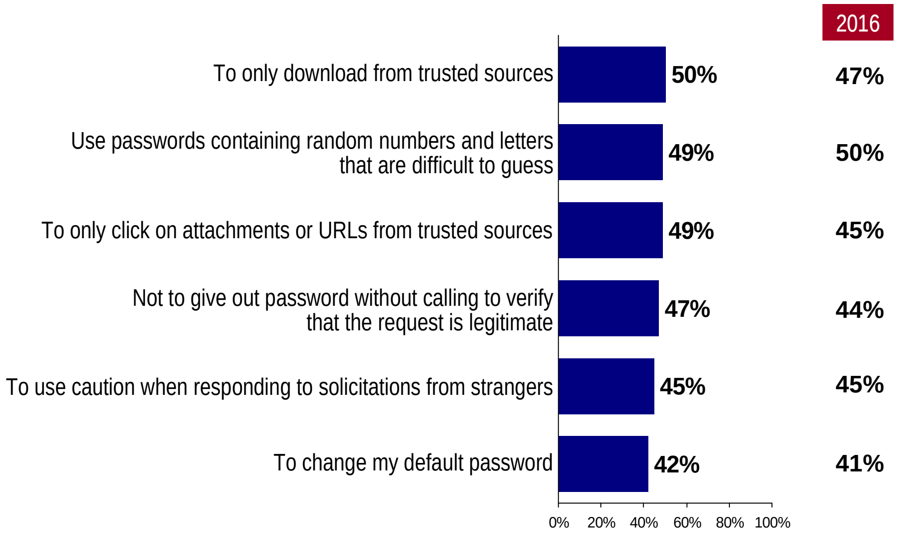
PS Cyber Security Survey, 2018

- Organizations with dedicated internal IT resources, as well as those who outsource this function are more apt to have taken most of the steps examined.

Roughly half of businesses also instruct employees to download only from trusted sources (50 per cent), use passwords that contain random numbers and letters (49 per cent), and/or instruct employees to only click on attachments from trusted sources (49 per cent), to use caution when responding to strangers (47 per cent), or not give out passwords without verification (47 per cent). Four in ten emphasize changing default passwords (42 per cent) and another one in three (32 per cent) do not allow browsers to remember passwords. About one in four instruct employees to use encryption (27 per cent), and/or ask employees to check privacy policies on websites (23 per cent), or read terms of service (22 per cent). One in ten (11 per cent) do not provide their employees with any of these instructions and one in five (22 per cent) did not provide a response. These results are largely on par with those found in 2016.

Chart 52a: Specific Security Instructions for Employees

"Which of the following instructions do you provide to employees to protect the organization against online threats and to protect your personal information?"



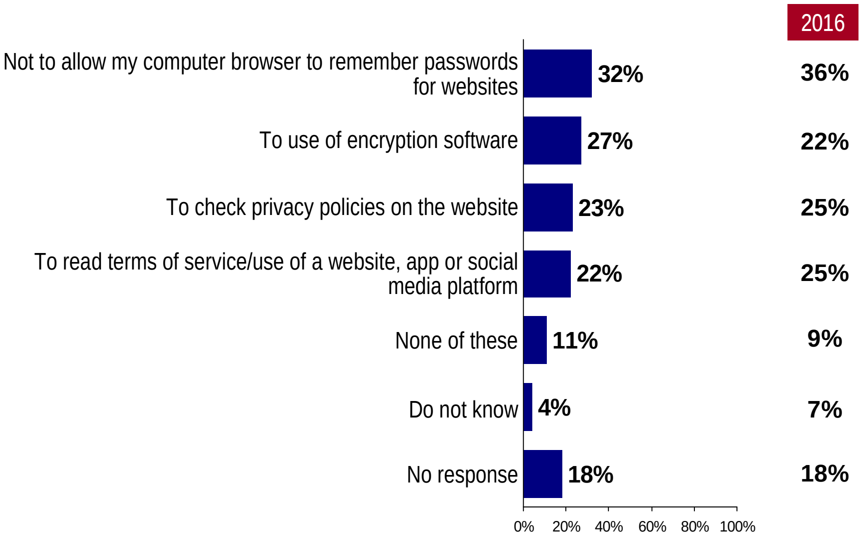
EKOS Research Associates Inc.

n=533

PS Cyber Security Survey, 2018

Chart 52b: Specific Security Instructions for Employees

"Which of the following instructions do you provide to employees to protect the organization against online threats and to protect your personal information?"



EKOS Research Associates Inc.

n=533

PS Cyber Security Survey, 2018

- Larger organizations tend to be more specific when instructing employees only to click on attachments from trusted sources, to use complex passwords, to change default passwords, and not give them out without verification, and to check privacy policies. Organizations in the 11-20 employee range also stand out in instructing employees to use complex passwords, to use caution when responding to solicitations from unknown sources, and to only download from trusted sources.
- Businesses with dedicated, internal IT staff are also more likely to say that they require most of these procedures. Those who outsource this function are most apt to instruct employees to only download or click on attachments from trusted sources, use caution when responding to solicitations and not to give out passwords without verification.

10.4 Beneficial Information

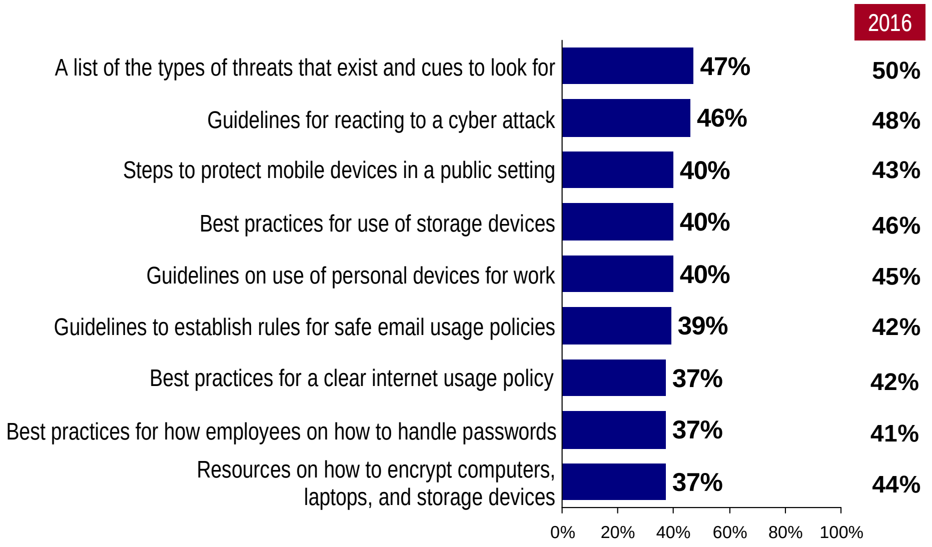
The ranking of potentially beneficial information points to Canadian businesses favouring solutions that can be handled by an IT department or policy rather than through informing employees. For example, ranked in the top, organizations feel they would benefit from information on the types of threats that exist (47 per cent), guidelines for reacting to cyber attacks (46 per cent), best practices for storage devices, steps to protect mobile devices in a public setting, and guidelines on use of personal devices for work (40 per cent for each) and guidelines to establish rules for safe email usage policies (39 per cent).

Slightly lower on the list are best practices for how employees on how to handle passwords, guidelines for establishing a strong social media policy, best practices for Internet usage, and resources on how to encrypt computers, laptops and storage devices (37 per cent in each case). The demand is similar for tips for software and hardware to secure networks (36 per cent) and best practices for safe cloud computing (35 per cent). Slightly fewer identified a need for information on steps for handling departing employees (33 per cent) and tips on communicating the importance of following cyber security policies (32 per cent).

Relative to results in 2016, the demand for information seems marginally lower in 2018 in some areas, including use of storage devices and use of personal devices, clear Internet usage policy, how to encrypt devices, the type of hardware/software to make networks secure, safe cloud computing, handling departing employees, and the importance of safe cyber policies.

Chart 53a: Required Information

“Which of the following types of information do you feel that your organization would benefit from having to protect itself against online threats?”



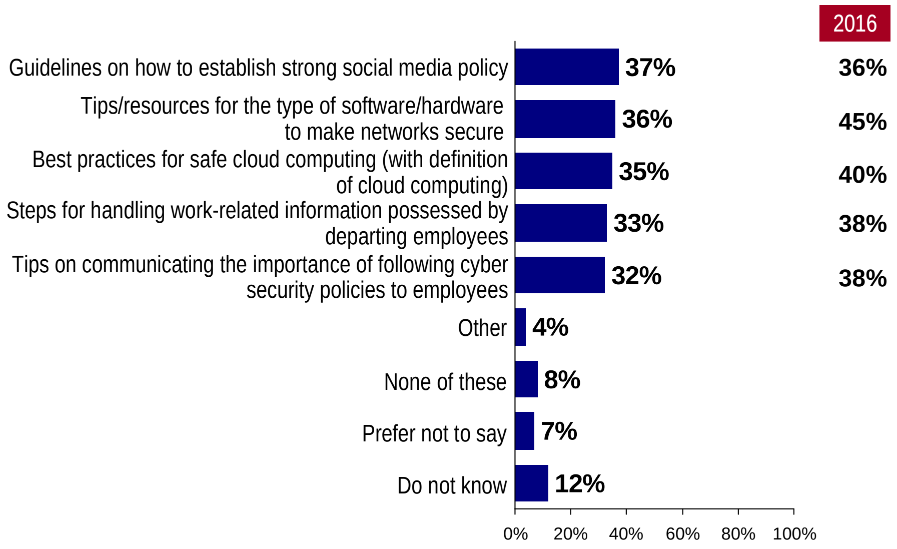
EKOS Research Associates Inc.

n=533

PS Cyber Security Survey, 2018

Chart 53b: Required Information

“Which of the following types of information do you feel that your organization would benefit from having to protect itself against online threats?”



