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: 2L165-220295/001/CY
Contract Value: $63,991.29
Award Date: December 13, 2021
Delivery Date: March 15, 2022

Registration Number: POR 070-21
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 2022

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 2,050 Canadians between January 21 and February 14, 2022.

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:
D96-17/2022E-PDF

International Standard Book Number (ISBN):
978-0-660-42688-4

Related publications (registration number: POR 070-21):
D96-17/2022F-PDF (French)
978-0-660-42689-1

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

B. METHODOLOGY

The sample consists of 2,050 completed interviews with Canadians 16 years of age or older who use the internet on a regular basis, including 553 interviews with parents of children under 18 years of age, and 301 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 12,295 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 17 per cent. The final survey sample of 2,050 yields a level of precision of +/-2.2 per cent for the sample overall and +/-3 to 6 per cent for most sub-groups that could be isolated in the analysis (including all regions, age, education, and income segments).

Prior to conducting the survey, the instrument was tested with 41 cases in English and 20 cases in French. The bilingual survey was administered between January 21 and February 14, 2022 and took an average of 15 minutes to complete online. 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. Over one in ten 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, the loss of files or photos, or their data held for ransom. Combining the likelihood across the three areas, however, less than one in ten 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. When thinking about cyber threats, three in four Canadians are concerned about identity theft. Other top threats on the mind of Canadians are general viruses, spyware or malware, and financial loss. 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.

Awareness

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, or only use websites that they know well. Less than half look for the "https" address as their method of verifying that a website is secure, verify a site through the security lock symbol.

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, one in four say they have been the victim of a virus, spyware, or malware on their computer or have been victimized by an email scam. Other cyber attacks experienced have included phishing, text scams, social media account hacks. Identity theft and ransomware were reported by a few.

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

Precautions

Similar to previous measurement periods, nearly nine in ten Canadians take precautions to protect their online and social media accounts, devices and networks. The majority say it is best to make passwords complex with a combination of letters, numbers and symbols. Over two in three 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 nearly nine in ten), followed by a code received by email, passwords, or PINs for about 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 an increasing number of Canadians 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

Two in five Canadians have looked up information about types of cyber security threats or how to tell if an email is a scam. Over one in three have looked for information on securing home Wi-Fi or how to protect mobile devices. This information was found by nearly half of Canadians by using a search engine. About three in ten or more found information through a government website, a software or hardware vendor's website, the media, including a news organization's website, or through friends and family. An employer's IT department was a source of information for one in three of those who searched for information; higher among those aged 25 to 54, and with higher education. Most 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. About one in five say they prefer instructional videos, stories of how people have been affected, social media, or newsletters such as email subscriptions.

As found in 2018 and 2020, if provided trustworthy information, two in three Canadians feel confident that they could protect themselves online or are confident they know how to find practical information online to protect against cyber threats. Over three in five agree it is up to individuals to protect their own personal privacy.

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

Experience of Business

Among the concerns business owners or managers have in daily operations, only about three in ten are concerned about work disruptions or financial loss. Slightly fewer are concerned about the damage to the organization's reputation due to a cyber threat or their company's data being held for ransom. Similar to 2018 and 2020, under half are not concerned because they feel the threat for their type of company is very low; higher among those with a college education. One in four have researched and taken steps to protect their business online. Over two in three business owners or managers report that their business has implemented password protection on all devices. Slightly fewer but still more than half keep security software up to date on all machines, use password or user authentication for wireless and remote access, or back up information on all devices.

Half of business owners or managers say that their organization would benefit from information containing guidelines for reacting to a cyber attack, a list of the types of threats that exist and clues to look out for. Two in five feel they would benefit from information on steps to protect mobile devices in a public setting, best practices for employees on how to handle passwords, best practices for safe cloud computing, guidelines on use of personal devices for work, resources on how to encrypt computers, tips on the type of software/hardware to make networks secure, guidelines to establish rules for safe email usage policies, best practices for use of storage devices, or best practices on a clear internet usage policy.

Nearly half of business owners or managers anticipate that it would take some effort or be difficult to recover from a ransomware attack. Two in three business owners or managers have employees that work from home, at least some of the time. Additional instructions were provided to employees on various ways to protect the organization against cyber threats when working from home. The top instructions were on the use of anti-virus software, multi-factor authentication, a firewall, or to back up information. Business owners or managers cite many types of information needed to protect their organization against cyber threats; half identify the need for guidelines for reacting to a cyber attack and a list of the types of threats that exist and cues to look for.

