Government of Canada Gouvernement du Canada

Get Cyber Safe Awareness Tracking Survey

Final Report

Prepared for Communications Security Establishment

Supplier: EKOS RESEARCH ASSOCIATES INC.

Contract Number: 2L165-200745/001/CY

Contract Value: $82,958.08

Award Date: March 2, 2020

Delivery Date: March 31, 2020

Registration Number: POR 086-19

For more information on this report, please contact CSE at: media@cse-cst.gc.ca

Ce rapport est aussi disponible en français

Canada

Get Cyber Safe Awareness Tracking Survey

Final Report

Prepared for Communications Security Establishment
Supplier name: EKOS RESEARCH ASSOCIATES INC.
Date: March 31, 2020

This public opinion research report presents the results of an online survey conducted by EKOS Research Associates Inc. on behalf of the Communications Security Establishment. The research study was conducted with 2,700 Canadians between March 16, and 29, 2020.

Cette publication est aussi disponible en français sous le titre : Sondage de suivi sur la connaissance de la campagne Pensez cybersécurité.

Communications Branch
Public Services and Procurement Canada
Portage III Tower A
16A1-11 Laurier Street
Gatineau QC K1A 0S5

Catalogue Number:
D96-17/2020E-PDF

International Standard Book Number (ISBN):
978-0-660-34869-8

Related publications (registration number: POR 086-19):

TABLE OF CONTENTS

LIST OF TABLES

LIST OF CHARTS

EXECUTIVE SUMMARY

A. 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 proposed research are as follows:

- Assess performance of the public awareness campaign.
- Profile awareness, attitudes and behaviour relating to cyber security among the campaign target audience(s) for the public awareness campaign.
- Identify and track motivators and barriers to behaviour change.
- Identify and track the best ways of communicating such information.

B. METHODOLOGY

The sample consists of 2,710 completed interviews with Canadians 16 years of age or older who use the Internet on a regular basis, including 350 interviews with youth between the ages of 16 and 24, and 350 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 panel of more than 120,000 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 15,312 was drawn from the online only portion of the Prob*it* panel and survey cases were 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 18 per cent. The final survey sample of 2,710 yields a level of precision of +/-1.9 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 14 cases in English and 10 cases in French. The bilingual survey was administered online between March 16 and 29, 2020. The database was subsequently reviewed 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.

C. Key Findings

Level of Concern

Most Canadians do not feel it is likely they will be affected by a cyber threat. Less than one in five are concerned that they will be affected by a cyber threat causing their personal information to be compromised and less than one in ten are concerned they would experience a threat that results in financial loss or the loss of files or photos. Combining the likelihood across the three areas, however, one in five Canadians believe it is likely that they will experience a cyber threat in the next year, largely driven by the higher likelihood of compromised personal information. Just over one in three believe they are unlikely to experience a threat in any of the three areas. Slightly more, over one-quarter, believe it is likely that a friend of family member will be affected by a cyber threat in the next year. When thinking about cyber threats, three in four Canadians are concerned about identity theft. Other threats on the mind of Canadians are financial loss, followed by general viruses, spyware or malware.

Awareness

For most Canadians who say they are not concerned about cyber threats, it is because they say they take steps to protect themselves online or that they do not do anything risky online. A portion of Canadians are aware of some steps to take to verify that a website is secure. The majority look for a website from a trustworthy source, such as a well-known software provider or a government website. Less than half only use websites that they know well, look for the "https" address as their method of verifying that a website is secure, verify a site through the security lock symbol or a checkmark or VeriSign authentication.

One in four Canadians feel they are not prepared to face cyber threats, primarily because they feel one can never really be protected online. In fact, two in five say they have been the victim of a virus, spyware, or malware on their computer and over one-quarter have been victimized by an email scam. Other cyber attacks experienced have included text scams, social media account hacks, or identity theft.

In the event of a cyber attack, four in five Canadians would change their passwords. Over two in three would reach out to their bank if they were the victim of a cyber attack. Slightly fewer say they would delete suspicious material or update security software.

Precautions

Similar to 2018, nearly nine in ten Canadians take precautions to protect their online and social media accounts, devices and networks. However, nearly two in three admit that they change some passwords more than others. One in four change passwords at least a few times a year, but one in ten never change their password. Passwords for online bank accounts are changed most often (by three in five). The majority say it is best to make passwords complex with a combination of letters, numbers and symbols.

Over half of Canadians use a multi-factor authentication in some form of their online activity. For these Canadians, authentication most often involves a code received by text (for four in five), followed by passwords, a code received by email, or PINs for two in three. Most Canadian households, nine in ten, secure their Wi-Fi with a unique password; however, only one in six use a separate password for visitors.

Nearly three in four Canadians save their files on a computer hard drive. Over half store their data on an external hard drive and fewer, although higher than in 2018, have implemented a virtual server or cloud. For one in five, data and personal files stored on the computer, smartphone, or other mobile device are automatically saved to the cloud. A similar proportion manually back up their files once or twice per year; one in six never back up their files.

Information

Just under half of Canadians have looked up information on how to tell if an email is a scam or other information about types of cyber security threats. Over one-third have looked for information on securing home Wi-Fi or how to protect mobile devices. This information was found by three in five Canadians by using a search engine. About three in ten found information through the media, including a news organization's website, a government website, a software or hardware vendor's website, or through friends and family. An employer's IT department was a source of information for one-quarter of those who searched for information. Just over one in four found the information helpful because of their confidence in the source of the information.

Over half of Canadians prefer to get information on cyber security protection through websites. Three in ten prefer check lists on what to do or fact sheets and infographics. One in five say they prefer instructional videos, social media, stories of how people have been affected, or newsletters such as email subscriptions.

Three in ten Canadians help others with their cyber security. For six in ten, this includes parents or friends. Less than half help other relatives. About three in ten help co-workers or their children.

As found in 2018, if provided trustworthy information, two in three Canadians feel confident that they could protect themselves online. Over three in five agree it is up to individuals to protect their own personal privacy or are confident they know how to find practical information online to protect against cyber threats.

Very few have heard of the Get Cyber Safe campaign. Of the nearly one in ten who stated awareness when prompted with the name, three in ten read about it on social media. One quarter saw a segment on the news or social media. Nearly one in five heard about it through a radio show or podcast, saw a video online, visited the GetCyberSafe.ca websites, or was told about it by someone.

Experience of Business

Among the concerns business owners or managers have in daily operations, only about one in four are concerned about work disruptions, financial loss, or damage to the organization's reputation due to a cyber threat. Similar to 2018, two in five are not concerned because they feel the threat for their type of company is very low. One in five have researched and taken steps to protect their business online. Just over half of business owners or managers report that their business has implemented password protection on all devices, use password or user authentication for wireless and remote access, or kept security software up to date on all machines.

Two in five business owners or managers say that their organization would benefit from a list of the types of threats that exist and clues to look out for, guidelines for reacting to a cyber attack, or steps to protect mobile devices in a public setting. Over three in ten would see value in information on best practices for safe cloud computing, resources on how to encrypt computers, laptops, and storage devices, best practices for use of storage devices, or guidelines on use of personal devices for work. About one in four indicate their organization would benefit from tips on the type of software/hardware to make networks secure, best practise for employees on how to handle passwords, guidelines to establish rules for safe email usage policies, guidelines on how to establish strong social media policy, tips on communicating the importance of following cyber security to employees, best practices on a clear internet usage policy, or having information on steps for handling work-related information possessed by departing employees.

D. Note to Readers

Detailed findings are presented in the sections that follow. Overall results are presented in the main portion of the narrative and are typically supported by graphic or tabular presentation of results. Bulleted text is also used to point out any statistically and substantively significant differences between sub-groups of respondents. If differences are not noted in the report, it can be assumed that they are either not statistically significant[1] in their variation from the overall result or that the difference was deemed to be substantively too small to be noteworthy. The programmed survey instrument can be found in Appendix A. Details of the methodology and sample characteristics can be found in Appendix B.

It should be noted that the survey asks a number of questions about behaviours that may have a tendency to exert social desirability pressure for respondents to underreport risky online practices[2]. Results for the proportion of respondents in the sample who either said "don't know" or did not provide a response may not be indicated in the graphic representation of the results in all cases, particularly where they are not sizable (e.g., 10% or less). Results may also not total to 100% due to rounding.

E. Contract Value

The contract value for the POR project is $82,958.08 (including HST).

Supplier Name: EKOS Research Associates
PWGSC Contract Number: 086-19
Contract Award Date: March 2, 2020
To obtain more information on this study, CSE at: media@cse-cst.gc.ca

[1] Chi-square and standard t-tests were applied as applicable. Differences noted were significant at the 95% level.

[2] Ivar Krumpal, "Determinants of Social Desirability Bias in Sensitive Surveys: A Literature Review", Quality and Quantity, June 2013, Volume 47, Issue 4, pp. 2025-2047.

F. Political Neutrality Certification

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: ______________________

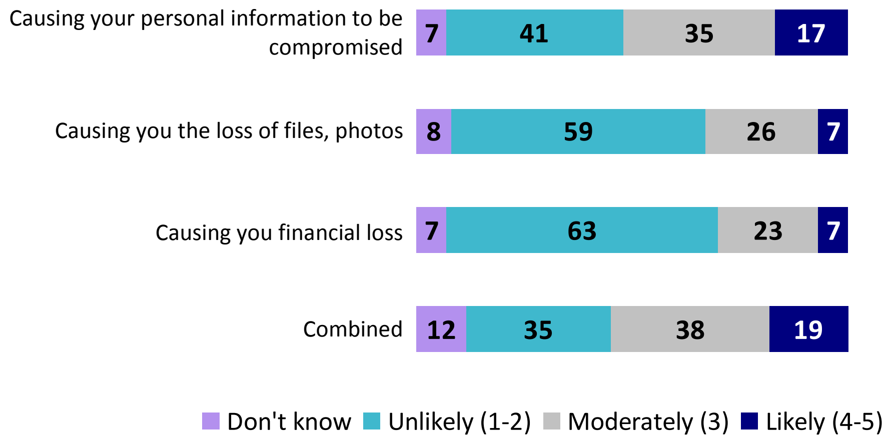
Susan Galley (Vice President)

Detailed Findings

A. Level of Concern/Likelihood of Incident

Over the next year, nearly one in five (17%) feel it is likely that they will be affected by a cyber threat causing their personal information to be compromised; two in five (41%) feel it is unlikely. Most Canadians feel that cyber threats will not affect them, with less than one in ten believing they would experience a threat that results in financial loss (7%) or the loss of files or photos (7%). Overall, combining the likelihood across the three areas, one in five Canadians (19%) believe it is likely that they will experience a cyber threat in the next year, largely driven by the higher likelihood of compromised personal information. Just over one in three (35%) believe they are unlikely to experience a threat in any of the three areas.

Chart 1: Likelihood of Threats



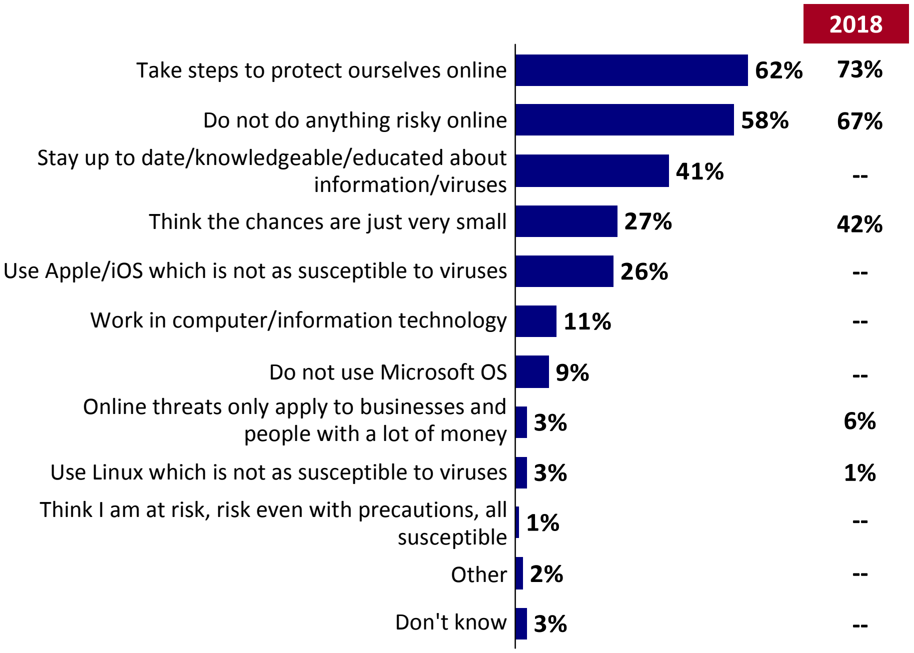
Q11abc. In the next year, how likely do you feel that you will be affected by a cyber threat...?
Base: n=2710

- Less likely to feel they would have their personal information compromised are those under 35, and residents of Alberta compared with others. Those more likely to feel open to being affected are residents of Quebec and individuals with a university education and households of $150,000 or greater, as well as parents of children five or older, compared with their counterparts.