EKOS Research Associates Inc.

n=533

PS Cyber Security Survey, 2018

- Businesses with dedicated, internal IT staff, as well as those who outsource this function are also more likely to say that they require most of these procedures.

11. Focus Group Findings

11.1 Awareness of Security Issues

Focus group participants primarily feel that there are security issues that pose a risk when engaged in online activities. Many are concerned about financial theft due to transactions conducted online. Many are also concerned about identity theft as a result of information entered online, data theft, hacking of institutions where individuals' information may be stored, or hacking into personal computers. Some are concerned about privacy issues that include a range of apprehensions such as predators accessing webcams or the use of an individual's purchasing data for marketing purposes.

11.2 Confidence in Ability to Protect Oneself

Most focus group participants say that while there are risks to engaging in online activity, they take some steps to protect themselves against those risks. These participants feel that while risk cannot be eliminated entirely, they are attempting to incorporate a reasonable amount of actions to stay safe while communicating with others, conducting transactions online, or protecting their documents and photos. Alternatively, some focus group participants feel extremely confident in their ability to safely engage in online activity, expressing that they are knowledgeable about the risks, and capable and diligent in their actions to protect themselves online. A few participants state that they feel protected from online threats because they minimize their presence or actions online; by not participating socially or financially online, they perceive that they mitigate risk.

> "I know that those risks cannot be reduced to zero." (Toronto)
>
> "Maybe I should be more concerned than I am, especially around identity theft." (Toronto)
>
> "I feel fairly comfortable with my level of security." (Calgary)
>
> "There's a certain risk. I think with all the companies being hacked, it's more a question of when than if. Since it happens so often, we know it's a risk that we don't really have control over. I won't stop myself from buying something online just because there's a risk but I'll pay more attention to who I do transactions with." (Montreal)
>
> "I don't shop online, that's why I feel confident." (Halifax)

11.3 Action Taken to Mitigate Risks

Most participants perceive that they are aware of many of the risks and take precautions against any adverse actions. Some areas where participants feel protected without effort are from actions taken by banks or internet service providers. These participants note (through personal experience or experience of others) that banks monitor financial transactions and can take steps to identify or reverse fraudulent transactions. Some participants also rely on virus protection and other security features on their computers to mitigate hackers, receiving corrupt files, and other forms of data, or identity theft.

> "I think a lot of it is awareness. I check my bank statements religiously." (Toronto)
>
> "I find using PayPal is the best way to go simply because you don't want to give your financial information to a bunch of different companies when you can just give it to one. That's only one point of vulnerability as opposed to many." (Calgary)
>
> "I'll never give my credit card number to a website that asks for it in order to register for something, but I know if I tell my bank I didn't make a transaction, they'll cancel it, so I feel protected by my bank." (Montreal)

Some participants cite action that they take to protect themselves from security issues online, such as knowledge of how to identify fraudulent emails (misspellings, links going to non-official sites), not using public or non-secure Wi-Fi, not entering birth dates or extensive personal information online, and changing passwords regularly or having complicated passwords.

> "I don't use my phone for financial stuff because I trust my laptop more than my phone. I don't know if that's valid or not, but I don't do anything financial with my phone." (Calgary)
>
> "They like to take some of my friends' names and their emails, they take the names and just change one letter and then they send me a spam email. That's a more recent thing, and it's like okay how did they get my friends' names? It makes me worry if they can get my friends' names what else are they getting?" (Toronto)
>
> "I won't do anything of a sensitive nature on public wifi." (Halifax)

11.4 How Real is the Threat Online?

Most focus group participants feel that the need to protect themselves online feels just as real as the need to protect themselves from tangible threats. For example, someone stealing personal belongings feels just as threatening, or a similar violation, as someone stealing identify online. For some, the threat of theft online is more of a concern than the threat of theft of a belonging. These participants state that with tangible items, an individual can watch their belongings, and the extent and consequences of the theft is known immediately. A few articulated that theft in "real life" is easier to understand than online threats. For a few, tangible threats feel more likely to occur than those online. These participants mention that with all the potential targets available to hackers (such as larger organizations or Governments), it's unlikely someone would target them personally.

> "I see them as being as sort of on the same level. In fact, my physical belongings I'm a bit less concerned about because there's only so much that can be done in a short span of time physically but online tens of thousands of dollars can be transferred in an instant." (Toronto)
>
> "It's more of a violation I think when it's digital. Somebody tries to steal from me for example, I punch their lights out, end of story. If somebody is sneaking into my online accounts and doing sneaky things I may not know about it right away, you know? By the time you know something has happened the bad guy has done his damage and is on to someone else." (Calgary)
>
> "The odds feel like they're more in my favour online. Like what are the odds that somebody's going to be looking to access my computer at the exact moment that I'm doing this exact thing. It just feels to me less likely to happen while if I put my wallet down and there's 10 people around, that's 10 chances I can visibly see." (Halifax)
>
> "I think there's less of a risk online, but that doesn't mean bad things can't happen, though it's less risky." (Montreal)
>
> [stealing physical belongings is more of a threat because…] "All my important documents like my passport etc. are at home and not online." (Montreal)

11.5 Barriers to Action

Few focus group participants can identify the specific reasons they have to not taken additional steps to protect themselves online. Some feel they are already taking sufficient precautions. A few others state that they take action to protect themselves generally, while acknowledging that that they do still take occasional risks (such as conducting transactions using a device on public Wi-Fi). Some participants say that they take some steps to protect themselves, but feel they are unlikely to be the target of any malicious intentions.

Still, a few say they are unaware of all that they should be doing to protect themselves when engaged in online activities, and that they have a lack of time, direction or information on what should be done to enhance their cyber security. A few indicate they feel somewhat helpless in taking precautions because even with security measures in place, threats still exist from online activity.

> “I don’t know if we know what to do. I mean, you think you’ve got things secure but then the headlines on the paper are ‘this was hacked’ and some pretty major corporations and so on are being hacked and I look at my little cellphone and I say ‘what hope have I got?’ I’m just hoping I’m too small for them to bother with.” (Calgary)
>
> “When CRA itself has been hacked, what hope does any individual have?” (Calgary)
>
> “The reason why I have all these devices when I know there’s a security risk is the convenience, and I’d take the convenience over the security risk any day.” (Toronto)
>
> “I looked up tips on how to remember different passwords, but it’s a matter of ease. Yes I could change it, but I don’t want to make the effort. It’s different for my work, but when it comes to personal, I figure my life is too boring and hackers wouldn’t bother.” (Montreal)

11.6 Adequacy of Information

Most focus group participants indicate they do not have enough information to adequately take steps to protect themselves and their family from online threats. Primarily, most participants say they have a “basic” or “tip of the iceberg” level of information. Some point out that because technology using the internet, and associated risks, are evolving, it can be difficult to keep up to date. Similarly, some participants indicate that it is not possible to understand all of the possible online threats and that some risks are inherent in most activities.

> “No, I feel like I don’t [have enough information] because the threat changes.” (Calgary)
>
> “To my knowledge there’s no place to go for Canadians to know what’s out there and what the upcoming threat was and what the threat was last week and that would be comforting to have.” (Halifax)
>
> “I don’t think I have all the information, but to a certain degree, it isn’t possible to get all the information. I can make a decision based on the information I have, but there’s no guarantee my bank won’t get hacked tomorrow and lose all my information.” (Montreal)

Some perceive that certain segments of the population (seniors, young people, new Canadians) are not exposed to information on what threats exist online and steps to take to protect against those threats. A few say that they have looked for information to protect family members, such as children or aging parents, from online threats. Of these individuals, no one pointed to any information that they found to help the particular segment protect themselves online.

> "I did try to find a site and there was nothing out there that could give my parents a checklist to say 'Do you see this? What does the email look like? What does the URL look like?' There's nothing out there, its scattered." (Toronto)

> "Being almost a senior and working with seniors, they are the group that gets targeted the most and they are the ones that don't have the education." (Toronto)

Participants who feel they have enough information typically include those individuals who also stated they are confident they know what steps to take to mitigate risk from online threats. These participants feel they have the technical knowledge to know what steps to take to protect themselves online, and feel that no further information is needed that would enhance their understanding. However, as one participant alluded, you can be confident in your information when you do not know what the problem is or what you are missing.

> "Spending time on the internet reading you learn how these things work and then once you kind of know how it works its way harder to fall into it." (Halifax)

11.7 Perceived Reliability of Information

Most participants feel they have developed an awareness of risks, derived from various sources. Many participants do not actively seek out information related to online risks, but are passively exposed to information that comes to them through word of mouth or the media. As one participant noted, "It's so frequent that most of the common steps you can take I'm very aware of because I'm constantly reminded of it in the media." A few participants starting thinking about steps to mitigate risk from online threats when they or their family members were affected by cyber security issues.

> "I didn't want to know about it until it happened to me and now I'm very conscious." (Halifax)

Most focus group participants perceive that information on cyber security is most reliable and trustworthy when it is from "official" sources such as their bank or internet service provider. Other sources of reliable information may be word of mouth from friends and family, or online reviews. Reliable information is also noted by many participants as any source or data that can be verified through other forums.