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.

[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.

E. 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 Policy on Communications and Federal Identity and the Directive on the Management of Communications.

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: 

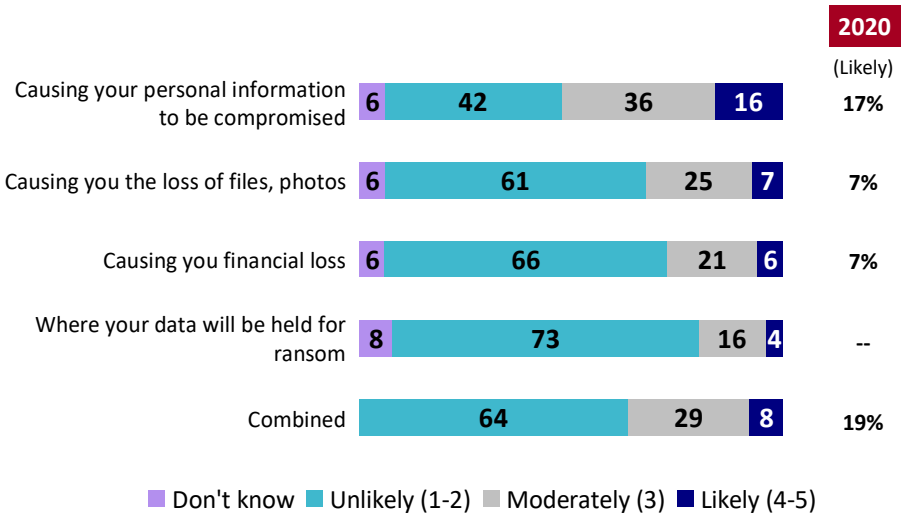
Susan Galley (Vice President)

DETAILED FINDINGS

A. LEVEL OF CONCERN/LIKELIHOOD OF INCIDENT

Over the next year, over one in ten (16%) feel it is likely that they will be affected by a cyber threat causing their personal information to be compromised; two in five (42%) 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 the loss of files or photos (7%), financial loss (6%), or where their data will be held for ransom (4%). Overall, combining the likelihood across the four areas, just under one in ten (8%) 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. Results are very similar to 2020; however, this is the first year that the threat of data held for ransom was measured.

Chart 1: Likelihood of Threats



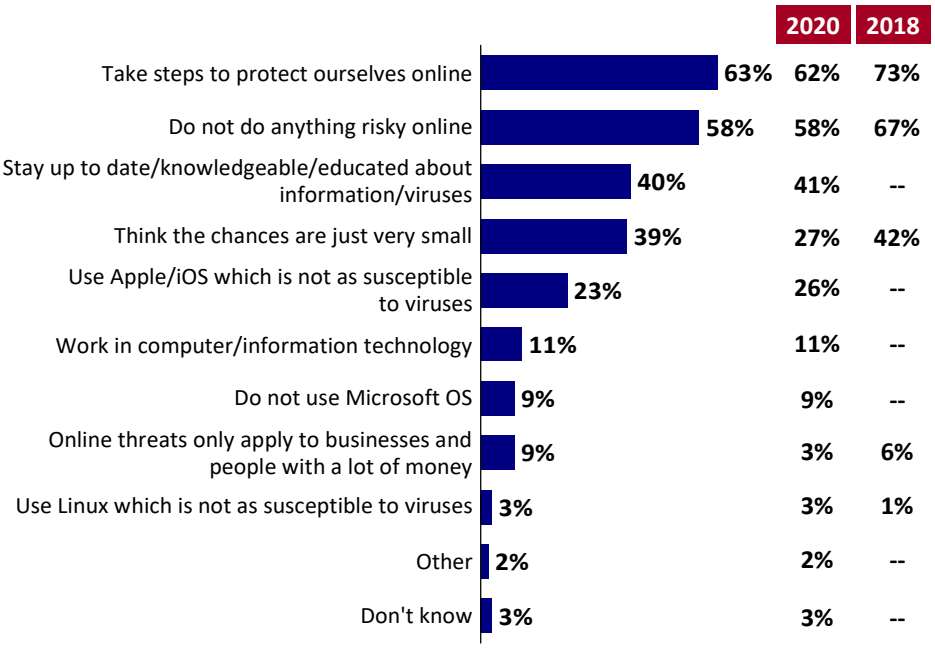
Q11abc. In the next year, how likely do you feel that you will be affected by a cyber threat...?
Base: n=2050