- In terms of both financial loss as well as loss of files, it is those who are 25 to 34, residents of Ontario and individuals with households of $150,000 or greater, as well as men who feel less likely to be affected compared with their counterparts.

Among those who are not concerned, the majority say that it is because they take steps to protect themselves online (62%) or that they do not do anything risky online (58%). Two in five (41%) indicate they feel unlikely to be affected because they stay informed about viruses. About one-quarter feel they are unlikely to be affected because they perceive the chances of being affected are very small (27%) or that they use Apple/iOS which is not as susceptible to viruses (26%).

Chart 2: Why Unlikely to Be Affected



QK8a. Why don't you think that it is likely that you will be affected by a cyber threat?
Base: n=1941 (Indicated unlikely to be affected by financial or file loss, or have personal information compromised), 2018: n=492 (Unlikely to be affected by online threat (in general)

- It is individuals 35 to 54 who are more likely to say they take steps to protect themselves. This is also true of men, residents of Alberta, and those with higher education and household income.

- Canadians under 35 more often say the likelihood of being affected is low compared with other age groups.
- People who say they do not do anything risky online are more often 65 or older and/or women compared with men and those who are younger. It is also more prevalent among those in Saskatchewan compared with the rest of the country.

Over one-quarter (27%) of Canadians believe it is likely that a friend of family member will be affected by a cyber threat in the next year. This is lower than the 32% reported in 2018, although in 2018 the question asked about "you or a family member". More often, Canadians are concerned about a friend (54%) or a parent (48%). About one-third feels that a co-worker (35%) or neighbour (33%) will be affected, while one-quarter are concerned about children (26%) or a grandparent (23%).

Table 1: Likelihood of Others Affected

--	Total 2020	Total 2018*
Q12. And how likely is it that a friend or family member will be affected by a cyber threat in the next year?	*n=2710*	*n=2072*
Unlikely (1-2)	22%	23%
Moderately (3)	37%	34%
Likely (4 5)	27%	32%
Do not know	13%	12%
Q13. Who do you think will be affected?	*n=740*	
Friend	54%	
Parent	48%	
Co-worker	35%	
Neighbour	33%	
Children	26%	
Grandparent	23%	
Other family	5%	
Spouse/partner	2%	
Anyone can be affected	2%	
Other	3%	
Do not know	9%	

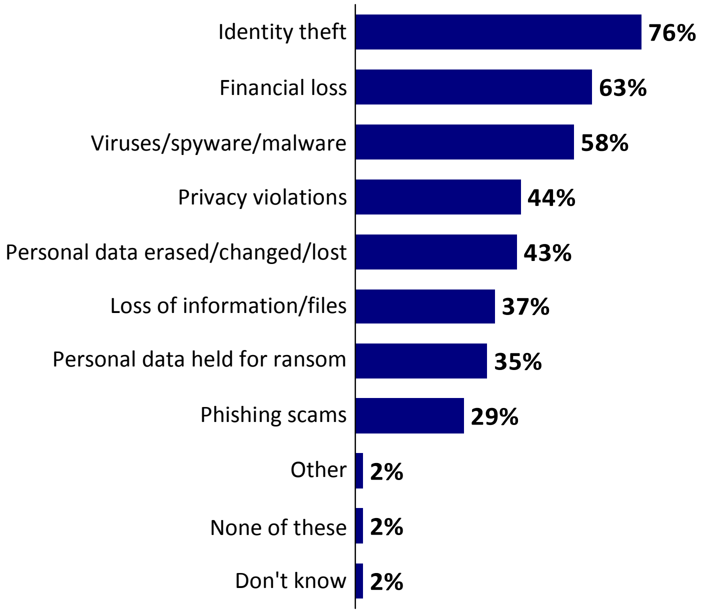
--	Total 2020	Total 2018*
Q14. Why do you think they will be affected?	*n=740*	
Careless usage, do not have security/take precautions	18%	
Happens all the time/everyone is at risk, frequent	17%	
Not tech-savvy, knowledgeable about precautions	16%	
Elderly are susceptible/more at risk/too trusting	4%	
Too trusting, naïve	3%	
Hackers/scams are becoming increasingly sophisticated	2%	
Use Internet for all transactions, use many sites	2%	
Personally experienced/know someone who has been a victim of fraud	2%	
Personal data not protected enough government/ business, lack of law enforcement/accountability when breaches occur	2%	
Other	11%	
Do not know	17%	
No response	7%	

*In 2018 the question asked about "you or a family member".

- Canadians under 35 years of age are less likely than others to say that someone they know will be affected by a cyber threat, which is also more often the case in Manitoba than elsewhere in Canada.
- Residents of Quebec as well as those reporting the highest education (university) and household ($150,000 or above), as well as parents of children five or older more often say it is likely someone they know will be affected.
- Naturally, certain age groups are more likely to be close to, and therefore concerned about others likely to be affected. For example, it is those under 35 likely to expect grandparents to be impacted, while individuals 25 to 44 are more likely than other age groups to feel this is likely among their parents or co-workers. Older age cohorts (ages 45 or older) still have greater expectations of this for their children.
- Men are more likely than women to believe this is likely among co-workers, neighbours or friends.
- Parents of children five or older are more likely than other segments to think a parent or their children, as well as co-workers or neighbours may be affected.

Three in four (76%) Canadians are concerned about identity theft. When thinking about cyber threats, Canadians are also concerned about financial loss (63%), and general viruses, spyware or malware (58%). Roughly two in five are concerned about privacy violations (44%), that personal data will be erased, changed or lost (43%), that information or files will be lost (37%), or their personal data will be held for ransom (35%). Three in ten (29%) Canadians are concerned about phishing scams.

Chart 3: Nature of Concern



Q15. What kinds of cyber threats are you most concerned about?
Base: n=2710

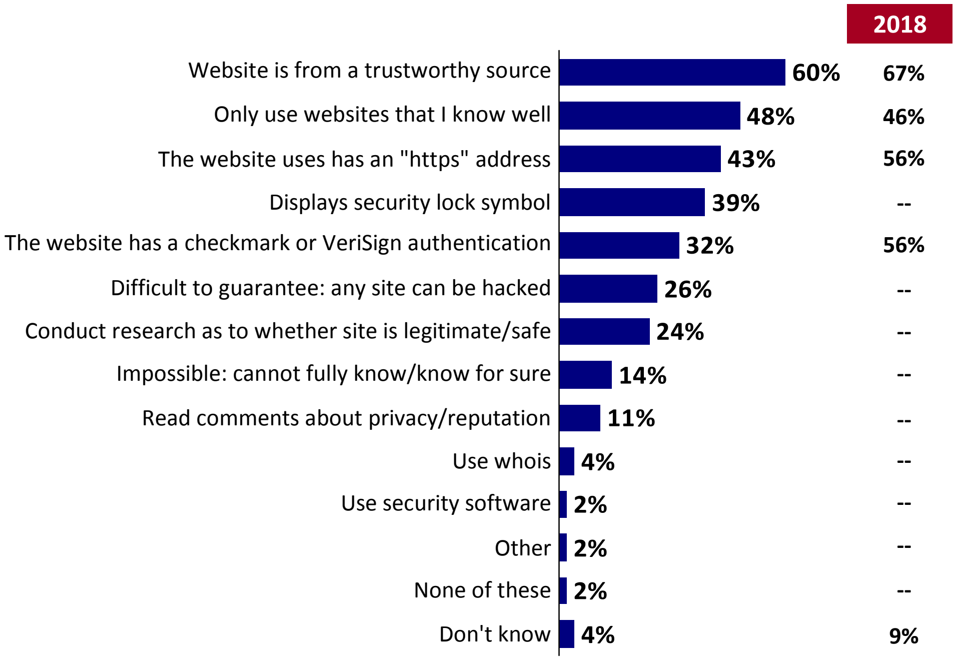
- Phishing scams and viruses are of greater concern to those 55 or older compared with younger Canadians.
- Identity theft is a concern more concentrated among individuals who are 45 to 65 than in other age groups.
- Financial loss, identity theft and personal information held for ransom are more often a concern noted among those with the highest education (university) and household incomes ($150,000) compared with other Canadians.

B. Awareness

Three in five (60%) Canadians say they look for a website from a trustworthy source, such as a well-known software provider or a government website. Just under half (48%) indicate they only use websites that they know well, while slightly fewer (43%) specifically look for the "https" address as their method of verifying that a website is secure. About one-third verify a site through the security lock symbol (39%) or that the website has a checkmark or VeriSign authentication (32%). One-quarter say it is difficult to guarantee that a site is secure as any site can be hacked (26%), or that they conduct research as to whether a site is legitimate (24%). Over one in ten indicate that it is impossible to know for sure if a website is secure (14%) or that they read comments about privacy or reputation of a website (11%).

Although a different question was asked in the 2018 survey (How do you know if a website is secure?), results show a relative parallel insofar as most know about and taken steps in terms of trusted or familiar sites and even the https, although the VeriSign is less apt to be checked relative to awareness in 2018.

Chart 4: Steps to Verify Website Is Secure



QK11a. What steps do you take to verify that a website is secure?
Base: n=2710, 2018 – How do you know if a website is secure? Base: n=1880

- Knowledge of multiple methods of determining secure sites is higher among those who are 25 to 34, and university educated.

Only one in five (19%) Canadians feel they are prepared to face cyber threats. Over one in four (27%) say they are unprepared, and another 45% claim to be somewhat prepared. Among those who are not prepared, 44% say it is because you can never really protect yourself online. Three in ten (31%) have a back up and can recover in the event of a cyber threat. About one in five cite a variety of other reasons, including a lack on information on the steps to take (23%), lack of awareness of the different types of threats (22%), a feeling that it is unlikely to happen (18%), lack of time to prepare (18%), or that the information they do find is not straightforward enough to be helpful (18%).

Table 2: Preparedness

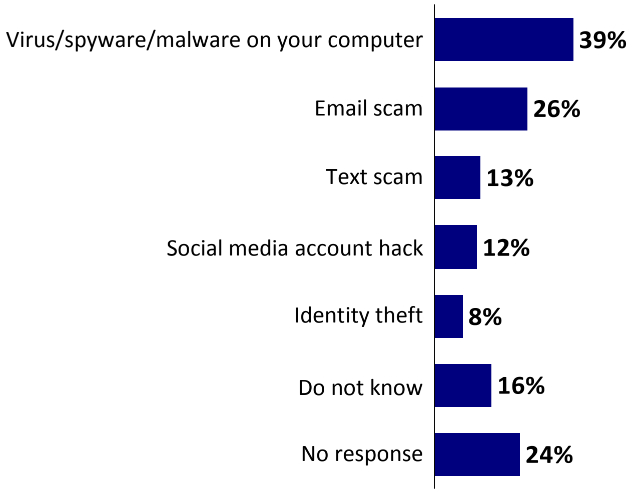
--	Total 2020
Q16. How well prepared are you to face cyber threats?	*n=2710*
Unprepared (1-2)	27%
Somewhat (3)	45%
Prepared (4-5)	19%
Do not know	8%
Q17. Why is that?	*n=1959*
You can never really protect yourself online	44%
I have a back up and can recover	31%
I don't know where to get information about the steps to take	23%
I don't know what the different type of threats are	22%
I don't think it's likely to happen to me	18%
I don't have the time/ never get around to it	18%
The information I find is not straightforward enough to help me	18%
There's no point in trying	4%
Nothing	2%
Other	3%
Do not know	6%

- While there are not significant portions of specific segments who feel well prepared to face a cyber threat, those who are 25 to 34, residents of Quebec, and individuals with a high school level of education are even more likely than average to say they feel unprepared to face such a threat.
- Unlikelihood and lack of time are more likely to be cited by those 35 or younger compared with others. Time is also a barrier cited more often by parents. A fatalistic view that you cannot ever really protect yourself is more prevalent among those 35 to 44. Lack of

understanding of the nature of threats is more common among older Canadians (65+) and those with a high school level of education compared with others. Not knowing where to find information to assist is a more common response among women compared with men.