> "I would have to say it's the recurrence of information. If I see a video on social media about what's occurring or what's been hacked, and I only see it once, it isn't as reliable. But if it's being shared and talked about by people I know, I might start to think there's something to it." (Montreal)

11.8 Responsibility of Partners

Most participants feel that every individual should be responsible to protect themselves against online threats. However, other parties are identified as potential sources to provide information to help individuals be aware of the risks and take steps to protect themselves. Primary sources identified include internet service providers and banks (also noted as reliable sources). Some participants feel that by purchasing security software, the onus is on the software provider to protect the individual from online threats. Some also identify the police, or non-government organizations as sources with potential responsibility to provide information and ensure Canadians are prepared to protect themselves against online threats. A few identified, without probing, Provincial or Federal governments as having responsibility.

> "Canadians should do it themselves. Every time you encounter something new you should try to familiarize themselves with all the risks associated with it." (Toronto)

> "If I'm paying for a security service to look after me, I think it's their responsibility. I use Shaw, and I think Shaw should have some kind of screening also, so we've got Shaw looking for these intrusions and we've got Norton or McAfee or whoever we're using and pay for, they should be doing that for me." (Calgary)

Many feel that schools should be providing information to students in an effort to create awareness of the risks of the Internet, and create a foundation for protecting themselves. Although efforts were noted to educate students on cyberbullying, this education could be extended to talk about areas such as the amount of personal information provided online, hacking threats, and financial transactions.

> "I think it should be implemented into the education system. Not at high school, I think even younger, like elementary because there are seven year olds going on Facebook." (Toronto)

> "I think because the internet is constantly changing it is the responsibility of the Government to implement different educational programs, especially for the new generations." (Toronto)

> "Shouldn't we also have this implemented in the curriculum in schools, in the education system?" (Halifax)

11.9 Role of the Government

Many focus group participants feel that the Government of Canada should have a role to play in helping Canadians find good information about online threats and what steps to take to protect themselves. These participants cite the government as a trustworthy source of information, and perceive that information provided through the Government of Canada would have been vetted and proven reliable. Further, some feel that the government has a responsibility to protect Canadians and the scope to reach all Canadians. A few point out that the government is in a position to, and should have an interest in, helping provide information to both individual citizens and businesses. Some feel the role of the government should be to prevent cyber threats from taking place, through policy, standards, or legislation.

> “They should provide a level of awareness to companies so they put security measures in place and make users aware of them.” (Montreal)
>
> “The government should impose sanctions on wrongdoers. It’s a global problem, which is my biggest worry, and they should be able to do this around the world.” (Montreal)
>
> “It would be good if there’s some Government standards (for industries) saying ‘you have to have at least this level of protection and this kind of advertising’.” (Toronto)
>
> “I think there should be some sort of regulation and rules in regards to these large companies that are actually purchasing data and manipulating it and selling it off of us.” (Calgary)

Some are concerned about the government’s ability to provide information in an efficient manner. These participants feel that the federal government can be overly bureaucratic and would not be able to produce information to Canadians in a timely or cost effective manner; particularly given the rate at which online risks are changing. Some participants also restate that they feel it is up to the individual to protect themselves from online threats and feel uncomfortable with the idea of the government being involved with how technology is used. The credibility of the government in relaying information about cyber security is also a concern for a few participants. These participants cite data breaches of federal departments, and the inability of the federal government in preventing some online scams such as those appearing to be from the CRA, as reasons they would not trust the government as a source of information about online threats.

> “How much would that cost us though? That’s the thing.” (Toronto)
>
> “It’s a question of reputation. The Government has been hacked, numerous different Government branches have been hacked.” (Calgary)

> "People should think and take responsibility because we're the ones using the technology. Now it's getting to the point where the government is knocking on our door telling us we need to be careful. There are limits." (Montreal)

A few say that an effective model could be for the Government of Canada to provide funding to third party organizations that would specialize in providing Canadians with reliable cyber security information to protect themselves online. These organizations are viewed as being more efficient and focused than the federal government and would be considered an impartial source of information.

> "I liked the idea of a non-profit group that maybe did get some funding from different people because they're not in it for themselves, they're in it for everybody." (Halifax)

> "I think the role of the government is to give tools to institutions to ensure things are secure rather than informing us directly." (Montreal)

11.10 WEBSITE TESTING

Few focus group participants were familiar with any Government of Canada campaigns or programs to promote cyber security. Of those who did, a few say that they vaguely recall something but cannot remember any details. A few others state a general recollection of Government of Canada produced information on "cyber-tips", cyberbullying, a statement that what you post on social media doesn't go away, or the image of a hacker in a hoodie. A few mention other recollections that come to mind such as pursuing the website of the Privacy Commissioner for anti-spam legislation or that the "agency responsible" for cyber security was hiring.

Very few participants have heard of the Get Cyber Safe campaign. One recalls noticing Get Cyber Safe material on social media. A few say it is possible they may have seen Get Cyber Safe images on social media, but are accustomed to ignoring advertisements on the Internet; "I don't even notice them anymore".

Overall appearance of website

Focus group participants had various initial reactions to the website. Predominately, most were surprised and pleased that there was a Get Cyber Safe website and asked if it was currently publicly available. Most participants had an initial reaction that the website seemed to have abundant information and an "official" or government look to it. According to many participants, the "government look" of the website resulted in a feeling of trust in the website. Many were curious and excited to explore the website further.

> "Yes, I'm actually planning to check out the website, but I didn't know about it." (Toronto)
>
> "Is this up and running right now?" (Calgary)
>
> "You have a positive attitude when you open it." (Calgary)
>
> "It's a Government website so people know it's safe to use and it's reliable." (Halifax)
>
> "I had no idea this existed and I'll be sending my mother to this thing." (Halifax)
>
> "As soon as I see a website ending in .gc.ca, I know I can trust it." (Montreal)

A few, particularly those in Toronto, did not like the overall appearance of the website, citing a "dated" look, that it "seems pretty usual" with nothing that stands out, and that it doesn't appear "mobile optimized". These participants would like to see a more "interactive" approach, one that uses more icons, and a news feed approach that contains information such as "Top 5 local things happening right now".

> "It's like the Internet from 2010." (Toronto)
>
> "Can I just say a first impression? This right here, the way the website is, proves to me they can't tell me information about cyber stuff because it is just so outdated." (Toronto)
>
> "The user interface isn't very appealing. A lot of companies design websites with very attractive interfaces that give people information. It looks like a typical government website. There are no customized images." (Montreal)

A few felt the website could be improved by having a more streamlined initial page. These participants felt that with the abundant menus and content on the first page, it would be unclear where to start when looking for information. Some said that the amount of information can be overwhelming if an individual doesn't know where to start. A few asked immediately if there was a glossary of terms available.

Participants suggested efforts to improve the first page of the website such as creating a "main message", having a news feed, or a prominent listing of current threats. Some did not like the quantity of information to scroll through on the first page. A few participants did not like the flashing images on the first page, while a few others did like the images because they set a personal tone (due to the human images) and caught their attention. Although some did notice and appreciate the "Warning" box on the home page, a few were disappointed that the link did not go to an area that listed what specific current cyber security threats. A few did not like the icon and/or the warning box as it looks like there was an error on the website or reaching the website.

> "I think maybe it lacks the main message right? So when you land on the page what is this telling the user? I think maybe the sites issue is that you need a single, clear message to tell people like 'be scared of the Internet'." (Toronto)
>
> "If you don't know the terms, how do you know what to click?" (Toronto)
>
> "It looks more like a warning message than problems with cyber security. It looks like an error message." (Montreal)
>
> "I think the banner at the top take too much room. You really have to scroll down to find any information on the page." (Montreal)

Content

Most focus group participants felt that there was sufficient and relevant content on the Get Cyber Safe website. Most say it is generally important to have information on cyber security available, and the website appears to have abundant information available. Most participants noted the menu bar and drop down items to be a positive feature of the website. Participants indicated that the amount of issues covered within the website is a very positive feature and most topics that participants asked about were generally covered within the website.

> "I like the top bar. I like the cyber security, way to protect yourself, the drop downs." (Calgary)
>
> "I think it's a fabulous idea because it looks like it's a broader thing. It's also talking about cyberbullying and then possible scams so you're covering the full bases of what's out there right now. Different people are affected by different things." (Halifax)
>
> "It looks like there would be tips for how to be careful with [everything listed]." (Montreal)
>
> "I think everything is there if you bother to read through it all." (Montreal)

Some participants indicated that while the content of the website appears to be abundant, some of the information is too generalized. These participants would like to see more specific information on the various online threats. Information, for example, on an email phishing scam could show an image of an actual email and highlight what to look for to discern if the email is "real" or not, and steps to take when an individual receives a phishing email.

> "I've got this problem with all Government of Canada websites; they give you a blurb, just like this and its highlights but there's no way of going deeper." (Calgary)
>
> "When you're talking about hacking there should be an illustration there saying this is what hacking looks like, this is what spam looks like, this is what phishing looks like. Instead of just describing you've got to tell people, not just show them." (Halifax)

Some participants state that they would be concerned that the information is not up to date on the site. Particularly, some participants noted the "Last Modified" date on some pages as being years old, creating scepticism that the information would still be relevant. With how quickly technology is changing, participants say that the content on the website would need to be continuously modified and that participants would only return to the website if it is clear that the content has been updated.

> "People will go on it more often if it's specific and updated, even on a weekly basis. If I knew that this was updated on a weekly basis then as things come about then I would go to something like scams and frauds or something on a regular basis. If it was just general information you'll get someone going on maybe once maybe twice, learn what they can and then never go back." (Calgary)
>
> "Is the site up to date? Can we be confident the people who put it together would have done all the necessary research to make sure the information is current?" (Montreal)

A few would like to see an area such as a "Kid Zone" that has information for children and youth. This could contain an icon to click on with a more appealing layout and contain images and content specifically for children. As noted earlier, some focus group participants felt there is a particular need to get cyber security information to children and young adults.