- Younger respondents, along with men, are apt to say it is unlikely that any of the four events would happen.
- Those with higher income (over $150K) are apt to say it is unlikely they will be affected by a cyber threat causing the loss of files/photos, financial loss, or data held for ransom.
- Residents of Quebec are more likely than those in other regions to feel they will be affected by a threat resulting in financial loss.

Among those who are not concerned, the majority say that it is because they take steps to protect themselves online (63%) or that they do not do anything risky online (58%). Two in five indicate they feel unlikely to be affected because they stay informed about viruses (40%), or they feel the chances are just very small (39%). About one in four feel they are unlikely to be affected because they use Apple/iOS which is not as susceptible to viruses (23%).

Most results are similar to previous years, with the exception of the proportion of those who think the chances are just very small which was reported down in 2020 (27%) but returned to a similar level as reported in 2018.

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=1694 (Indicated unlikely to be affected by a cyber threat); 2020: n=1941, 2018: n=492 (Unlikely to be affected by online threat (in general)

- Men and those with higher education are more likely to say they take steps to protect themselves.
- Canadians who are 25 to 34 are more likely to say they are not likely to be affected because they stay up to date or work in IT.
- Those with less education and income are apt to say online threats only apply to businesses and people with a lot of money. Those with higher income ($80K and over) are more likely

than those with lower income to say it is unlikely because they take steps to protect themselves online or they stay up to date.

Over three in four (78%) Canadians are concerned about identity theft. When thinking about cyber threats, Canadians are also concerned about general viruses, spyware or malware (62%) or financial loss (60%). Roughly two in five are concerned about privacy violations (48%), that personal data will be erased, changed or lost (47%), their personal data will be held for ransom (45%), or that information or files will be lost (38%). Three in ten (31%) Canadians are concerned about phishing scams.

Most concerns are reported slightly higher than in 2020, with the most notable increase among those concerned about personal or financial data held for ransom (45%, compared to 35% in 2020).

Chart 3: Nature of Concern

Q15. What kinds of cyber threats are you most concerned about?
Base: n=2050; 2020: n=2710

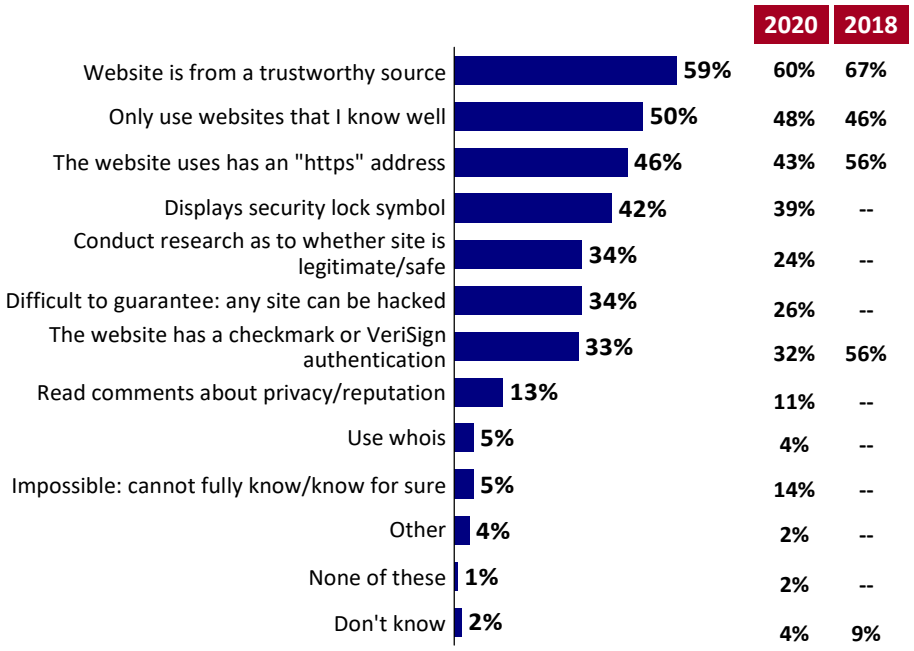
- Phishing scams and viruses are of greater concern to those 55 or older compared with younger Canadians.
- Identity theft is a concern more concentrated among individuals who are 45 to 54 than in other age groups.
- Canadians aged 25-34 are more likely than other age groups to be concerned about financial loss, privacy violations and ransomware.
- Identity theft, personal information held for ransom, and loss of information/files are more often a concern noted among those with the highest education (university) compared with other Canadians.