Two in five (39%) Canadians indicate they have been the victim of a virus, spyware, or malware on their computer. Over one-quarter (26%) report they have been victimized by an email scam. Other cyber attacks experienced have included text scams (13%), or a social media account hack (12%). Just less than one in ten (8%) have been the victim of identity theft. About four in ten in total said they do not know if they have been a victim (16%) or would not provide a response (24%).

Chart 5: Incidence of Victimization

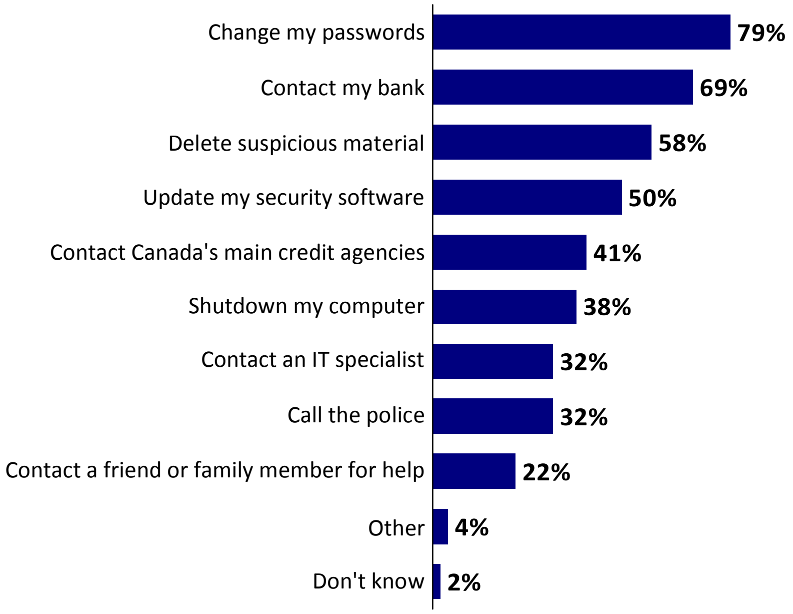


Q18. Have you ever been a victim of any of the following cyber attacks?
Base: n=2710

- Those most likely to have been a victim of an email scam are under 25 or 65 or older, compared with other age groups, as well as residents of Quebec compared with other Canadians.
- The incidence of victimization from text scams is also higher among those under 25, and residents of Saskatchewan and Quebec.
- Virus, software and malware are more likely to be an issue in Alberta than elsewhere in Canada, as well as among men.
- Social media account hacking is more commonly experienced by individuals under 45, particularly those under 25, compared with Canadians who are 45 or older.

If they knew or suspected that they had been a victim of a cyber attack, most (79%) Canadians say they would change their passwords. Over two in three (69%) would prudently contact their bank. Over half would delete suspicious material (58%) or update security software (50%). Other steps anticipated include contacting Canada's main credit agencies (such as Trans Union or Equifax) (41%) or shutting down the affected computer (38%). One-third would contact an IT specialist (32%) or call the police (32%). Just less than one in four (22%) would solicit the support of a friend or family member.

Chart 6: Steps Taken to Protect if Victim of Cyber Attack



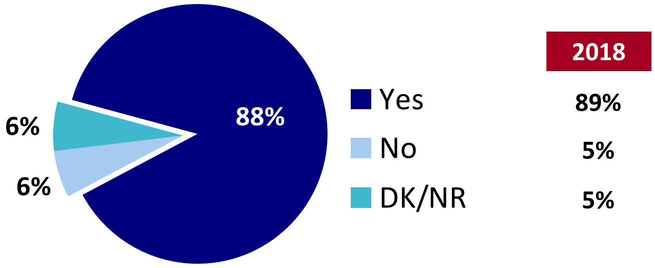
Q19. If you knew or suspected that you'd been a victim of a cyber attack, what steps would you take to protect yourself?
Base: n=2710

- Changing passwords is a more common step taken among those 25 to 44 compared with other age groups, as well as among parents compared with others. Contacting the bank is also more common among individuals 35 to 44 and least common among those under 25.
- Deleting suspicious materials is a more likely response among those 55 to 64 compared with others. Similarly, shutting down the computer is a more common step taken individuals who are 55 or older compared with younger Canadians. It is also a more prevalent response in Manitoba and least so in Quebec.
- Contacting the credit agencies is a considerably more prevalent response among Canadians 35 to 54, parents, and in Quebec, as well as among individuals who are more educated (post-secondary), and reporting medium to higher household incomes ($80,000 or above).

C. Precautions – Behaviour

Nearly nine in ten Canadians (88%, similar to the 89% reported in 2018) report they take precautions to protect their online accounts, social media accounts, devices and networks.

Chart 7: Take Actions to Protect Online Accounts



Q1. Do you take precautions to protect your online accounts, social media accounts, devices, and networks?
Base: n=2710

- Although high across the board, Canadians more likely to take precautions to protect their online accounts are 35 to 54, and residents of British Columbia and Ontario compared with others. Men are also more likely to report taking precautions as are those with more education and income compared with others.
- Least likely to say they take precautions are those under 25, residents of Quebec and individuals with high school completion.

One step Canadians can take to protect themselves includes changing account passwords; however, only about one-quarter do this at least a few times a year (19%) or more (7%). One in ten (12%) say they change their passwords once per year, while 15% estimate that they do this every few years. One in five (19%) change a password whenever they are prompted to and 14% change a password when ever they think of it with no set pattern. Nearly one in ten (9%) say they never change their password and 3% change their password only when they hear about a security breach in the news.

Almost two in three (64%) change some passwords more than others. Highest on the priority list is online banking accounts (62%). Fewer change their work email (34%) or home email (26%) more often. One-quarter change their online shopping accounts (25%) or social media accounts (24%) more often.

Table 3: Changing Passwords

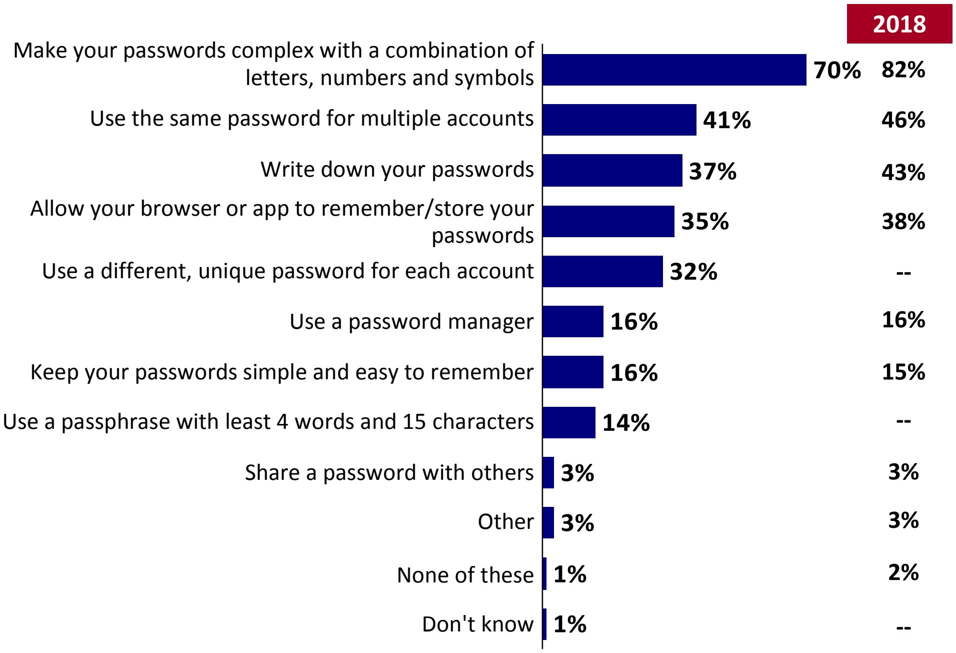
--	Total 2020
Q2. In general, how often do you change your account passwords?	*n=2710*
Never	9%
Every few years	15%
Once a year	12%
A few times a year	19%
More often than a few times a year	7%
Whenever I am prompted to	19%
Whenever I think of it, no set pattern	14%
When I learn about a security breach in the news	3%
Do not know	2%
Q3. Do you change some passwords more often than others?	*n=2457*
Yes	64%
No	28%
Do not know	6%
No response	2%

--	Total 2020
Q4. Which passwords do you change more often?	*n=1569*
Online banking accounts	62%
Email at work	34%
Email at home	26%
Online shopping accounts	25%
Social media accounts	24%
Work network accounts	2%
School network accounts, university email	1%
As prompted/password manager, when password is forgotten	1%
Other	5%
Do not know	3%

- Changing passwords a few times per year or more is a step more commonly taken among those 45 to 54 years of age. Residents of Quebec, as well as those with a high school education or less, are more likely to report never changing their password.
- Residents of British Columbia, along with those 18 to 24 say they change passwords once annually while individuals 25 to 34 years, along with men and those with a university education report changing passwords every few years. Women, along with individuals with a university education and those earning more than $150,000 annually are more likely to update a password when prompted.
- The likelihood of changing some passwords more than others rises with income level; the lowest annual earners ($40,000 or less) are among the least likely, while the highest earners ($150,000 or more) are the most.
- Those with a university education, as well as parents are also more likely to report they change some passwords more often than others while individuals 65 and older, and Quebec residents more often say they do not.
- Unsurprisingly, young people between the ages of 18 and 24 years change their social media, and school account passwords more often than others while those 25-54 (of typical working age), as well as parents are more likely to report changing their work email password more often. Individuals 55 and over change their online shopping account passwords more often than others, and those 65 or older change their online bank account password more often.
- Those who are men, university educated, or earning at least $80, 000 annually also report changing their workplace email passwords more often than others.

When it comes to passwords, most (70%) Canadians say that they try to make their passwords complex, with a combination of letters, numbers and symbols. Two in five (41%) use the same password for multiple accounts. About one-third write down passwords (37%), allow a browser or app to remember or store passwords (35%), or use a different, unique password for each account (32%). Fewer than one in five use a password manager (16%), keep passwords simple and easy to remember (16%), or use a passphrase with at least four words and 15 characters (14%).

Chart 8: Actions Taken Regarding Passwords



Q5. When it comes to your passwords, which of the following actions do you take?
Base: n=2710

- Individuals between the ages of 25 and 34 are more likely to take most actions listed regarding passwords. A similar pattern is seen among those with highest education (university degree) education and income ($150,000 or more). Individuals who are less educated (high school or less), earning less income ($40,000 or under), and are younger (18 to 24 years) are more likely to keep passwords simple and easy to remember.
- Those 18 to 24 years are also more likely to use the same password for multiple accounts and those ages 55 and older are more likely to write down passwords. Women are more likely to engage in both of these behaviours when compared with their male counterparts who prefer using password managers, and unique passwords for each account.

- Parents are also more likely than their counterparts to use password managers.

Just over half (53%) of Canadians use a multi-factor authentication. This most often involves a code received by text message (79%). Three in five use passwords (65%), a code received by email (64%), or PINs (63%). Over half (57%) use fingerprints. Two in five (41%) use a code received by an authentication application and three in ten (29%) use a code received by phone call. One in five use facial recognition (23%) or passphrases (20%). Fewer use token devices (14%), voice verification (9%), smart cards (7%), or USB devices (4%).