> "Especially now for the younger kids, it's only going to get worse and there's going to be all the time new scams coming out and you need to be able to educate them." (Toronto)
>
> "Could make a little game on here for children." (Montreal)

A few participants did not like the campaign slogan "Get Cyber Safe". Although many did like the wording, unprompted, a few participants indicated (in both French and English language groups) that the message should be to "Stay Cyber Safe" or "Be Cyber Safe" as it seems more proactive. If an individual needs to "Get" cyber safe, perhaps it may already be too late to protect against online threats.

11.11 INFOGRAPHIC

Views were mixed regarding the infographic, although views about the intent of the product were largely positive. Several said that the information is useful and makes one stop and think. Several also said that it is an effective communications tool that is easy to follow. A few, however, said that it would be more relatable if it used an online activity that is more universal. For example, a few said it may not apply to those who do not engage in online shopping. A small number of participants also said that they are already aware of what to look for when shopping online, so would not need this type of reminder.

> "It did what it needed to do; its visual, there's not a lot of reading but it gives you the information you need to interest you to go further." (Calgary)
>
> "It would make me curious though to do what it asks you to do, go to #Mosomething to find out what happened." (Halifax)
>
> "It's very visual, so I like it. I don't have a tendency to read an entire text, so this caught my attention." (Montreal)
>
> "I might suggest a more commonplace product than a drone as well. I mean who here has used a drone?" (Calgary)
>
> "I would think 'I would never purchase something just with an email address'." (Halifax)

A primary concern expressed about the infographic is the time that it takes to get to the message, including the number of panels and/or number of seconds it takes to get to the main message. Several said that it should be in one panel, and/or that the point needs to be made within the first 10 seconds. Multiple participants mentioned the short attention span of social media users as a concern with many saying that if the content and style do not grab the audience immediately, the ad will be ignored.

> "I didn't get the purpose of the [infographic] until the third time through." (Calgary)
>
> "I feel like it would be more impactful to have a 3 framed thing where someone can see the whole thing the whole time like a comic strip. I think that would help people make the connection a bit more." (Halifax)
>
> "In that format 30 seconds is just way too long, which is sad, but in our world right now 30 seconds is too long." (Halifax)
>
> "That's the way to make content now. Make something that can be boiled down to into a ten second video and then also a three minute and then an hour podcast." (Toronto)

The second major concern to participants in most cities (Toronto excluded) is that it is not obvious, or obvious early enough that this is a Government of Canada product, which would immediately legitimize the information and message. For some, it does not have the Government look and feel and they suggest the GC branding should be made more prominent. Suggestions for changes included using common markers such as the 'Brought to you by the Government of Canada' slogan on the last slide or the 'Oh Canada' bells jingle.

> "It's about familiarity." (Calgary)
>
> "When I'm on an app like Instagram if I saw the Government of Canada logo I would be more inclined to see what they're saying." (Halifax)
>
> "People are conditioned to ignore advertising. If this looks too much like commercial advertising, people will ignore it." (Calgary)
>
> "As soon as you leave that first page you have no idea it's from the Government of Canada. If you miss that little symbol at the bottom, it could be from anyone." (Halifax)
>
> "I find Government of Canada ads on things like Instagram and Facebook very novel so I tend to think 'why do they want me to look at these things?' Cause I know they're not trying to sell me stuff." (Halifax)

For some, the lack of conclusion was bothersome and, for a few, even annoying. They felt that the final points should be clear, and that people would not go to another source to see the end of the story. As one participant put it, "this could be phishing itself, the way it's set up".

> "If I have to click again on something else I'm not going to." (Calgary)
>
> "It assumes right off the bat I'm on Twitter, and it means I have to go do something to learn more and I do not do that for anything online." (Halifax)
>
> "I absolutely hate things that do that, that are like 'here's two panels of the story, to find the rest click here'. Just tell me the story, I don't care enough to go to that page." (Halifax)
>
> "Nobody is going to #moandfriends." (Toronto)

For a few the format and approach seem too child-like and will have narrow appeal. A few also said that they would prefer to see the infographic feature some text or bullet points.

> "I think it would be taken more seriously if it had a more professional look to it." (Calgary)
>
> "I understanding wanting something welcoming, but this is too baby-like." (Montreal)
>
> "I like it. It would be good for teenagers or young adults who shop online." (Montreal)
>
> "I think short and sweet content, little bullets, whatever else to make it catchy and interesting so in five seconds I know what it means and if it's relevant to me." (Halifax)
>
> "Generally it all just seems too busy. It's got to be boiled down to the key bits." (Toronto)

11.12 Facebook Post

Some participants liked the post and found it to be useful, although some also said that they would not notice it. Those who liked the post cited features like the quick tips, and catchy introduction line as positive attributes.

> "This is good. This is the sort of thing that if I were interested in this kind of information, this is how I would want it presented." (Calgary)
>
> "It's a catchy intro, the first line there." (Halifax)
>
> "I think those (mascots) are kind of cute." (Toronto)
>
> "I think it's fine. Not everyone can understand technology or how it works, so this would speak to a lot of people." (Montreal)

A few who were less favourable about the post seemed more concerned about the large amount of text and lack of clarity in the messaging. Several also echoed the sentiment about the child-like approach to the ad expressed about the infographic.

> "Looks like its geared more to five year olds than adults." (Calgary)
>
> "I think the lingo is weird." (Calgary)
>
> "For people who don't already know what phishing is, they have no idea what you're talking about. No one know what this is." (Toronto)
>
> "I see the picture, it catches my eye and then I see there's like three paragraphs and I'm like 'hmm I don't know if this picture grabs me enough to make me want to read through three paragraphs of information." (Calgary)
>
> "It's got to be like four words." (Toronto)
>
> "The messages don't stand out and don't make me want to continue reading." (Montreal)

As with the infographic, several said that it is not obvious that this is a Government of Canada product, which should be made a priority. Related to this, several said they would be suspicious about clicking a link unless the source was clearly legitimate. It was suggested by some that the campaign should use a full length URL (with gc.ca clearly visible), as a short URL causes suspicion and is a hallmark of phishing scams.

> "You want me to follow a link from an unknown sender with a picture and a short link? No I'm good." (Calgary)

“If it was coming from the Government of Canada I would feel more comfortable clicking on the link.” (Calgary)

“The Government of Canada logo adds weight to it if it’s clearly visible.” (Halifax)

“Some people avoid the shortened URLs and I think because it’s the Government of Canada they don’t need to use the shortened URLs. I would rather it be at gc.ca.” (Halifax)

“The Government of Canada logo is missing so I’m not as inclined to trust it.” (Montreal)

Appendix A
Survey Instrument

APPENDIX A: Survey Instrument

INTRO

WEB INTRO

EKOS Research Associates is surveying people across the country on behalf of the federal Government about issues related to the use of internet-enabled devices (e.g. personal computers, cell phone, smart phones, smart TVs, tablets, etc). The survey should take approximately 20 minutes to complete. Your participation is voluntary and your responses will be kept completely confidential and anonymous. Any information you provide will be administered in accordance with the Privacy Act and other applicable privacy laws. This survey is registered with the National Survey Registration System. **A few reminders before beginning: -** On each screen, after selecting your answer, click on the "Continue" button at the bottom of the screen to move forward in the questionnaire. **-** If you leave the survey before completing it, you can return to the survey URL later, and you will be returned to the page where you left off. Your answers up to that point in the survey will be saved. **-** If you have any questions about how to complete the survey, please call Prob*it* at 866.211.8881 or send an email to online@ekos.ca. Thank you in advance for your participation.

D2

Which of the following categories best describes your current employment status? Are you ... ?

Working full-time (35 or more hours per week)	1
Working part-time (less than 35 hours per week)	2
Self-employed	3
Student attending full time school (not working)	4
Unemployed, but looking for work	5
Not in the workforce (for example, unemployed, but not looking for work, a full-time homemaker or parent)	6
Retired	7
Other (please specify)	77
No response	99
ON DISABILITY PENSION	8
MATERNAL/PATERNAL LEAVE	9

QEMP

Employed, D2

How many employees are there at all locations in your organization, including those working full and part-time?

Please specify	77
None	98
Don't know/ No response	99

QEMPB [1,2]

Full/part-time employed, D2; Fewer than 250 employees, QEMP

Do you have any of the following responsibilities:

Please select all that apply

Employees who report to you/ you oversee work of other employees	1
Involvement in decisions about processes and procedures followed by employees in your organization	2
None of these	99

D5

Are there any children under the age of 18 currently living in your household?

Yes	1
No	2
No response	9

D4

In what year were you born?

Year	1
No response	9

B1 [1,8]

What kinds of devices do you use to access the internet for **personal use**?

Please select all that apply

Desktop computer or laptop	1
Smart phone capable of accessing data, video, etc (e.g. iPhone, Android)	2
Tablet/ ereader/iPod (e.g. iPad, Amazon Kindle)	3
Home gaming system (e.g. Sony PlayStation, Microsoft Xbox)	4
Streaming service (e.g. Apple TV, Chromecast)	5
Smart TV	6
Smart watch/wearable technology	7
Smart home devices (e.g. Nest, smart locks, smart baby monitor, etc.)	8
Voice activated assistive devices (e.g., Google Home, Amazon Echo, etc.)	9
Do not know	98
No response	99

B2 [1,20]

Where do you typically access the internet?