B. AWARENESS

Three in five (59%) Canadians say they look for a website from a trustworthy source, such as a well-known software provider or a government website. Half (50%) indicate they only use websites that they know well, while slightly fewer (46%) specifically look for the "https" address as their method of verifying that a website is secure. Over two in five verify a site through the security lock symbol (42%). About one in three conduct research as to whether a site is legitimate/safe (34%), look for a checkmark or VeriSign authentication (33%), or generally say it's hard to guarantee and any site can be hacked (33%). Over one in ten indicate that they read comments about privacy or reputation of a website (13%).

Although a different question was asked in the 2018 survey (How do you know if a website is secure?), results show a relative parallel to other measurement periods; however, more say that they conduct research or that it is difficult to guarantee as any site can be hacked than in 2020.

Chart 4: Steps to Verify Website Is Secure



QK11a. What steps do you take to verify that a website is secure?
Base: n=2050; 2020: n=2710; 2018 – How do you know if a website is secure? n=1880

- Knowledge of multiple methods of determining secure sites is higher among those who are 25 to 34, and university educated.
- Residents of Quebec are more likely to look for a website with an “https”, while those in Ontario are more likely than those in other regions to say they look for a security lock symbol.

Only one in five (22%) Canadians feel they are prepared to face cyber threats. Over one in four (28%) say they are unprepared, and another 43% claim to be somewhat prepared. Among those who are not prepared, 41% say it is because you can never really protect yourself online. Three in ten (35%) 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 (26%), a feeling that it is unlikely to happen (26%), lack of time to prepare (20%), lack of awareness of the different types of threats (19%), or that the information they do find is not straightforward enough to be helpful (18%). More Canadians believe it won’t happen to them in 2022 (26%) than in 2020 (18%).

Table 1: Preparedness

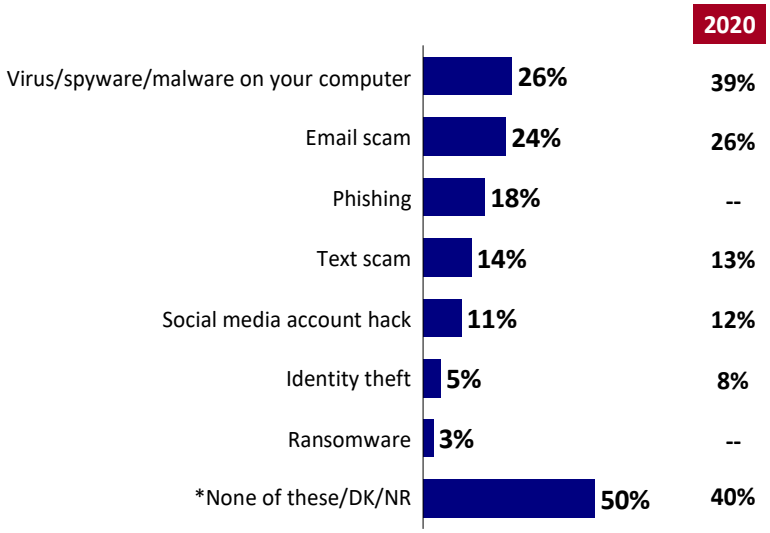
--	**Total 2022**	**Total 2020**
Q16. How well prepared are you to face cyber threats?	*n=2050*	*n=2710*
Unprepared (1-2)	28%	27%
Somewhat (3)	43%	45%
Prepared (4-5)	22%	19%
Do not know	7%	8%
Q17. Why is that?	*n=1453*	*n=1959*
You can never really protect yourself online	41%	44%
I have a back up and can recover	35%	31%
I don't know where to get information about the steps to take	26%	23%
I don't think it's likely to happen to me	26%	18%
I don't have the time/ never get around to it	20%	18%
I don't know what the different type of threats are	19%	22%
The information I find is not straightforward enough to help me	18%	18%
There's no point in trying	3%	4%
Nothing	2%	2%
Other	2%	3%
Do not know	4%	6%

- While there are not significant portions of specific segments who feel well prepared to face a cyber threat, residents of Quebec, women, 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 34 or younger compared with others. Older Canadians (65+) are apt to say they don't know where to find information, or the information they find is not straightforward enough.
- Men are more likely to say they don't think it will happen to them, or that they have a back up and will recover. Women are apt to say they don't know where to get information, the information is not straightforward, or they don't know what the different types of threats are.