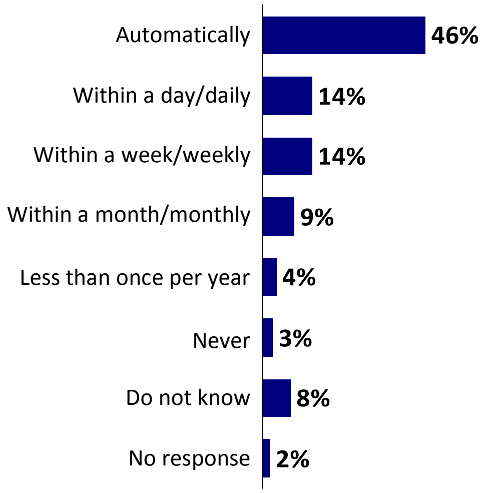
Table 4: Multi-Factor Authentication

--	**Total 2020**
Q6. Do you use multi-factor authentication?	*n=2710*
Yes	53%
No	31%
Do not know	14%
No response	2%
Q7. Which of the following authentication factors have you used?	*n=1423*
Code received by text message	79%
Passwords	65%
Code received by email	64%
PINs	63%
Fingerprints	57%
Code received by an authentication application	41%
Code received by phone call	29%
Facial recognition	23%
Passphrases	20%
Token devices	14%
Voice verification	9%
Smart cards	7%
USB drives	4%
Other	2%
Do not know	1%
No response	1%

- Canadians more likely to use multi-factor authentication are 25 to 54 years of age, parents, male, residents of Alberta, and earning at least $80,000 per year. Those least likely to use this type of authentication are 55 to 64 years of age, and Quebec residents.
- While use of passwords is common among all sub-groups, those authenticating their passwords by text message code are most likely to be between 25 and 44, residents of Ontario, university educated, and earning at least $80,000 per year. Those between 25 and 34 are also more likely to receive a code via email or an authentication application, and individuals 35 to 44 are more likely than other groups to receive a code by email, or use a smart card or a token device.
- Fingerprint authentication is used most often by those 18 to 24, and 35 to 44 years of age; also more common among parents. Facial recognition is also used more often by young people 18 to 24, as well as among residents of Atlantic Canada. Those making $150,000 or more annually are more apt to use both of these methods.
- Residents of Ontario, those with higher education (university) and income ($150,000 or more annually), as well as men are more likely than others to use a token device for authentication purposes. Men are also more likely than women to receive a code by phone or authentication application, or use a smart card. Regionally, residents of Quebec are more likely than others across the country to use a smart card.

For nearly half (46%), operating system updates happen automatically. For others, updates are typically enabled within a day (14%), week (15%), month (9%) or year (4%). A small proportion (3%) claim that they never enable updates.

Chart 9: Frequency of OS Updates



Q8. Devices often prompt you to update the operating system (OS). When do you enable this update?
Base: n=2710

- Those more likely to rely on automated schedules to update their operating system are between the ages of 35 to 44 and 55 or older compared with other age groups. It is also more common in Quebec, and among men compared with their counterparts.
- Those who update weekly or less frequently are more often under 25, and in terms of monthly specifically, also those 25 to 34 compared with other age groups.

Nine in ten (90%) Canadians secure their home Wi-Fi with a unique password, although 29% used the default password. Seven in ten (68%) created the password. Only 17% use a guest network with a separate password for visitors.

Table 5: Securing WiFi

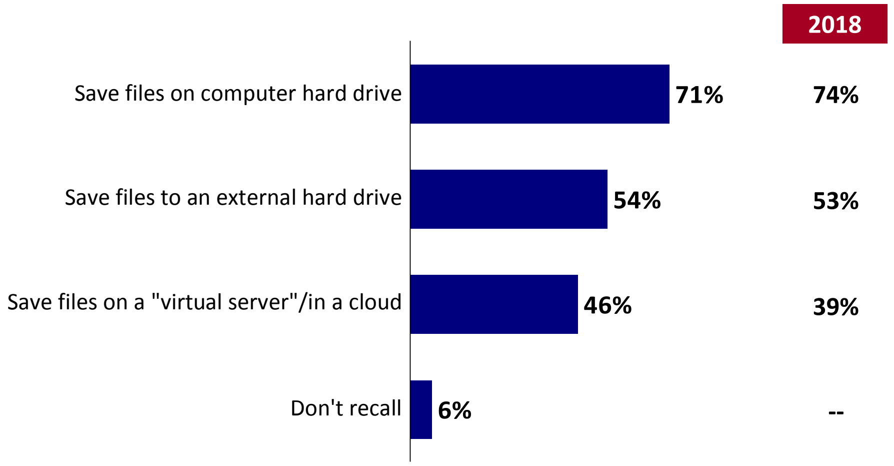
--	Total 2020	Total 2018
QB2B. Do you secure your home Wi-Fi with a unique password?	*n=2710*	*n=1801*
Yes	90%	96%
No	4%	3%
Do not have Wi-Fi at home	3%	--
Do not know	2%	1%
No response	1%	--
Q9. Was the password you used the default one that came with the device (e.g. a router) or is it a new one you created yourself?	*n=2430*	
Yes, default password	29%	
No, I created it myself	68%	
Do not know	2%	
No response	1%	
Q10. Do you use a guest network with a separate password for your smart devices and/or for visitors?	*n=2710*	
Yes	17%	
No	77%	
Do not know	4%	
No response	3%	

- Although almost everyone secures their home Wi-Fi, this is most prevalent among Canadians 25 to 54 years of age, as well as among Ontarians and those reporting the highest education and household incomes compared with other Canadians. Even among those least likely to do so the incidence is just short of 90% or higher, except among those with high school and the lowest household incomes where it is only 82%.
- The default password is used somewhat more commonly among those under 25, and 55 to 64 compared with other age groups. It is also more prevalent in Quebec compared with other regions, as well as among women compared with men.

- While relatively few use a guest password, this is somewhat more common among those 35 to 44, parents and among those reporting the highest household incomes, compared with other Canadians

Nearly three in four (71%) Canadians save their files on a computer hard drive. Over half (54%) store their data on an external hard drive and fewer (46%) have implemented a virtual server or cloud. Results were very similar in 2018, although slightly higher proportions of Canadians rely on the cloud in 2020.

Chart 10: Data Storage

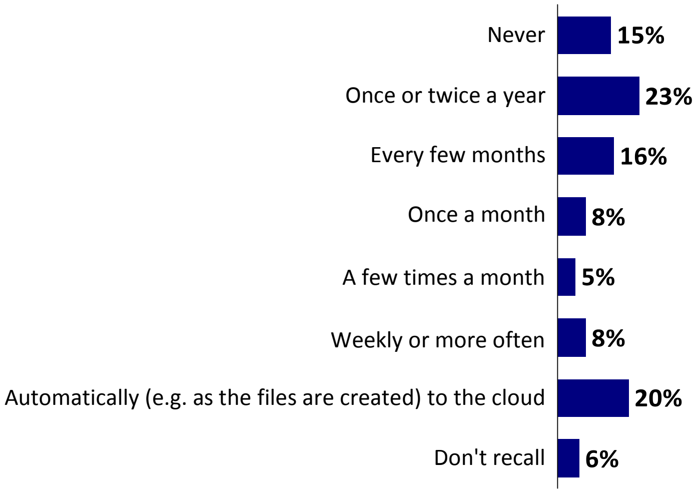


QD1B. Thinking about data storage of information for personal use, do you save information on your computer hard drive, an external hard drive (i.e., extra storage / back up), or on a "virtual server" (i.e., cloud computing)?
Base: n=2710

- Education, age, income, and gender are strong predictors of whether any type of the above data storage options is used. Canadians age 54 or under are more likely than older counterparts to use a cloud, which is also more common among parents. 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.

For one in five (20%), data and personal files stored on a computer, smartphone, or other mobile device are automatically saved to the cloud. A similar proportion (23%) manually back up their files once or twice per year, while fewer have implemented the practice of backing up files every few months (16%), once a month (8%), a few times a month (5%) or weekly or more (8%). A portion of Canadians never (15%) back up their files.

Chart 11: Frequency of Backing Up Devices



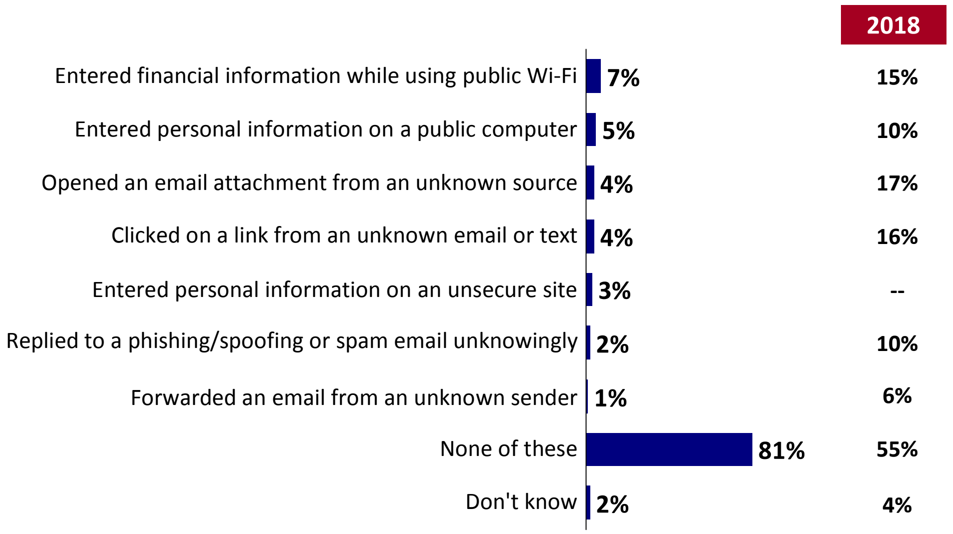
QB5X. How often do you back up data/personal files stored on your computer, smartphone or other mobile device?
Base: n=2710

- Younger Canadians (under age 25) are more likely than other age groups to back up their files once or twice a year, while those 25 to 54, parents, and people with higher income and education, are more apt to back up files automatically (as they are also more likely to use a cloud) compared with their counterparts. Older Canadians, along with women, those in Quebec, and Canadians with lower income and education are more likely than other segments to say they never back up their files.

In the past month, eight in ten (81%) Canadians claim not to have participated in behaviour that may threaten cyber security. Fewer than one in ten have entered financial information while using public Wi-Fi (7%), entered personal information on a pubic computer (5%), opened an email attachment from an unknown source (4%), clicked on a link from an unknown email or text (4%), entered personal information on an unsecure site (3%) or replied to a phishing, spoofing or spam email unknowingly (2%).

A similar question was posed in 2018, although it asked about behaviour that had "ever" occurred, rather than in the past month. While not strictly comparable, it provides a sense of the degree of behaviour in some areas (e.g., opening an attachment or clicking a link, replying to phishing/spam, forwarding an email from unknown source). Use of public Wi-Fi and personal information on a public device are still at relatively higher occurrences, even in the past month.

Chart 12: Types of Risks Taken



2018 question: To your knowledge, have you ever done any of these things?