Please select all that apply

Home using wired connection only	1
Home using wifi	2
At work	3
Public Wifi (e.g. libraries, coffee shops, malls, airports, etc.)	4
On your provider's cellular network (LTE, 3G, etc.)	5
At school	6
At the home of friends or relatives	7
Other	77

No response	99

B2B

Home wifi, B2

Do you secure your home wifi with a password?

Yes	1
No	2
Do not know	98
No response	99

B3 [1,20]

Which of the following activities have you done over the internet in the past year?

Please select all that apply

Used email	1
Financial transactions (making payments, other, banking, investments, etc.)	2
Purchased at an online store or an auction site (such as eBay)	3
Used your credit card online	4
Browse websites	5
Used social network sites/apps (Facebook, Myspace, Twitter, Snapchat, Instagram, LinkedIn, Pinterest, etc.)	6
Used app-based services (Uber, Lyft, Just Eat, Airbnb, etc)	7
Telephone or video calls via Skype or other similar applications	8
Accessed government information services	9
Viewed videos or movies (YouTube, Netflix, etc.)	10
Played online games	12
Streamed or downloaded music, podcasts, or other content	13
Participated in an online contest	14
Participated in online training course	15
Participated in blogs/discussion groups/message boards	16
Submitted applications (e.g. for employment) online	17
Read news, watched television, listened to radio	18
Downloaded software	19
No response	99

B3B [1,7]

Financial transactions, B3

How do you usually do these transactions?

Please select all that apply

From your computer at home	1
From your smartphone using a secure payment app	2
From your smartphone from your Internet browser	3
Using a voice activated device (e.g., Google Home, Amazon Echo)	4
Escrow services (e.g. Paypal)	5
Other	77
No response	99

B11 [1,8]

To your knowledge, have you ever done any of these things?

Please select all that apply

Opened an email attachment from an unknown source	1
Clicked on a link from an unknown email or text	2
Entered personal details on a computer that you did not know was secure	3
Forwarded an email or text attachment from an unknown source	4
Entered bank account or credit card information on a site that you did not know was secure	5
Replied to spam mail unknowingly	6
Replied to spoof or phishing email unknowingly	7
Entered financial information while using public Wi-Fi	8
None of these	97
Do not know	98
No response	99

K1

Canadians have expressed a wide range of views regarding their ability to protect their personal information when going online. Some are quite concerned and others are not concerned. How ***concerned*** would you say that you are about your personal information being fraudulently obtained online and used for purposes of illegal activities?

Not at all	1
Not very	2
Fairly	3
Very	4
Do not know	8
No response	9

B5

Some people take precautions to protect their computer and other devices they use to access the internet, while others do not. Do you take precautions to protect your devices?

Yes	1
No	2
Do not know	8
No response	9

B5A [1,20]

Which of the following precautions do you take, if any, to protect your devices?

Please select all that apply

Keep security software up-to-date	1
Only download files from trusted sources	2
Use spam filters	3
Verify the source before clicking on URL links or opening attachments	4
Lock the device using a password or PIN	5
Change the default password right away	14
Turn off the device when not using it	6
Back up information on my device	7
Store information in an account in the cloud	8

Use encryption software	9
Do not use administrator account when accessing the web	10
Use a password or user authentication for wireless and remote access	11
Use caution when responding to solicitations from strangers	12
Use two-step or two-factor authentication	13
None of these	97
Do not know	98
No response	99

B5B [1,20]

Which of the following precautions do you take to protect yourself against online threats and to protect your personal information?

Please select all that apply

Use passwords that contain random numbers, letters and symbols that are difficult to guess	1
Check privacy policies or terms of use on the website	2
Change my device's default password	3
Do not share passwords	4
Use caution when giving out real name, address and phone number	5
Use additional email accounts under a pseudonym/false name for organizations you don't trust	6
Do not allow my computer browser to remember passwords for websites	7
Use caution when responding to solicitations from strangers	8
Do not use administrator account when accessing the web	9
Use of encryption software	10
None of these	97
Do not know	98
No response	99

B4 [1,6]

Desktop computer or laptop, B1

Do you have anti-virus software on your computer, smartphone or tablet?

Select all that apply

Yes, for computer	1
Yes, for smartphone	3
Yes, for tablet	4
No	2
Do not know	8
No response	9

B4C

Computer, B4

How often is the anti-virus software on your computer, smartphone or tablet updated (by you or automatically) to the latest version?

Please select only one response

Daily	1
Weekly	2
Monthly	3
Yearly	4

It is not updated	5
Do not know	8
No response	9

B4D [1,20]

Smartphone, B4

People have a number of different reasons for not having anti-virus software. What is the reason that you don't have anti-virus software?

Please select all that apply

I do not know what it is	1
It would cost too much	2
I haven't had time to install it	3
I don't believe I need it for a smartphone or tablet	10
I thought my computer does it automatically	4
I don't know what to buy or how to install and run it	5
I don't go online with my computer very often	6
I only go to websites I know are safe	7
I only do activities online that I know are safe	8
I don't think I need it	9
Other (please specify)	77
Do not know	98
No response	99
Operating system not susceptible to viruses, use mac/apple/linux, do not use windows/microsoft	11
Impedes performance, slows down system, uses too many system resources	12
Antivirus software ineffective/insufficient, attracts additional viruses	13
I can take care of viruses easily myself	14
My isp (internet service provider) has an antivirus component to it	15
Other	97

B4E

No need, B4D

Why don't you feel that you need it?

Response	77
No response	99
Operating system not susceptible to viruses, use mac/apple/linux, do not use windows/microsoft	1
I only go to trusted websites, secure sites, careful user, exercise caution	2
I know how to get rid of viruses	3
Not effective, invasive, do not trust anti virus	4
Other	97

K5 [1,20]

Below is a list of some of the threats individuals can face when using the internet. Which of the following were you already aware of?

Please select all that apply

Computer/mobile devices get viruses, spyware, malware	1
Identity theft	2
Privacy violations	3
Personal data erased or changed or lost	4

Financial loss	5
Seeing or receiving information of a criminal nature	6
Device unknowingly taken over or used in other crimes	7
Destruction of computer	8
Loss of files/information (music, photos, etc.)	9
Being a victim of an online scam or fraud	10
Personal data held for ransom (i.e., locked by ransomware)	11
None of these	97
No response	99

K7 [1,7]

Which of the following have the potential of being affected by an online threat?

Select as many as apply

PC/Laptop	1
Tablet/ereaders/iPod	2
Smartphones	3
Wearable devices (e.g. fitbit, smart watch)	4
Smart TV	5
Smart home devices	6
Voice activated devices (e.g., Google Home, Amazon Echo, Apple HomePod)	7
None of these	97
Do not know	98
No response	99

QATT1

Please rate the degree to which you agree or disagree with the following statements.

QA12A2

Parents only

I can't keep up with technology/apps/games that young people are using.

Strongly disagree	1
2	2
3	3
Neither	4
5	5
6	6
Strongly Agree	7
Do not know	8
No response	9

QA12A3

Parents only

I am confident that I have the information I need to help navigate my child's online world

Strongly disagree	1
2	2
3	3
Neither	4
5	5
6	6

Strongly Agree	7
Do not know	8
No response	9

QA13

It's up to individuals to protect their own personal privacy.

Strongly disagree	1
2	2
3	3
Neither	4
5	5
6	6
Strongly Agree	7
Do not know	8
No response	9

QA15

The security of your computer could be compromised without you even knowing it.

Strongly disagree	1
2	2
3	3
Neither	4
5	5
6	6
Strongly Agree	7
Do not know	8
No response	9

QA117

Half-sample

As long as the anti-virus software that came with my computer isn't more than a couple years old, it should be good enough to protect me from online threats.

Strongly disagree	1
2	2
3	3
Neither	4
5	5
6	6
Strongly Agree	7
Do not know	8
No response	9

QA110

I am confident that businesses and other organizations have adequate security safeguards to protect my personal information.

Strongly disagree	1
2	2
3	3
Neither	4
5	5

6	6
Strongly Agree	7
Do not know	8
No response	9

QA111

Half-sample

Taking steps on how to protect myself and my family from online threats is something that everyone knows how to do and regularly does these days

Strongly disagree	1
2	2
3	3
Neither	4
5	5
6	6
Strongly Agree	7
Do not know	8
No response	9

K8

How ***likely*** is it that you or a family member will be affected by an online threat in the next 2 years?

Not at all	1
2	2
3	3
Moderately likely	4
5	5
6	6
Extremely likely	7
Do not know	8
No response	9

K8A [1,5]

Unlikely, K8

Why don't you think that it is likely that you or your family will be affected by an online threat?

Please select all that apply

Take steps to protect ourselves online	1
Do not do anything risky online	2
Think the chances are just very small	3
Online threats only apply to businesses and people with a lot of money	4
Other (please specify)	77
No response	99
Stay up to date/knowledgeable/educated about information/viruses, work in computer/information technology, educate/teach family/friends to protect themselves	5
Use apple/mac/linux which not as susceptible to viruses, do not use microsoft network	6
OTHER	97

PK2

How ***important*** do you think each of the following are:

K2A

For the average Canadian to take steps to protect **their *personal information* online**?

Not at all	1
2	2
3	3
Moderately important	4
5	5
6	6
Extremely important	7
Do not know	8
No response	9

K2B

For Canadians to take steps to protect the **security of *home computers or mobile devices, like smartphones, tablets, and other smart devices***?

Not at all	1
2	2
3	3
Moderately important	4
5	5
6	6
Extremely important	7
Do not know	8
No response	9

K6B

How ***common*** is it for Canadians to be affected by online threats?