One in four Canadians indicate they have been the victim of a virus, spyware, or malware on their computer (26%) or that they have been victimized by an email scam (24%). Other cyber attacks experienced have included phishing (18%), text scams (14%), or a social media account hack (11%). Few have been the victim of identity theft (5%) or ransomware (3%). Half say they have not been a victim of any cyber attacks (43%), are not sure (5%), or do not want to respond (2%).

Fewer Canadians say there were a victim or a virus, spyware, or malware than in 2020 (down to 26% from 39%). Phishing was added in 2022 as an option presented to respondents, along with "none of these" to distinguish from don't know or no response.

Chart 5: Incidence of Victimization



* "None of these" was added in 2022

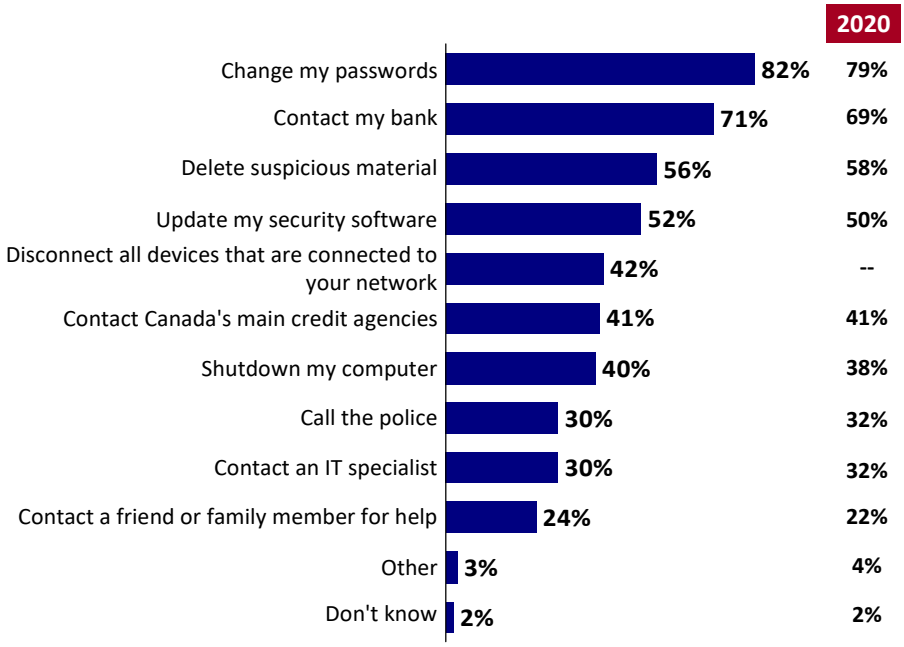
Q18. Have you ever been a victim of any of the following cyber attacks?
Base: n=2050; 2020: n=2710

- Those most likely to have been a victim of an email scam are 55 or older, compared with other age groups.
- Residents of Manitoba and Quebec are more likely to be victims of an email or a text scam compared with other Canadians.
- The incidence of victimization from social media account hacks is higher among those under 25.
- Virus, software and malware are more likely to be an issue in Alberta than elsewhere in Canada, as well as among men.
- Those with higher income ($150,000 and over) are more likely to say they have not been the victim of any of these.

If they knew or suspected that they had been a victim of a cyber attack, most (82%) Canadians say they would change their passwords. Over two in three (71%) would pro-actively contact their bank. Over half would delete suspicious material (56%) or update security software (52%). Other steps anticipated include disconnecting all devices connected to your network (42%) contacting Canada's main credit agencies (such as Trans Union or Equifax) (41%) or shutting down the affected computer (40%). Three in ten would contact an IT specialist (30%) or call the police (30%). Just less than one in four (24%) would solicit the support of a friend or family member.