QB11. In the past month, have you...?
Base: n=2710, 2018 Base: 2072

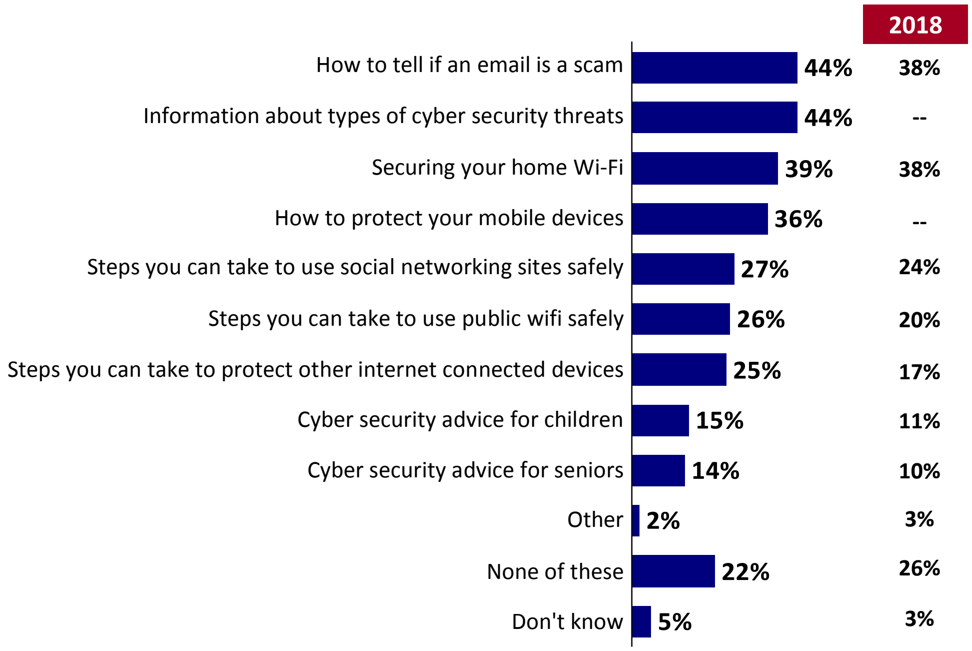
- Those under age 25 (along with individuals with a household income under $40,000) are more likely than others to have entered personal information on an unsecure site, on a public computer, or entered financial information while using public Wi-Fi. Older Canadians (age 55+) are more apt to say they did none of these compared with other age groups.

D. Information

Fewer than half of Canadians have looked up information on how to tell if an email is a scam (44%) or other information about types of cyber security threats (44%). Over one-third have looked for information on securing home Wi-Fi (39%) or how to protect mobile devices (36%). One-quarter have looked for information on using social networking sites safely (27%), steps to take to use public Wi-Fi safely (26%), or to protect other internet connected devices (such as smart TVs, home security systems, fitness monitors, voice activated devices (25%). Just over one in ten have looked for cyber security advice for children (15%) or seniors (14%). One in five (22%) have not looked for any cyber security information.

Although responding to a slightly different question, 2020 results suggest that several topics are more likely to have been researched than they were in 2018 (determining email scams, how to use public Wi-Fi safely, and steps to protect other internet connected devices).

Chart 13: Type of Information Looked For

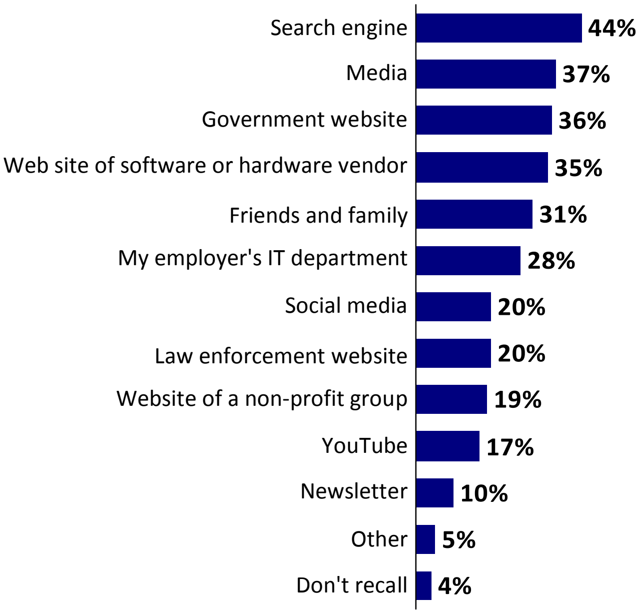


QIC5a. Have you ever looked for the following types of cyber security information?, 2018 – Which of the following types of online threats, if any, have you looked for information for?
Base: n=2710, 2018: n=2072

- Younger Canadians (under age 25) are less likely than other age groups to have searched for information on types of cyber security threats. Canadians who are 65 or older are more likely than others to have searched for information on Internet safety for seniors, and less likely to have looked for steps to use public Wi-Fi safely or to use social networking sites safely. Those aged 35-54 are comparatively more likely to have looked for information on securing home Wi-Fi, or cyber security advice for children.
- Similarly, parents are more likely than other Canadians to search for information on securing home Wi-Fi, and protecting mobile and other internet connected devices such as smart TVs, home security systems and voice activated devices, as well as cyber security advice for children and safe social networking practices.
- Men, along with those with higher income and education, are more likely than women and those with less education and income to report searching for information on most areas.
- Quebec residents are less apt to have looked for information in most areas than other Canadians.

For 44% of Canadians, information on cyber security was found by using a search engine. About three in ten found information through the media, including a news organization's website (37%), a government website (36%), a software or hardware vendor's website (35%), or through friends and family (31%). One-quarter (28%) found information through their employer's IT department. One in five sourced information through social media (20%), a law enforcement website (20%), the website of a non-profit group (19%), or YouTube (17%). Ten percent found information in a newsletter.

Chart 14: Information Source



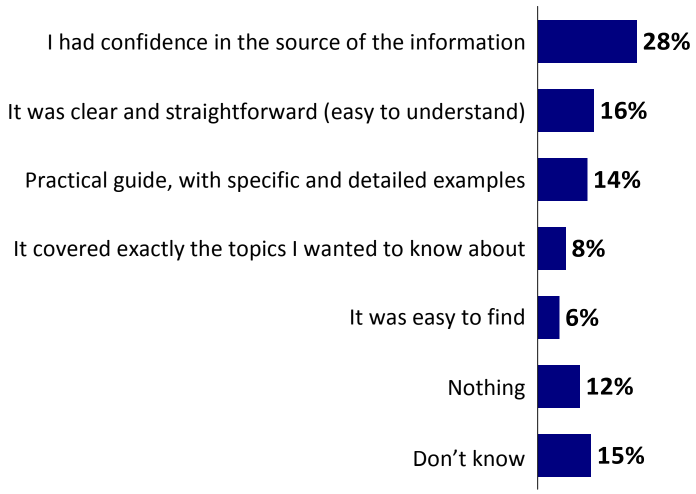
QIC5b. Where did you find that information?
Base: n=1977 (Anyone searching for information on one of the listed topics in Chart 13)

- Those under age 25 are more likely than other age groups to have found information on social media or YouTube. Those 25 to 54, and parents, along with those with higher income and education, are more likely than their counterparts to say they found information from their employer's IT department. Older Canadians (age 55+) are comparatively more likely to have found information from friends or family or a newsletter. Those 55-64 have a higher tendency than other age segments to look for information on a website of a vendor or a government website.
- Men are more likely than women to have found information through a search engine, a website of a vendor, a website of non-profit group, YouTube, or a newsletter.

- Those with higher education, along with those in British Columbia, are more likely than others to have used the website of a non-profit group.
- Residents of Ontario are more apt than those in other regions to have used YouTube.

Just over one in four (28%) found the information helpful because of their confidence in the source of the information. Other reasons for confidence include information that was found to helpful because it was clear and straightforward (16%), or because it offers a practical guide with specific steps and detailed examples (14%). Fewer than one in ten had confidence because the information covered precisely the topics they were interested in (8%) or that the information was easy to find (6%).

Chart 15: Reasons Information is Helpful

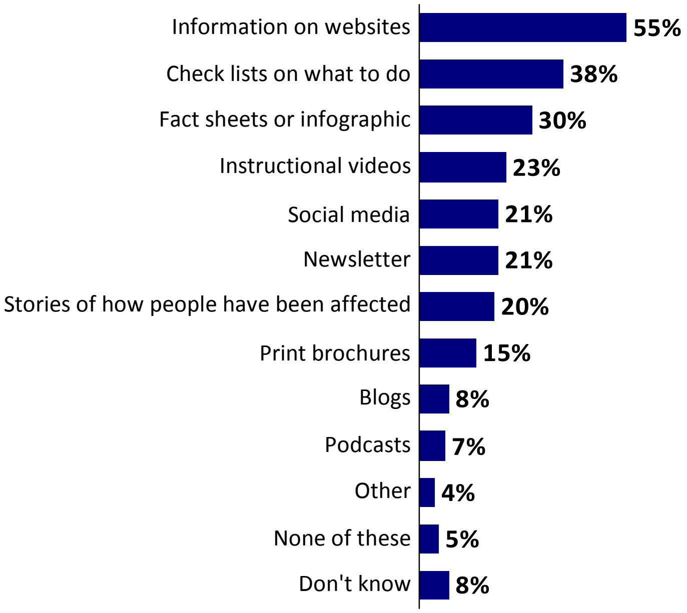


QIC8b. What was it about this information that made it helpful?
Base: n=2710

- Younger Canadians are more likely than those 25 or older to say the information was clear and easy to understand (this group was more apt to have used social media or YouTube).
- Those with a university education are more likely than individuals with less education to say they were confident in the source of the information, or that the information was a practical guide with specific and detailed examples.

Over half (55%) of Canadians prefer to get information on cyber security protection through websites. Three in ten prefer check lists on what to do (38%) or fact sheets or infographics (30%). One in five say they prefer instructional videos (23%), social media (21%), newsletters such as email subscriptions (21%), or stories of how people have been affected (20%). Fewer cite print brochures (15%), podcasts (8%) or blogs (7%) as their preferred vehicle for getting the information.

Chart 16: Preferred Type/Method of Information



Q20. How do you prefer to get information to protect yourself from cyber threats?
Base: n=2651

- Younger Canadians (under 25) are more likely than other age groups to prefer fact sheets or infographics, stories of how people have been affected, or social media. Parents are also more likely than others to point to social media. Older Canadians (55 and over) are more likely than those who are younger to prefer check lists of what do to, print brochures or newsletters.
- Individuals who are between 35 and 44, along with men, residents of Ontario, and those with higher income and education are more likely than their counterparts to prefer information on websites.
- In addition to older Canadians, those in Quebec, women, and those with higher education are more likely to prefer check lists on what to do compared with others.

Nearly one-third (30%) of Canadians reportedly help others with cyber security. This most often includes assistance they give to parents (61%) or friends (59%). Nearly half (48%) of those who help others with cyber security assist other relatives. One-third (33%) listed co-workers and three in ten (29%) help their children. About one in five help neighbours (21%) or grandparents (17%). Nine percent help small business owners.

Table 6: Helping Others with Cyber Security

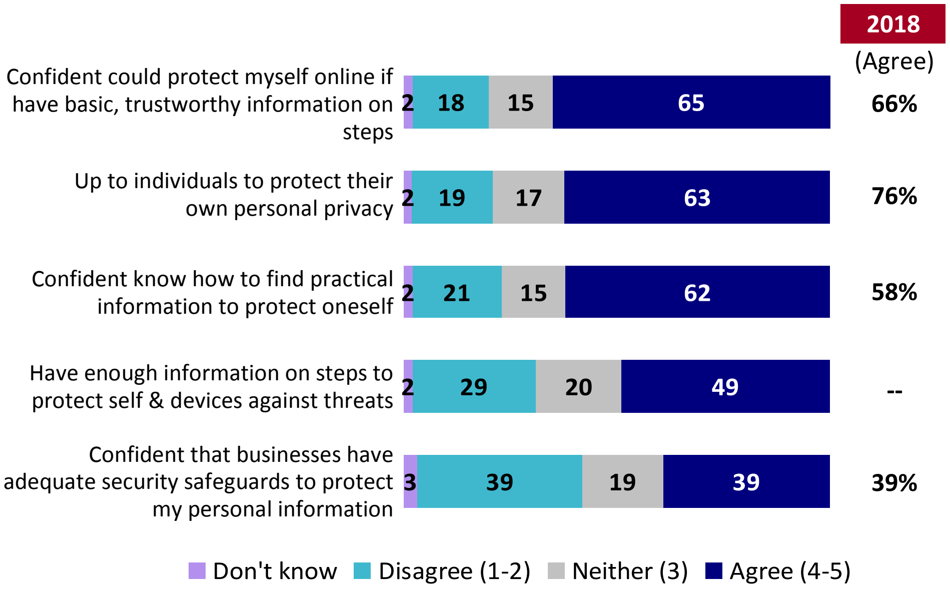
--	**Total 2020**
Q21. Do you help others with cyber security?	*n=2710*
Yes	30%
No	64%
Do not know	4%
No response	2%
Q22. Who do you help?	*n=803*
Parents	61%
Friends	59%
Other relatives	48%
Co-workers	33%
Children	29%
Neighbours	21%
Grandparents	17%
Small business owners	9%
Other	2%

- Canadians between 25 and 44, parents, along with men, those in Ontario, and those with higher income and education, are more likely than others to say they help others with cyber security.
- Canadians who are 18 to 44 are more likely than other age groups to be helping their parents, while those age 35-54 are typically helping their children. Younger Canadians (18-34) are also more apt to be helping their grandparents than other age segments.
- Parents are more likely than others to say they are helping children, parents and grandparents.
- Men are more likely than women to be helping friends, their neighbours or other relatives.
- Those in Quebec are more likely than residents of other regions to be helping other relatives.