Not at all	1
2	2
3	3
Moderately common	4
5	5
6	6
Extremely common	7
Do not know	8
No response	9

K10A

Half-sample

How familiar are you with the practice of purchasing crypto currency that can be used for online purchasing or trading?

Not at all familiar	1
2	2
3	3
Moderately familiar	4
5	5

6	6
Very familiar	7
Do not know	8
No response	9

K10B

Familiar, K10A

Have you ever purchased, traded or used crypto currency for online purchases/activities?

Yes	1
No	2
Uncertain	9

K11 [1,13]

Below is a list of steps to reduce the chances of experiencing an online threat. Some people are aware of these steps, while others are not. Which of the following were you already aware of?

Please select all that apply

Only doing banking on a computer you know is safe	1
Not sharing your passwords with others	2
Using different passwords for different accounts and websites	3
Using longer/more complex passwords	4
Not opening email attachments from people you do not know	5
Being selective in the sites you use for online shopping	6
Limiting the personal information you share online	7
Using antivirus/anti-spyware software on your computer, tablet or smartphone	8
Using firewalls and passwords to protect computers and other web-enabled devices	9
Password protecting your wireless home network	10
Avoiding using open, public wifi to do shopping or banking	11
None of these	97
No response	99

K11A [1,20]

Banking on safe computer, K11

How can you tell if a website is secure?

Please select all that apply

HERE

Know the site well	1
Site belongs to a trustworthy source (e.g. well known internet Service Provider or software provider, government, etc)	2
The site has an "https" address	3
The site has a checkmark or VeriSign authentication	4
Other (please specify)	77
Do not know	98
No response	99
Displays security lock symbol	5
Impossible, cannot fully know/know for sure, difficult to guarantee, any site can be hacked	6
Will get a warning message about security, security warnings from browser/software/computer, will say if not encrypted/if has security ticket, green/red certificate in browser	7

Go directly to site, type it in, do not use third party links/hyperlinks, avoid redirects/email links	8
Check independently through web (web of trust) or site advisor	9
Conduct research as to whether site is legitimate/safe, check url (see if registered/secured properly), use whois, check spelling of url, read comments about privacy/reputation	10
Other	97

B6

Have you ever had a *virus, spyware or malware* on your devices

(Please note - when we ask about *virus, spyware or malware* we mean: Viruses, spyware, and malware are designed to destroy data, monitor your computer use and report it back to a third party without your knowledge, or allow a third party to take control of your computer).

Yes	1
No	2
Do not know	8
No response	9

B8A

Yes, B6

How much of an impact did this *virus, spyware or malware* have on you or your family?

No impact at all	1
2	2
3	3
Moderate impact	4
5	5
6	6
Very large impact	7
Do not know	8
No response	9

B7A

Have you ever suffered financial loss or been the victim of financial fraud as a result of your online activity?

Yes	1
No	2
Do not know	8
No response	9

B8B

Yes, B7A

How much of an impact did the *financial fraud as a result of your online activity* have on you or your family?

No impact at all	1
2	2
3	3

Moderate impact	4
5	5
6	6
Very large impact	7
Do not know	8
No response	9

B7B

Have you ever been a victim of *identity theft* a result of online activity?

(Please note - when we ask about *identity theft* we mean: The unauthorized collection and fraudulent use of your personal information, usually for criminal purposes.

Yes	1
No	2
Do not know	8
No response	9

B8C

Yes, B7B

How much of an impact did your *identity theft* have on you or your family?

No impact at all	1
2	2
3	3
Moderate impact	4
5	5
6	6
Very large impact	7
Do not know	8
No response	9

PB13

Half-sample

Many people use the same passwords for different accounts and devices, and many keep the same passwords over time. How often would you say you change a password in each of the following:

B13A

Half-sample

Your social media accounts

Never	1
Every few years	2
Once a year	3
A few times a year	4
More often than a few times a year	5
Whenever I am prompted to	6
Whenever I think of it no set pattern	7
When I learn about a security breach	10
Not applicable (don't have any)	8
No response	9

B13B

Half-sample

Your online shopping accounts

Never	1
Every few years	2
Once a year	3
A few times a year	4
More often than a few times a year	5
Whenever I am prompted to	6
Whenever I think of it no set pattern	7
When I learn about a security breach	10
Not applicable (don't have any)	8
No response	9

B13D

Half-sample

Your email accounts

Never	1
Every few years	2
Once a year	3
A few times a year	4
More often than a few times a year	5
Whenever I am prompted to	6
Whenever I think of it no set pattern	7
When I learn about a security breach	10
Not applicable (don't have any)	8
No response	9

B14 [1,20]

Which of the following do you do, if any?

Please select all that apply

Share a password with your friends	1
Write down your passwords	2
Use the same passwords for multiple accounts	3
Use a password keeper	4
Allow your browser to remember your passwords	5
Make your passwords complex with a combination of letters, numbers and symbols	6
Keep your passwords simple and easy to remember	7
Use a multi-step or multi-factor authentication	8
Use a biometric protection (e.g. fingerprint lock, facial recognition)	9
Other	77
None of these	97
No response	99

B16

Half-sample

How likely are you to take precautions against online threats as you are to take precautions against "in-person" threats? As an example, how likely are you to avoid posting vacation pictures and information on social media while you are away as you are to cancel deliveries or ask neighbours to watch your home while you are away?

Not nearly as likely as in-person 1	1
2	2
3	3
As likely as in-person 4	4
5	5
6	6
Much more likely than in-person 7	7
No response	99

IC5A [1,20]

Which of the following types of online threats have you looked for information on, if any?

Please select all that apply

Protecting devices with anti virus software	1
How to know if an email is a scam	2
Things you can do to protect your computer files	3
Steps you can take to use public wifi safely	4
Steps you can take to use social networking sites safely	5
PARENT = 1	
Internet safety for your children	6
Internet safety for seniors	7
Things you can do to protect your mobile devices	8
Definition of terms (glossary) about internet safety or cyber security	9
Cyberbullying, online harassment	10
Securing home networks/wifi	11
Steps you can take to protect other internet connected devices (e.g. smart TVs, home security systems, fitness monitors, voice activated devices such as Google Home and Amazon Echo)	12
Other	77
None of these	97
No response	99

IC5B [1,15]

1-8, IC5A

Where did you go for that information?

Please select all that apply

Web site of software or hardware vendor	1
Friends and family	2
Media	3
Web site of a non-profit group	4
Newsletter	5
Government web site	6
Employer IT dept	7

School	8
Search engine (e.g. Google, Bing, etc.)	9
Law enforcement website	10
Other (please specify)	77
Do not know	98
No response	99
Computer technician, it professional/consultant	11
Internet service provider	12
Discussion forums, blogs, message boards	13
Computer stores, staff at stores, stores that sold them the computer	14
Bank/financial institutions	15
Books, magazines, articles/journals	16
Sites specifically for security news/updates, independent sites of experts, specialized debunkers of misinformation (various, e.g.:: snopes.com)	17
Other	97

QATT2

Please rate the degree to which you agree or disagree with the following statements.

QA211

I feel I have enough information to know how new technologies might affect my personal privacy.

Strongly disagree	1
2	2
3	3
Neither	4
5	5
6	6
Strongly Agree	7
No response	9

QA211B

I feel I have enough information on how to take steps to protect myself and my computer against online threats.

Strongly disagree	1
2	2
3	3
Neither	4
5	5
6	6
Strongly Agree	7
No response	9

QA218

I am confident that I could protect myself online as long as I have basic and trustworthy information on steps to take.

Strongly disagree	1
2	2
3	3
Neither	4

5	5
6	6
Strongly Agree	7
No response	9

PQA22

Parents only

As a parent of a youth, how concerned are you, if at all, about each of the following:

QA22A

Parents only

Cyberbullying, online harassment

Not at all concerned	1
2	2
3	3
Moderately concerned	4
5	5
6	6
Extremely concerned	7
Do not know	8
No response	9

QA22B

Parents only

Your child's privacy

Not at all concerned	1
2	2
3	3
Moderately concerned	4
5	5
6	6
Extremely concerned	7
Do not know	8
No response	9

QA22C

Parents only

Legal implications of your child downloading copyrighted materials (e.g. music, books, movies)

Not at all concerned	1
2	2
3	3
Moderately concerned	4
5	5
6	6
Extremely concerned	7
Do not know	8
No response	9

QA22D

Parents only

Legal implications of your child sharing pictures or content of others under 18

Not at all concerned	1
2	2
3	3
Moderately concerned	4
5	5
6	6
Extremely concerned	7
Do not know	8
No response	9

QA22X [1,7]

Parents only; Not concerned, QA22D

Why is it that you are not concerned?

Please select all that apply

I never really thought about it	1
I don't know what the issues are to be concerned about	2
I have looked for information and talked with my child about these issues	3
My child has received information and instructions at school on these issues	4
My child has looked for information and told me about what they do to avoid risks	5
I just trust my child to know what to do	6
My child isn't online very much	7
Do not know	8
No response	9

IC6 [1,15]

Who would you trust to give you the best **technically reliable and up-to-date information** about online threats and steps you can take to protect yourself?

Please select all that apply

Friends or family	1
Internet Service Provider	2
Security Software company	3
Financial Institutions	4
Vendor website (e.g. online store where you are shopping, etc.)	5
Not-for-profit organization dedicated to electronic security	6
Government	7
Law enforcement organization	8
Other (please specify)	77
Do not know	98
No response	99
It personnel/computer/security technician, computer consultant, software programmers/experts (includes it staff from work)	9
Computer store/vendor, retail outlets/software vendor, geek squad from best buy	10
On line sources (e.g.: forums/blogs/podcasts/websites/online articles	11
Television, magazines, newspapers, radio	12
Computer manufacturer	13
Through work, my employer, work employees	14

Myself	15
No one, these sources are the problem, none of the above	16
Other	97

IC7 [1,15]

And who would you trust to give you the most **unbiased** information about online threats and steps you can take to protect yourself?