Results are very similar to 2020; however, disconnect all devices connected to your network was added in 2022.

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



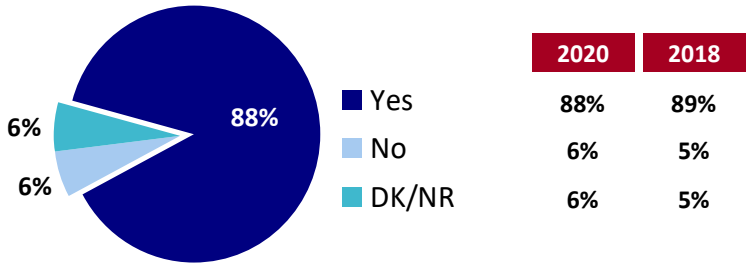
Q19. If you knew or suspected that you'd been a victim of a cyber attack, what steps would you take to protect yourself?
Base: n=2050; 2020: n=2710

- Canadians aged 25-44 are more likely to say they would change their passwords, contact their bank, or Canada's main credit agencies. Older Canadians, aged 55 and over, are apt to say they would shut down their computer or contact an IT specialist.
- Regionally those in Ontario are apt to say they would shutdown their computer or delete suspicious material. Those in Quebec are more likely to say they would contact the credit agencies.
- Women are more likely than men to seek external support, such as contacting an IT specialist, the help of a friend or family member, or the police.
- Those with higher education are apt to identify most steps measured. Those with higher income ($80,000 and over) are more likely to say they would change their passwords, contact their bank or contact the main credit agencies.

C. PRECAUTIONS – BEHAVIOUR

Nearly nine in ten Canadians (88%, consistent with 2020 and 2018) report they take precautions to protect their online accounts, social media accounts, devices and networks.

Chart 7: Take Actions to Protect Online Accounts



	2020	2018
Yes	88%	89%
No	6%	5%
DK/NR	6%	5%

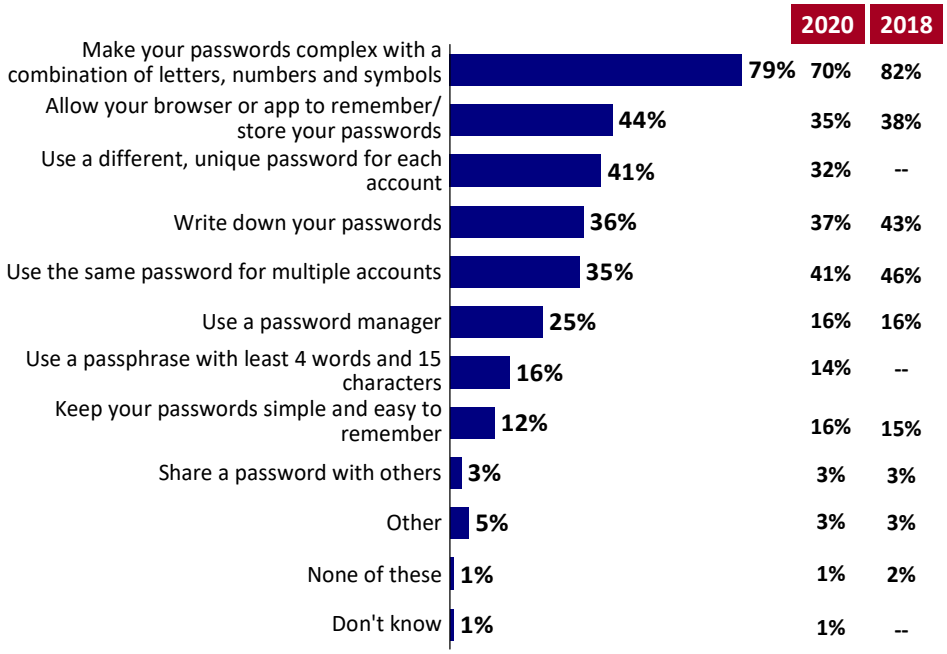
Q1. Do you take precautions to protect your online accounts, social media accounts, devices, and networks?
Base: n=2050; 2020: n=2710; 2018: n=2,072

- Although high across the board, men are more likely to report taking precautions as are those with higher education and income compared with others.
- Regionally, those in Alberta are less likely to take precautions.