Nearly two-thirds (65%) of Canadians feel confident that they could protect themselves online, as long as basic and trustworthy information is available on steps to take. Slightly fewer agree that it is up to individuals to protect their own personal privacy (63%) or feel confident that they know how to find practical information to protect themselves online (62%). Only half (49%), however, feel they have enough information on how to take steps to protect against cyber threats. Two in five (39%) are confident that businesses and other organizations have adequate security safeguards to protect personal information.

Results from 2018 are similar for three of the four repeated questions, although Canadians are less apt to agree in 2020 that it is up to individuals to protect their own personal privacy compared with the 76% who agreed in 2018.

Chart 17: Attitudes About Information



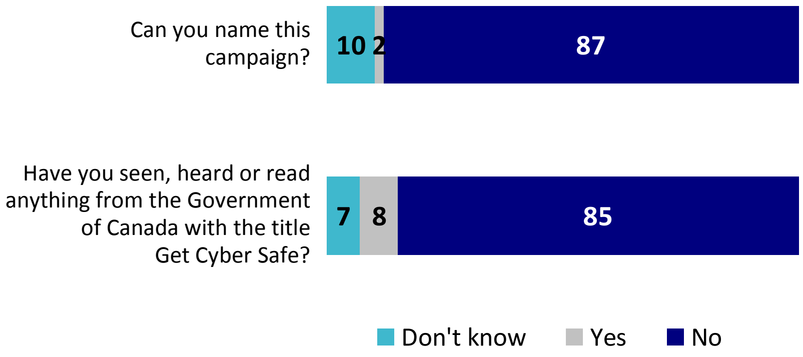
QA13, A11B, A118, Q120, A110 . Please rate the degree to which you agree or disagree with the following statements.
Base: n=2710, 2018 – n=2072

- Individuals who are 18 to 44 are more likely than other age groups to agree they have enough information to take steps and know how to find practical information. Younger Canadians (under age 25) are more likely than others to feel confident that businesses have adequate safeguards to protect their personal information.
- Parents are also more likely than others to say know how to find practical information online.

- Men, and those with higher income, are more likely to agree they have enough information to take steps, that they know how to find practical information, and to be confident they could protect themselves online compared with their counterparts.
- Residents in Quebec are least likely than others across the country to be confident they can find practical information.

Very few (2%) Canadians can name the Government of Canada awareness campaign created to inform Canadians about cyber security and the simple steps they can take to protect themselves online. Once prompted, slightly more (8%) reported familiarity with the Get Cyber Safe campaign from the Government of Canada.

Chart 18: Awareness of Get Cyber Safe Campaign



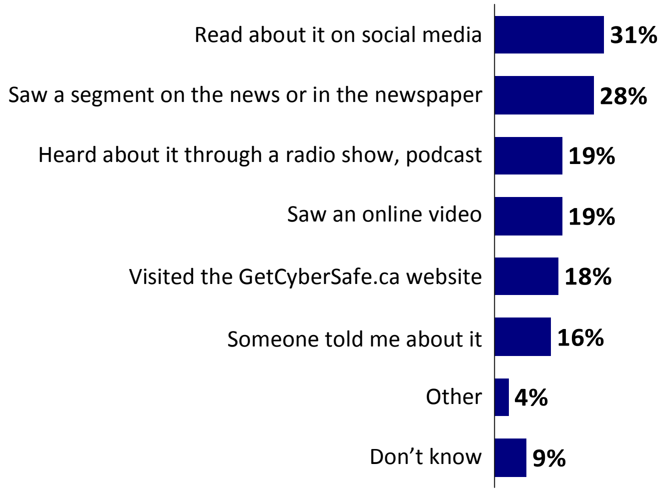
Q23. There is a Government of Canada awareness campaign created to inform Canadians about cyber security and the simple steps they can take to protect themselves online. Can you name this campaign?
Base: n=2683

QGOCAD. Have you seen, heard or read anything from the Government of Canada with the title Get Cyber Safe that talked about online threats and how to protect yourself?
Base: n=2710

- When prompted, younger Canadians (under age 25), parents, those with higher income ($150,000), and those from Manitoba or Quebec are more likely than others to say they heard of Get Cyber Safe.

Of those who indicated familiarity with the Get Cyber Safe campaign, 31% say they read about Get Cyber Safe on social media and 28% saw a segment on the news or in the newspaper. Fewer than one in five heard about it through a radio show or podcast (19%), saw an online video (18%), visited the GetCyberSafe.ca website (18%), or heard from someone else (16%).

Chart 19: Awareness of Get Cyber Safe Campaign

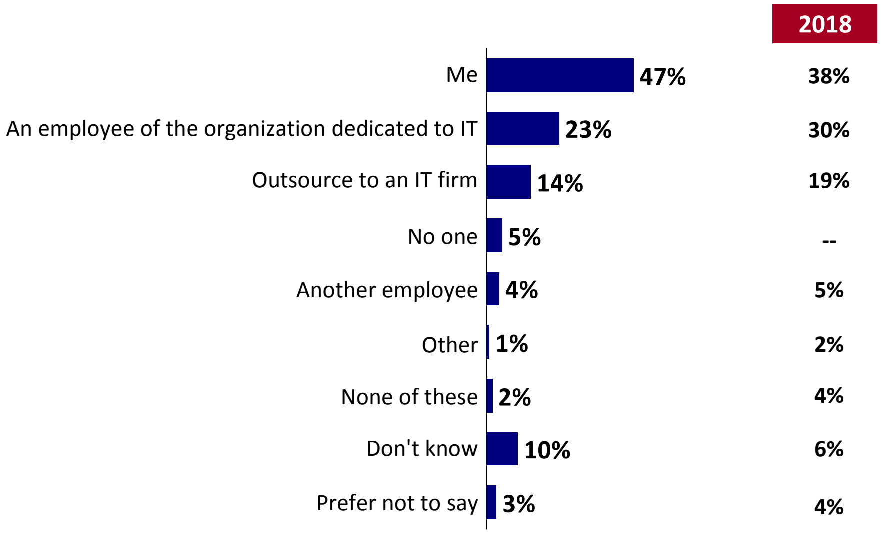


QGOCADA. Where did you see, hear, or read this?
Base: n=210

E. Experience of Businesses

Nearly half (47%) of business owners or managers are responsible for their company's IT. More than one in five (23%) cite an employee of the organization dedicated to IT. Over one in ten (14%) outsource this function to an IT firm and five percent do not have anyone responsible for IT.

Chart 20: Responsibility for IT



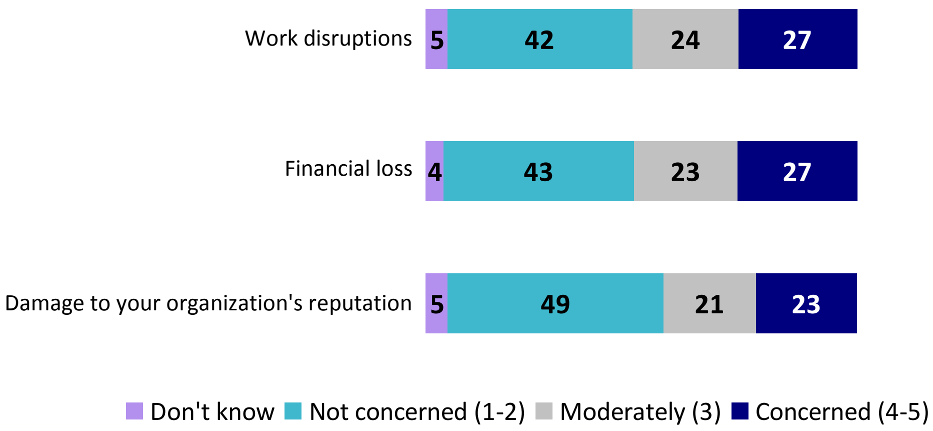
QBUS4. Who is responsible for your company's IT?

Base: n=356

- Older business owners or managers (age 65+) are more likely than younger representatives to say they are responsible for their company's IT. Those with higher income ($150,000 or more) are more likely than those reporting less income -to say they outsource to an IT firm.

When thinking about the various concerns of daily operations, over one-quarter of business owners or managers are concerned about work disruptions (27%) or financial loss (27%) in the event of a cyber threat. Slightly fewer (23%) are concerned about damage to the organization's reputation.

Chart 21: Level of Concern

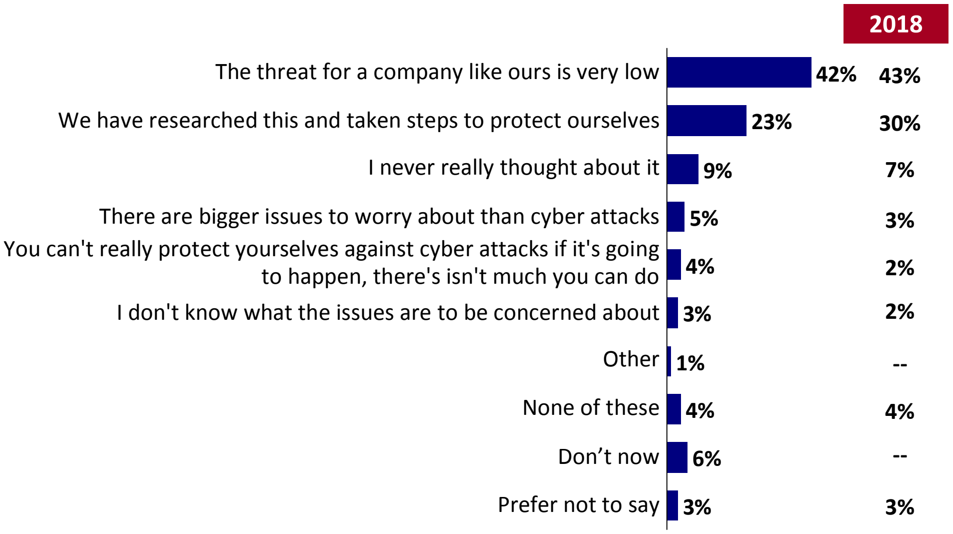


QBUS5A1-A3. Thinking about the various concerns of daily operations of your organization, how concerned are you that a cyber threat will cause...?
Base: n=360

- Men are more likely than women to be concerned about work disruptions.

Among those who are not concerned, over two in five (42%) cite their perception of minimal threat for their type of company. One in five (23%) say they have conducted research and taken steps to protect their business. One in ten (9%) report they have never really thought about cyber security. Other mentions include having bigger issues than cyber attacks to worry about (5%), that there is not much that can be done to prevent a cyber attack (4%), or unsure of what issues there are to be concerned about (3%).