Please select all that apply

Friends or family	1
Internet Service Provider	2
Security Software company	3
Financial Institutions	4
Vendor website (e.g. online store where you are shopping, etc.)	5
Not-for-profit organization dedicated to electronic security	6
Government	7
Law enforcement organization	8
Other (please specify)	77
Do not know	98
No response	99
It personnel/computer/security technician, computer consultant, software programmers/experts (includes it staff from work)	9
Computer store/vendor, retail outlets/software vendor, geek squad from best buy	10
On line sources (e.g.: forums/blogs/podcasts/websites/online articles	11
Television, magazines, newspapers, radio	12
Computer manufacturer	13
Through work, my employer, work employees	14
Myself	15
No one, these sources are the problem, none of the above	16
Other	97

IC8

When someone talks about "fake news" in connection with information that people/consumers need to protect themselves, do you think that this typically refers to:

Information that is from a biased source (i.e., someone/individual/company/political party)	1
that stands to gain from misinformation consumer use)	2
Information from a source that is not transparent (i.e., hidden or falsely	3
attributed to a more reputable source)	4
Information that is falsely used to shape opinion or facts	5
Parodies intended as a joke, that are presented as factual (i.e., The Onion)	6
Other (specify)	77
Don't know	99

IC10

1-5, IC8

How can consumers tell that information about online threats is "fake news"?

Response :	77
Don't know	99

IC11

Half-sample

Who should play a role in helping Canadians recognize what is "fake news" when it comes to information about online threats and consumer protection?

Government	1
Not for profit organizations dedicated to electronic security	2
Software providers	3
Internet service providers	4
Manufactures of the devices	5
Retailers of devices (computers, mobile devices)	6
Teachers	7
Other (please specify):	77
Do not know	98
No response	99

B10 [1,20]

As far as you know, who is primarily responsible for ensuring that personal devices that Canadians use to access the internet with (e.g. computer, smart phone, tablet, other smart devices etc.) are safe and secure?

Please select all that apply

Individual owners of the devices	1
Private sector	2
Government	3
Not for profit organizations dedicated to electronic security	4
Software providers	5
Internet service providers	6
Manufactures of the devices	7
Retailers of devices (computers, mobile devices)	8
Other (please specify)	77
Do not know	98
No response	99
Nobody	9
Website owners where information should be protected (e.g.: bank websites...)	10
Other	97

GOCAD

Have you seen, heard or read any Government of Canada advertising or websites related to the use of internet-enabled devices and security of online activities?

Yes	1
No	2
Do not know	99

GOCEDU

The Government of Canada has a public education campaign in place to tell Canadians about the importance of taking steps to protect yourself from online threats, along with some steps to think about. Do you recall seeing, hearing or reading anything like this from the Government of Canada?

Yes	1
No	2
Do not know	99

DEMIN

These last questions are about you and will be used strictly for statistical purposes to understand the results of the survey.

D1C

How many hours do you spend online each day?

Enter number of hours	77
Do not know	98
Prefer not to say	99

D1B [1,3]

Thinking about data storage of information for personal use, do you save information on your computer hard drive, an external hard drive (i.e., extra storage / back up), or on a "virtual server" (i.e., cloud computing)?

Save files on computer hard drive	1
Save files to an external hard drive	2
Save files on a "virtual server"/in a cloud	3
Do not know	8
Prefer not to say	99

B5X

How often do you back up data/personal files stored on your computer, smartphone or tablet?

Never	1
Once or twice a year	2
Every few months	3
Once a month	4
A few times a month	5
Weekly or more often	6
Don't know	99

D11

Are you ...

Male	1
Female	2
Other	3

Prefer not to say	99

D3

What is the highest level of formal education that you have completed to date?

Elementary school or less	1
Secondary school	2
Some post-secondary	3
College, vocational or trade school	4
Undergraduate university program	5
Graduate or professional university program	6
Prefer not to say	99

D6

Which of the following categories best describes your total household income? That is, the total income of all persons in your household, before taxes?

Under $20,000	1
$20,000 to just under $40,000	2
$40,000 to just under $60,000	3
$60,000 to just under $80,000	4
$80,000 to just under $100,000	5
$100,000 to just under $150,000	6
$150,000 and above	7
Prefer not to say	99

D7

What is the language you first learned at home as a child and still understand?

English	1
French	2
Other	77
Prefer not to say	99

D9

Were you born in Canada?

Yes	1
No	2
Do not know	98
Prefer not to say	99

D5B

Parents only

How old is your oldest child still living at home?

Year(s)	1
Prefer not to say	99

D5C

Parents only, 11 or younger, D5B

Do any of your children use a computer or mobile device to access the internet?

Yes	1
No	2
Prefer not to say	99

BUS1 [1,20]

Responsible, QEMPB; Self-employed, D2

Turning to your work as a business owner/manager, which of the following steps has your business taken to protect itself against online threats?

Select all that apply

Keep security software up-to-date on all machines	1
Set spam filters	2
Require password protection on all devices	3
Back up information on all devices	4
Use encryption software	5
Do not use administrator account when accessing the web	6
Use a password or user authentication for wireless and remote access	7
Follow information removal protocols when employees leave the organization	8
None of these	97
Do not know	98
Prefer not to say	99

BUS2 [1,20]

Responsible, QEMPB; Self-employed, D2

Which of the following instructions do you provide to employees to protect the organization against online threats and to protect your personal information?

Select all that apply

To use passwords that contain random numbers and letters that are difficult to guess	1
To check privacy policies on the website	2
To read terms of service/use of a website, app or social media platform	3
To change my default password	4
Not to give out password without calling to verify that the request is legitimate	5
To only download from trusted sources	6
To only click on attachments or URLs from trusted sources	7
Not to allow my computer browser to remember passwords for websites	8
To use caution when responding to solicitations from strangers	9
To use of encryption software	10
None of these	97
Do not know	98
No response	99

BUS3 [1,20]

Responsible, QEMPB; Self-employed, D2

Which of the following types of information do you feel that your organization would benefit from having to protect itself against online threats?

Select all that apply

A list of the types of threats that exist and cues to look for	1
Tips on communicating the importance of following cyber security policies to employees	2
Best practices for a clear internet usage policy	3
Guidelines to establish rules for safe email usage policies	4
Guidelines on how to establish strong social media policy	5
Tips/resources for the type of software/hardware to make networks secure	6
Best practices for how employees on how to handle passwords	7
Steps to protect mobile devices in a public setting	8
Steps for handling work-related information possessed by departing employees	9
Guidelines for reacting to a cyber attack	10
Best practices for safe cloud computing (with definition of cloud computing)	11
Best practices for use of storage devices (e.g. USBs)	12
Resources on how to encrypt computers, laptops, and storage devices	13
Guidelines on use of personal devices for work	14
Other	77
None of these	97
Do not know	98
Prefer not to say	99

BUS4 [1,20]

Responsible, QEMPB; Self-employed, D2

Who is responsible for your company's IT?

Select all that apply

Me	1
Another employee (specify role in company) BOXBUS4	2
An employee of the organization dedicated to IT	3
Outsource to an IT firm	4
Other	77
None of these	97
Do not know	98
Prefer not to say	99

BUS5A

Responsible, QEMPB; Self-employed, D2

Thinking about the various concerns of daily operations of your organization, how worried would you say you are about work disruptions or financial loss as a result of online threats?

Not at all concerned	1
2	2
3	3
Moderately concerned	4
5	5
6	6

Extremely concerned	7
Do not know	98
Prefer not to say	99

BUS5B

Unconcerned, BUS5A

Why is this?

I never really thought about it	1
I don't know what the issues are to be concerned about	2
We have researched this and taken steps to protect ourselves	3
The threat for a company like ours is very low	4
There are bigger issues to worry about than cyber attacks	5
You can't really protect yourselves against cyber attacks if it's going to happen, there's isn't much you can do	6
Other	77
None of these	97
Do not know	98
Prefer not to say	99

THNK

The Government of Canada, and EKOS, thank you very much for your time.

That concludes the survey. This survey was conducted on behalf of the Public Safety Canada. In the coming months, a report with the findings from this study will be available from Library and Archives Canada. Thank you very much for taking part. It is appreciated.

THNK2

Screened out

Thank you for your cooperation! Based on the information you have provided, unfortunately you are not eligible to complete the remainder of this survey.

APPENDIX B
FOCUS GROUP RECRUITMENT SCRIPT

APPENDIX B: Focus Group Recruitment Script

Hello, my name is ________________ from EKOS Research. We are conducting a series of focus group discussions with Canadians who are 16 years of age or older on behalf of the Government of Canada. The research is related to use of Internet-enabled devices and security issues of concern to all Canadians and we think that you'll find the topic interesting.

Your participation in the research is completely voluntary and your decision to participate or not will not affect any dealings that you may have with EKOS Research or the Government of Canada. The purpose of the research is to understand the opinions and experiences of Canadians not to sell any service or product.

The sessions will be audio and video recorded for research purposes. Representatives of the Government of Canada will also be observing the discussions. The information is being collected under the authority of the Privacy Act and other applicable privacy laws. The full names of participants will not be provided to the government or any other third party. Also, the results from the discussions will be grouped together in a report, which will contain non-identifying information. May I continue?