Chart 22: Reasons for Lack of Concern



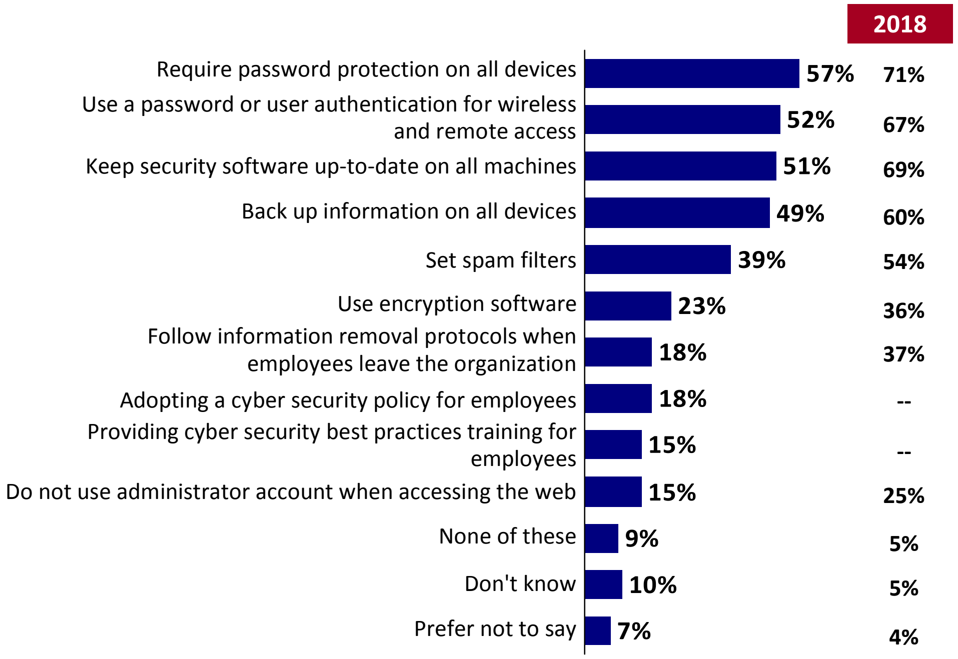
QBUS5b. Why is this?

Base: n=203

- Those with higher income and education are comparatively less apt to be concerned because they have researched and taken steps to protect themselves.
- Men, along with those age 25-34, are more likely than other representatives to say it is because they never really thought about it. Women business owners and managers are less likely than others to worry because they feel the threat for their type of company is low.

Over half of business owners or managers report that their business has implemented password protection on all devices (57%), use password or user authentication for wireless and remote access (52%), or kept security software up to date on all machines (51%). Just under half (49%) have taken the steps to back up information on all devices while two in five (39%) have set spam filters to protect against online threats. About one in five have implemented encryption software (23%), followed information removal protocols when employees have left the organization (18%), adopted a cyber security policy for employees (18%), provided cyber security training for employees (15%), or refrain from using an administrator account when accessing the web (15%).

Chart 23: Steps Taken to Prevent/Protect Against Attacks

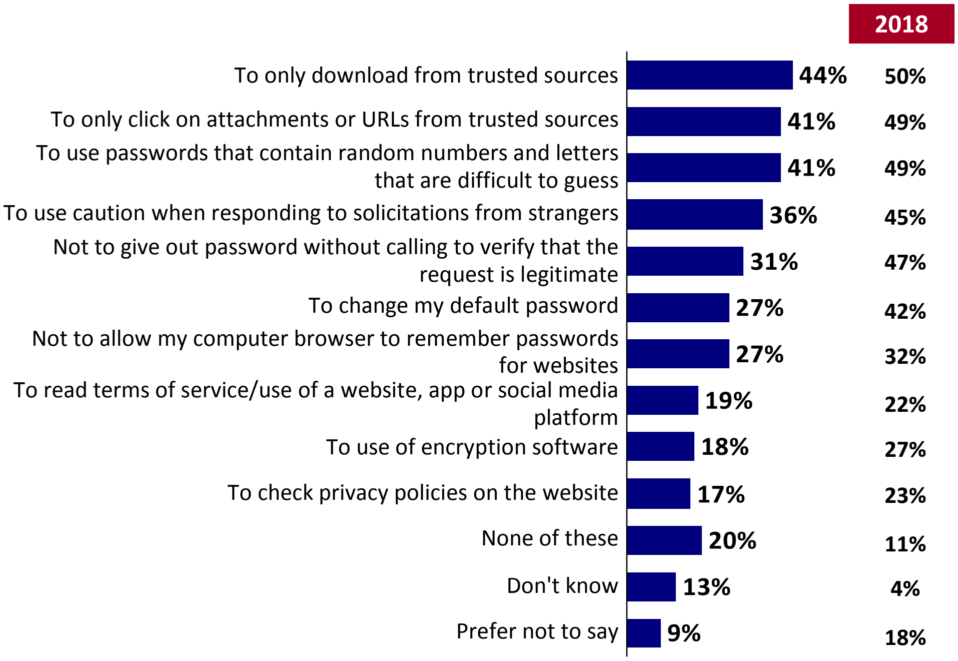


QBUS1. Turning to your work as a business owner/manager, which of the following steps has your business taken to protect itself against online threats?
Base: n=360

- Business representatives with higher education and income are more likely to have kept security software up to date, set spam filters, adopt a cyber security policy for all employees and require password protection on all computers compared with others.

About two in five business owners or managers report that employees are instructed to only download from trusted sources (44%), to only click on attachments or URLs from trusted sources (41%), or to use passwords that contain random numbers and letters that are difficult to guess (41%). About one-third instruct employees to use caution when responding to solicitations from strangers (36%) or to not give out passwords without calling to verify that the request is legitimate (31%). Just over one-quarter have directed employees to change default passwords (27%) or to not allow computer browsers to remember passwords for websites (27%). One in five ask employees to read terms of service of a website, app, or social media platform (19%), to use encryption software (18%), or to check privacy policies of websites (17%). One in five (20%) do not provide any instructions to employees to protect the organization against cyber threats.

Chart 24: Instructions to Employees



QBUS2. Which of the following instructions do you provide to employees to protect the organization against cyber threats and to protect your personal information?
Base: n=360

- Those with higher education are more apt to have provided most instructions to employees than other business representatives.

Two in five business owners or managers say that their organization would benefit from a list of the types of threats that exist and clues to look out for (41%), guidelines for reacting to a cyber attack (40%), or steps to protect mobile devices in a public setting (39%). Over three in ten would see value in information on best practices for safe cloud computing (36%), resources on how to encrypt computers, laptops, and storage devices (34%), best practices for use of storage devices (34%), or guidelines on use of personal devices for work (31%). About one in four indicate their organization would benefit from tips on the type of software/hardware to make networks secure (29%), best practise for employees on how to handle passwords (29%), guidelines to establish rules for safe email usage policies (28%), best practices on a clear internet usage policy (27%), guidelines on how to establish strong social media policy (26%), or tips on communicating the importance of following cyber security to employees (25%). Slightly fewer see value in having information on steps for handling work-related information possessed by departing employees (22%).

Table 7: Beneficial Information for Small and Medium Businesses

--	**Total 2020**	**Total 2018**
QBUS3. Which of the following types of information do you feel that your organization would benefit from having in order to protect itself against cyber threats?	*n=360*	*n=533*
A list of the types of threats that exist and cues to look for	41%	47%
Guidelines for reacting to a cyber attack	40%	46%
Steps to protect mobile devices in a public setting	39%	40%
Best practices for safe cloud computing (with definition of cloud computing)	36%	35%
Resources on how to encrypt computers, laptops, and storage devices	34%	37%
Best practices for use of storage devices (e.g. USBs)	34%	40%
Guidelines on use of personal devices for work	31%	40%
Tips/resources for the type of software/hardware to make networks secure	29%	36%
Best practices for employees on how to handle passwords	29%	37%
Guidelines to establish rules for safe email usage policies	28%	39%
Best practices for a clear internet usage policy	27%	37%
Guidelines on how to establish strong social media policy	26%	37%
Tips on communicating the importance of following cyber security policies to employees	25%	32%

--	Total 2020	Total 2018
Steps for handling work-related information possessed by departing employees	22%	33%
Other	3%	4%
None of these	9%	8%
Do not know	13%	12%
Prefer not to say	7%	7%

- Business respondents age 55-64, along with those with higher education are more likely to state their organization would benefit from most types of information.

APPENDICES

A. SURVEY QUESTIONNAIRE (ENGLISH)

INTRO

WEB INTRO

EKOS Research Associates is surveying people across the country on behalf of the federal Government about issues related to online security. The survey should take approximately 15 minutes to complete. Your participation is voluntary and your responses will be kept completely confidential. Any information you provide will be handled in accordance with the *Privacy Act*. This survey is registered with the Research Verification Service. **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
On disability pension	7
Maternal/parental leave	8
Retired	9
Other (please specify)	77
No response	99

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

QEMPA

DK/NR, QEMP

Do you believe the number of employees at all locations in your organization is over or under 100?

Over 100	1
Under 100	2
Don't know/ No response	99

QEMPB [1,2]

Full/part-time employed, D2; Fewer than 100 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	99

QCHILDA [1,5]

Parents, D5

What are the ages of children in the home?

Select all that apply

Under 5	1
6 to 12	2
13 to 15	3
16 to 18	4
19 to 24	5
25 or older	6
No response	9

D4

In what year were you born?

Year	1
No response	9999

QAGEY

Hesitant, D4; <18 or NR, terminate

In which of the following age categories do you belong?

Less than 18 years old	1
18 to 24	2
25 to 34	3
35 to 44	4

45 to 54	5
55 to 64	6
65 or older	7
Prefer not to say	99

Q1

Opening

Do you take precautions to protect your online accounts, social media accounts, devices, and networks?

Yes	1
No	2
Do not know	98
No response	99

Q2

Passwords

In general, how often do you change your account passwords?

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 in the news	8
Do not know	99

Q3

Do you change some passwords more often than others?

Yes	1
No	2
Do not know	98
No response	99

Q4 [1,8]

Yes, Q3

Which passwords do you change more often?

Please select all that apply

Email at home	1
Email at work	2
Social media accounts	3
Online banking accounts	4
Online shopping accounts	5
Other (please specify)	77
Do not know	99

Q5 [1,13]

When it comes to your passwords, which of the following actions do you take?

Please select all that apply

Keep your passwords simple and easy to remember	1
Make your passwords complex with a combination of letters, numbers and symbols	2
Use a passphrase with least 4 words and 15 characters	3
Use the same password for multiple accounts	4
Use a different, unique password for each account	5
Share a password with others	6
Write down your passwords	7
Use a password manager	8
Allow your browser or an app to remember/ store your passwords	9
Other	77
None of these	98
Do not know	99

Q6

MFA

Do you use <abbr title="Multi-factor authentication means that you need more than one authentication factor to log in to a device or an account. For example, to unlock your phone, you need to enter a passcode and scan your fingerprint", style = "colour: blue; border-bottom: 1px dotted black;">multi-factor authentication?

Mobile only:

Multi-factor authentication means that you need more than one authentication factor to log in to a device or an account. For example, to unlock your phone, you need to enter a passcode and scan your fingerprint

Yes	1
No	2
Do not know	98
No response	99

Q7 [1,15]

Yes, Q6

Which of the following authentication factors have you used?

Please select all that apply

Passwords	1
Passphrases	2
PINs	3
Code received by email	4
Code received by text message	5
Code received by phone call	6
Code received by an authentication application	7
Smart cards	8
USB drives	9
Token devices	10
Fingerprints	11
Facial recognition	12
Voice verification	13

Other (please specify)	77
Do not know	98
No response	99

Q8

Auto updates

Devices often prompt you to update the operating system (OS). When do you enable this update?

Automatically	1
Within a day/daily	2
Within a week/weekly	3
Within a month/monthly	4
Less than once per year	5
Never	6
Do not know	98
No response	99

B2B

Do you secure your home Wi-Fi with a unique password?

Yes	1
No	2
Do not have Wi-Fi at home	3
Do not know	98
No response	99

Q9

Yes, B2B

Was the password you used the default one that came with the device (e.g. a router) or is it a new one you created yourself?

Yes, default password	1
No, I created it myself	2
Do not know	98
No response	99

Q10

Do you use a guest network with a separate password for your smart devices and/or for visitors?

Yes	1
No	2
Do not know	98
No response	99

D1B [1,5]

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)?