Yes	1
No	2

Q1

The session will last an hour and a half and an incentive is offered for participation. May we have your permission to ask you some further questions to see if you fit in our study?

Yes	1
No	2

QGENDR

Record gender of respondent (DO NOT ASK)[ELSE]Are you...>

Male	1
Female	2

QAGEX

May I have your year of birth, please?

RECORD YEAR :	77
REFUSED	99

QEDUC

What is the highest level of formal education that you have completed to date?

Grade 8 or less	1
Some high school	2
High school diploma or equivalent	3

Registered Apprenticeship or other trades certificate or diploma	4
College, CEGEP or other non-university certificate or diploma	5
University certificate or diploma below bachelors level	6
Bachelor's degree	7
Post graduate degree above bachelor's level	8
Don't know / No answer	9

QINCOME – ASK ONLY OF 19+

Which of the following categories best describes your total household income? That is, the total income of all persons in your household, before taxes?

Under $20,000	1
$20,000 to just under $40,000	2
$40,000 to just under $60,000	3
$60,000 to just under $80,000	4
$80,000 to just under $100,000	5
$100,000 to just under $120,000	6
$120,000 to just under $150,000	7
$150,000 and above	8
Don't know / No answer	9

D2

Which of the following categories best describes your current employment status? Are you ... ?

Working full-time (35 or more hours per week)	1
Working part-time (less than 35 hours per week)	2
Self-employed	3
Student attending full time school (not working)	4
Unemployed, but looking for work	5
Not in the workforce (for example, unemployed, but not looking for work, a full-time homemaker or parent)	6
Retired	7
Other (please specify)	77
No response	99

Q2

Are you or is any member of your household or immediate family employed in:

Q2A

Government of Canada

Yes	1
No	2

Q2B

An advertising agency

Yes	1
No	2

Q2C

A market research company

Yes	1
No	2

Q2D

The media (Print, Radio, TV, Internet)

Yes	1
No	2

NOTE: If a response of “YES” to any of the above (Q2a-Q2D) Thank and Terminate →THNK2

Q3

Participants in group discussions are asked to voice their opinions and thoughts. How comfortable are you in voicing your opinions in front of others, in English? Are you...

Very Comfortable	1
Comfortable	2
Fairly Comfortable	3
Not Very Comfortable	4
Very Uncomfortable	5

Q4

Have you ever attended a focus group or one to one discussion for which you have received a sum of money?

Yes	1
No	2

Q5

When did you last attend one of these discussions that was sponsored by the Government of Canada?

Please specify :	77
Months	1
Years	2
Never	999

Calculate:

Within last 6 months, thank and terminate	1
Continue	99

Q5B

Have you attended more than 6 of these discussions that were sponsored by the Government of Canada?

Yes	1
No	2

QEMP

How many employees are there at all locations in your organization, including those working full and part-time?

Please specify	77
None	98
Don't know/ No response	99

QEMPB [1,2]

Do you have any of the following responsibilities:

Please select all that apply

Employees who report to you/ you oversee work of other employees	1
Involvement in decisions about processes and procedures followed by employees in your organization	2
None of these	99

QFOCUS

The focus group is about an hour and 30 minutes in length, but we are asking that all participants arrive 10 minutes prior to the start time of the session. Are you able to be at the facility 10 minutes prior to the session time?

Yes	1
No	2

QTELE

We are providing each participant with a $85 cash incentive for their participation, although late arrival (i.e., more than a few minutes) may result in not being able to participate or receive the incentive. Replacements are not permitted and you will need to bring ID, which you may be asked to present on arrival for the discussion. If you usually use reading glasses you should bring those along as well because there may be a few short phrases to read throughout the discussion.

We will be giving you a reminder telephone call and sent an email or if you prefer, a text, a day or two prior to your group discussion. What is your preferred method of receiving a reminder?

Email

Text

Phone call

If phone/text:

Is this the best number at which to reach you?

If email, please provide your email address

FNAME

Please provide your first and last names.

NOTE TO INTERVIEWER: Confirm proper spelling. Ensure proper capitalization (IE: not all upper or lowercase).

Name :	1

THNK

If you have any questions or something comes up and you can no longer participate in the discussions, please let us know by calling us toll-free at XXXXXXXXX or by sending an email to XXXXXXX. Thank you for your cooperation and time.

APPENDIX C
FOCUS GROUP MODERATOR'S GUIDE

APPENDIX C: Focus Group Moderator's Guide

1. INTRODUCTION

- I represent EKOS Research and these groups are being conducted for Public Safety Canada to explore perceptions regarding exposure to online threats and steps that Canadians can take to protect themselves online.
- This research will help the Government of Canada plan communications activities designed to make Canadians aware of various risk factors related to online activities, and steps they can take to reduce their risk.
- This group is part of a series of focus groups taking place across Canada. This session will last about an hour and a half and we can start by going over the format and "ground rules":
    - Discussion is being audio taped and video recorded so that I can listen closely to what you are saying and not be distracted by having to write things down.
    - There are observers from the Government of Canada.
    - All comments are confidential.
    - Please try to speak one at a time and be respectful of one another's opinions.
    - There are no right or wrong answers to the things we'll be talking about.
    - It's okay to disagree. Please speak up even if you think you're the only one who feels a certain way about an issue. Everyone may have different experiences and different points of view. And we want to hear everyone's opinions.
- Moderator's role: raise issues for discussion, watch for time and make sure everyone has a chance to participate. We do not work for the Government of Canada.
- Please make sure that your cell phones, notifications on smart watches, etc. are turned off. We ask for your full attention for this time, without distractions.

2. Introduction

1. Let's start by going around the table. Tell me your first name, and who you have in your household?

2. What kinds of devices do you and others in your household use to access the Internet?
   a. How many use voice activated assistance, like Google Home or Amazon "Echo" types of devices to do things online?

3. What kinds of activities do you and others in your household do online (e.g., financial transactions, online shopping, social media, app-based shared services like Uber/Airbnb, online games)?
   a. How many of you use phone-based apps to make payments on the go?

3. Awareness and Concerns

4. Do you feel there are any security issues that pose a risk to you and your family when you are engaged in online activities?
   a. What are the nature of the risks that concern you (financial theft, identity theft, breach of privacy, loss of information/data, other?)

5. Do you currently take any action to prevent these risks?
   a. What kinds of actions do you take?
   b. Do you feel it works? Do you feel like you are making a difference?

6. How confident are you that you know how to protect yourself? How have you decided what steps you will take and what you won't?
   a. Is it about feeling you are aware of the risk and have information about steps you can take to protect yourself and your family from online threats?

7. For those of you not taking any steps or for those of you who think you could do more, what are the things that hold you back from taking steps or making changes to prevent risk?
   a. How much is it about knowing if something does pose a risk or not (i.e., recognizing the risk)? Or knowing what to do about it?
   b. Do you feel that it is up to others to address these things not you?

8. Does it feel just as "real" when it happens online or do you have to remind yourself about protecting yourself online? For example, does someone stealing your belongings feel more real or more like a real threat, than someone stealing your identify online?

4. Information & Role of Government

9. Do you feel like you have enough information to adequately take steps to protect you and your family from online threats?

10. What got you started thinking about or taking steps to mitigate risk from online threats? Did you go looking for information or did you happen upon it or learn from friends and family?

11. Where have you looked for this information? Where have you found information that was useful to you?

12. How can you tell if the information you are getting is reliable and trustworthy? Unbiased?
    Is it hard to tell who/where information is coming from and whether it's a trusted source

13. Whose responsibility do you think it is to ensure that Canadians are prepared to protect themselves against online threats?

14. Do you feel it is the Government of Canada's responsibility to inform the Canadian public about the potential for online threats and steps everyone can take to protect themselves from online risks? Why or why not?

15. Could the GC have a role to play in helping Canadians find good information that helps them to know what steps to take?
    a. In what way would that be helpful?
        i. Finding information
        ii. Access to trustworthy and unbiased information
        iii. Easy to understand information? Tips sheets on things to thing about
        iv. Other?

16. Are you familiar with any Government of Canada campaigns or programs to promote cybersecurity?

17. Have you heard of Get Cyber Safe?

5. Website Testing

Now we are going to look at a Government of Canada website on cyber safety and get everyone's reaction to various elements of it. This is the Get Cyber Safe website that is part of the campaign.

18. Let's have a look at the website homepage. What do you think of the overall look and layout of the page?
    a. Is it appealing? Does it command attention / is it compelling (i.e., makes you curious to know what it's about and keep looking)?
    b. What stands out most on the page?
    c. Is there anything about it that turns you off right away (tone, images, information)?

19. Does it feel like this is a trustworthy site?
    Why do you feel that way (GC site, good information, look and feel of site?)

20. Does it seem like a site that you could get useful/informative information from? Would you visit it and read the information there?
    a. Is it the right kind of information (i.e., information Canadians should have)?
    b. Does it seem like the right level of detail for a public campaign? Why or why not?

21. Let's look at how the content is organized. There is a section for social media posts with added information. There are menus along the top. Let's have a look at the headings and a few of the topics under each.
    a. How do you feel about the organization of the page overall?
    b. How do you feel about the menus - how they are organized, topics under each?
    c. Is there anything that you feel should be changed, added or done differently? What and why?

22. Have a look at an infographic the Government is developing. What do you think of it?
    Is it clear?
    a. How about this FaceBook ad?

23. Overall, does the site encourage you to think carefully about the type of online threats you and your family may be exposed to, and the steps you take or need to take to protect yourself from online threats?
    a. Does it make you want to look for more information?

6. Wrap up

24. Is there anything that we haven't talked about or that you would like to add before we go?

THANK YOU