Please select all that apply

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
Don't recall	99

B5X

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

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
Automatically (e.g. as the files are created) to the cloud	7
Don't recall	99

B11 [1,10]

Phishing

In the past month, have you

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
Forwarded an email from an unknown sender	3
Entered personal information on an unsecure site	4
Entered personal information on a public computer	5
Entered financial information while using public Wi-Fi	6
Replied to a phishing/spoofing or spam email unknowingly	7
None of these	97
Do not know	98

K11A [1,20]

What steps do you take to verify that a website is secure?

Please select all that apply

Only use websites that I know well	1
Website is from a trustworthy source (e.g. well known Internet Service Provider or software provider, government, etc)	2
The website uses has an "https" address	3
The website has a checkmark or VeriSign authentication	4
Displays security lock symbol	5
Conduct research as to whether site is legitimate/safe	6
Use whois	7
Read comments about privacy/reputation	8
Impossible: cannot fully know/know for sure	9
Difficult to guarantee: any site can be hacked	10
Other (please specify)	77
None of these	98
Do not know	99

Q11A

Threats

In the next year, how likely do you feel that you will be affected by a cyber threat causing:

...your personal information to be compromised?

Not at all likely 1	1
2	2
Moderately likely 3	3
4	4
Extremely likely 5	5
Do not know	99

Q11B

Threats

In the next year, how likely do you feel that you will be affected by a cyber threat causing:

...you financial loss?

Not at all likely 1	1
2	2
Moderately likely 3	3
4	4
Extremely likely 5	5
Do not know	99

Q11C

Threats

In the next year, how likely do you feel that you will be affected by a cyber threat causing:

...you the loss of files, photos?

Not at all likely 1	1
2	2
Moderately likely 3	3
4	4
Extremely likely 5	5
Do not know	99

Q12

And how likely is it that a friend or family member will be affected by a cyber threat in the next year?

Not at all likely 1	1
2	2
Moderately likely 3	3
4	4
Extremely likely 5	5
Do not know	99

Q13 [1,9]

Likely (4-5), Q12

Who do you think will be affected?

Co-worker	1
Neighbour	2

Friend	3
Parent	4
Children	5
Grandparent	6
Other:	77
Do not know	99

Q14

Likely (4-5), Q12

Why do you think they will be affected?

Please specify:	77
Do not know	98
No response	99

K8A [1,11]

Unlikely (1-2), Q11

Why don't you think that it is likely that you will be affected by a cyber 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
Stay up to date/knowledgeable/educated about information/viruses	5
Work in computer/information technology	6
Use Apple/iOS which is not as susceptible to viruses	7
Use Linux which is not as susceptible to viruses	8
Do not use Microsoft OS	9
Other (please specify)	77
Do not know	99

Q15 [1,11]

What kinds of cyber threats are you most concerned about?

Please select all that apply

Phishing scams	1
Viruses/spyware/malware	2
Identity theft	3
Privacy violations	4
Financial loss	5
Personal data held for ransom	6
Loss of information/files	7
Personal data erased/ changed/ lost	8
Other (please specify)	77
None of these	98
Do not know	99

Q16

How well prepared are you to face cyber threats?

Not at all prepared	1
Not prepared	2
Somewhat prepared	3

Prepared	4
Very well prepared	5
Do not know	99

Q17 [1,12]

Not prepared, Q16

Why is that?

Please select all that apply

I don't think it's likely to happen to me	1
I don't have the time/ never get around to it	2
I don't know what the different type of threats are	3
I don't know where to get information about the steps to take	4
The information I find is not straightforward enough to help me	5
You can never really protect yourself online	6
There's no point in trying	7
I have a back up and can recover	8
Nothing	9
Other (specify)	77
Do not know	99

Q18 [1,7]

Have you ever been a victim of any of the following cyber attacks?

Please select all that apply

Email scam	1
Text scam	2
Virus/spyware/malware on your computer	3
Identity theft	4
Social media account hack	5
Do not know	98
No response	99

Q19 [1,13]

If you knew or suspected that you'd been a victim of a cyber attack, what steps would you take to protect yourself?

Please select all that apply

Shutdown my computer	1
Delete suspicious material (email, text, downloaded content, etc.)	2
Update my security software	3
Change my passwords	4
Contact my bank	5
Contact Canada's main credit agencies (Trans Union, Equifax)	6
Contact an IT specialist	7
Contact a friend or family member for help	8
Call the police	9
Nothing	10
Other (specify)	77
Do not know	99

Q20 [1,13]

How do you prefer to get information to protect yourself from cyber threats?

Please select all that apply

Podcasts	1
Blogs	2
Fact sheets or infographics	3
Check lists on what to do	4
Instructional videos	5
Stories of how people have been affected	6
Information on websites	7
Print brochures	8
Newsletter (e.g. an email subscription)	9
Social media	10
Other (specify)	77
None of these	97
Do not know	99

Q21

Where do you go for Information

Do you help others with cyber security?

Yes	1
No	2
Do not know	98
No response	99

Q22 [1,11]

Yes, Q21

Who do you help?

Please select all that apply

Small business owners	1
Co-workers	2
Neighbours	3
Friends	4
Parents	5
Children	6
Grandparents	7
Other relatives	8
Other:	77
Do not know	99

IC5A [1,12]

Have you ever looked for the following types of cyber security information?

Please select all that apply

How to tell if an email is a scam	1
Steps you can take to use public wifi safely	2
Steps you can take to use social networking sites safely	3
Securing your home Wi-Fi	4
Steps you can take to protect other internet connected devices (e.g. smart TVs, home security systems, fitness monitors, voice activated devices and smart assistants)	5

How to protect your mobile devices	6
Cyber security advice for children	7
Cyber security advice for seniors	8
Information about types of cyber security threats (e.g. phishing scams, malware, etc.)	9
Other (specify):	77
None of these	98
Do not know	99

IC5B [1,14]

1-9,77, IC5A

Where did you find that information?

Please select all that apply

Search engine	1
Web site of software or hardware vendor	2
Friends and family	3
Media (e.g. news organizations' website)	4
Website of a non-profit group	5
Newsletter	6
Government website	7
Law enforcement website	8
My employer's IT department	9
Social media	10
YouTube	11
Other (please specify)	77
Don't recall	99

IC8B

What was it about this information that made it helpful?

I had confidence in the source of the information	1
Practical guide, with specific and detailed examples	2
It covered exactly the topics I wanted to know about	3
It was clear and straightforward (easy to understand)	4
It was easy to find	5
Other (specify)	77
Nothing	97
Do not know	99

QA13

Who do you trust

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

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

Strongly disagree 1	1
2	2
3	3
Neither 4	4
5	5
6	6
Strongly agree 7	7
Do not know	99

QA111B

Who do you trust

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

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

Strongly disagree 1	1
2	2
3	3
Neither 4	4
5	5
6	6
Strongly agree 7	7
Do not know	99

QA118

Who do you trust

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

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	1
2	2
3	3
Neither 4	4
5	5
6	6
Strongly agree 7	7
Do not know	99

QA120

Who do you trust

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

I am confident that I know how to find practical information I can use to protect myself online

Strongly disagree 1	1
2	2
3	3
Neither 4	4
5	5
6	6
Strongly agree 7	7
Do not know	99

QA110

Who do you trust

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

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

Strongly disagree 1	1
2	2
3	3

Neither 4	4
5	5
6	6
Strongly agree 7	7
Do not know	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
Providing cyber security best practices training for employees	9
Adopting a cyber security policy for employees	10
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 cyber 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
Prefer not to say	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 in order to protect itself against cyber 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 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
No one	5
Other	77
None of these	97
Do not know	98
Prefer not to say	99

BUS5A1

Responsible, QEMPB; Self-employed, D2

Thinking about the various concerns of daily operations of your organization, how concerned are you that a cyber threat will cause...

...work disruptions?

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

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

BUS5A2

Responsible, QEMPB; Self-employed, D2

Thinking about the various concerns of daily operations of your organization, how concerned are you that a cyber threat will cause...

...damage to your organization's reputation?

Not at all concerned 1	1
2	2
3	3
Moderately concerned 4	4
5	5
6	6
Extremely concerned 7	7
Do not know	98
Prefer not to say	99

BUS5A3

Responsible, QEMPB; Self-employed, D2

Thinking about the various concerns of daily operations of your organization, how concerned are you that a cyber threat will cause...

...financial loss?

Not at all concerned 1	1
2	2
3	3
Moderately concerned 4	4
5	5
6	6
Extremely concerned 7	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

Q23

Awareness of GCS

There is a Government of Canada awareness campaign created to inform Canadians about cyber security and the simple steps they can take to protect themselves online. Can you name this campaign?

Yes:	77
No	2
Do not know	98
No response	99

GOCAD

Have you seen, heard or read anything from the Government of Canada with the title GetCyberSafe that talked about online threats and how to protect yourself?

Yes	1
No	2
Do not know	99

GOCADA [1,8]

Yes, GOCAD

Where did you see, hear, or read this?

Visited the GetCyberSafe.ca website	1
Heard about it through a radio show, podcast	2
Read about it on social media	3
Saw an online video	4
Someone told me about it	5
Saw a segment on the news or in the newspaper	6
Other (specify)	77
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.

QGENDR

With which gender do you identify?

Male	1
Female	2
Prefer to self-identify (Please specify):	77
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

THNKSP

Children under 18, QCHILDA

Thank you for completing this survey. As part of this study, we would also like to speak with youth between the ages of 16 and 24. All participants aged 16-24 will receive a $10 Amazon gift card as our 'thank you' for their time and careful consideration. May we include your son or daughter, aged 16-24 in this study?

Yes	1
No	2

THNKSP2

Children under 18, QCHILDA; Yes, THNKSP

We would like to send you an invitation to forward to your son or daughter, aged 16-24 to participate in this study. Please provide us with your email address.

Email :	1
Refuse	2

THNK

<THNK: [THNKSP = 1 and QCHILDA = 4,5]We have sent you an invitation to forward to your son or daughter, aged 16-24 to participate in this study. If you have more than son or daughter, aged 16-24 at home, please forward the invitation to the young person aged 16-24 who most recently celebrated a birthday.[ELSE]> 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 Communications Security Establishment. 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. Please press the "continue" button to submit your answers.

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.

B. Methodology Details

The sample consists of 2,710 completed interviews with Canadians 18 years of age or older who use the Internet on a regular basis, including 350 interviews with youth between the ages of 16 and 24, and 350 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 120,000 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 15,312 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 18 per cent[3]. The final survey sample of 2,710 yields a level of precision of +/-1.9 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 14 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.

[3] Among the sample of 15,312 cases, 179 bounced as undeliverable (15,133 valid sample) and 76 were screened out as out of scope.

The survey was administered between March 16 and 29, 2020, 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.

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, level of education and annual household income.

Table 1: Demographic Table

Table 1a: Province / Territory (unweighted)

-	**Total**
n=	*2710*
British Columbia and Yukon	13%
Alberta and Northwest Territories	12%
Saskatchewan and Manitoba	10%
Ontario	34%
Quebec and Nunavut	23%
Atlantic	9%

Table 1b: Gender (unweighted)

-	**Total**
Male	48%
Female	59%

Table 1c: Age (unweighted)

-	**Total**
16-24	13%
25-34	12%
35-44	16%
45-54	21%
55-64	19%
65 up	20%

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

--	**Total**
n=	*2710*
Yes	27%
No	72%
Prefer not to say	1%

Table 1e: Age of children in the home

-	**Total**
n=	*2710*
Under 6	31%
6 to 12	48%
13 to 15	32%
16 or older	39%
Prefer not to say	1%

Table 1f: Level of education completed

-	**Total**
n=	*2710*
High school or less	10%
Some post secondary	10%
College, vocational or trade certificate or diploma	29%
Undergraduate university degree	30%
Graduate or professional degree	19%
Prefer not to say	1%

Table 1h: Annual household income

-	**Total**
n=	*2710*
<$20,000	5%
$20,000-$39,999	10%
$40,000-$59,999	12%
$60,000-$79,999	14%
$80,000-$99,999	13%
$100,000-$149,999	18%
$150,000 or more	14%
Don't know/No response	14%

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 49 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). As previously described, each sample was weighted by age, gender, and region.