When it comes to passwords, most (79%) Canadians say that they try to make their passwords complex, with a combination of letters, numbers and symbols. Two in five allow a browser or app to remember or store passwords (44%), or use a different, unique password for each account (41%). About one in three write down passwords (36%) or use the same password for multiple accounts (35%). One in four use a password manager (25%), and fewer use a passphrase with at least four words and 15 characters (16%) or keep passwords simple and easy to remember (12%).

More Canadians appear to be allowing their browser or app to remember/store passwords (up from 35% in 2020 and 38% in 2018) using a different, unique password for each account (up from 32%) or using a password manager (up from 16%).

Chart 8: Actions Taken Regarding Passwords



Q5. When it comes to your passwords, which of the following actions do you take?

Base: n=2050; 2020: n=2710; 2018: n=2,072

- Canadians under age 45 are more likely to use the same password for multiple accounts, use a password manager or allow the browser or app to store passwords. Those aged 55 and over are more likely to write down passwords.
- Residents of Ontario are more likely than other Canadians to allow the browser or app to store passwords, or use the same password for multiple accounts. Those in BC are apt to use a different, unique password for each account.
- Those with a university degree, and higher income, are more likely to mention most actions. However, those with lower income are more likely to say they write down their passwords.

Just over two in three (69%) Canadians use a multi-factor authentication. This most often involves a code received by text message (87%). Three in five use passwords (62%), a code received by email (66%), or PINs (60%). Nearly half use fingerprints (49%) or a code received by an authentication application (47%). Three in ten use a code received by phone call (32%) or use facial recognition (32%). Less than one in five use passphrases (17%) or token devices (14%). Few use voice verification (9%), smart cards (5%), or USB devices (4%).

Multi-factor authentication usage has changed since 2020 with more notable higher usage of codes received by text, authentication application and facial recognition, and lower usage of fingerprints.

Table 2: Multi-Factor Authentication

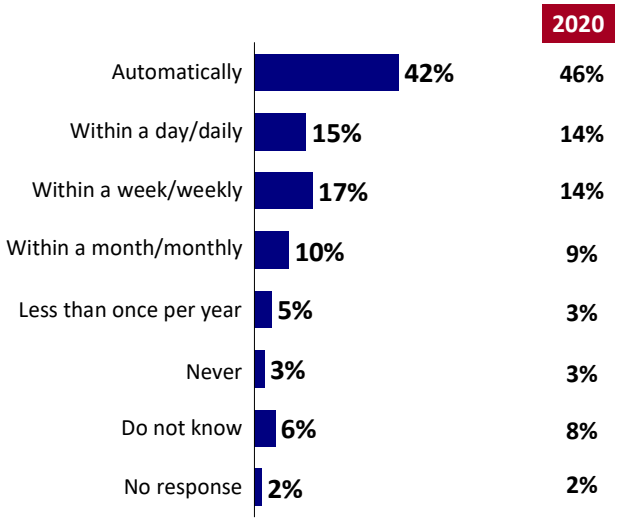
--	Total 2022	Total 2020
Q6. Do you use multi-factor authentication?	*n=2050*	*n=2710*
Yes	69%	53%
No	17%	31%
Do not know	12%	14%
No response	2%	2%
Q7. Which of the following authentication factors have you used?	*n=1423*	*n=1423*
Code received by text message	87%	79%
Code received by email	66%	64%
Passwords	62%	65%
PINs	60%	63%
Fingerprints	49%	57%
Code received by an authentication application	47%	41%
Code received by phone call	32%	29%
Facial recognition	32%	23%
Passphrases	17%	20%
Token devices	14%	14%
Voice verification	9%	9%
Smart cards	5%	7%
USB drives	4%	4%
Other	2%	2%
Do not know	0%	1%
No response	0%	1%

- Canadians aged 25-44, along with men, those with a university education, and higher income, are more likely to use multi-factor authorization. Regionally, residents of Alberta, British Columbia and the Territories, and Ontario are most likely to use authentication; those in Quebec are least likely.
- Younger Canadians (under age 35) are more likely to use a code received by email, text, or an authentication application.
- Men are apt to use a code received by an authentication application, or token devices, then women. Women are more likely than men to use voice verification.
- Canadians with a university education, and higher income, are more apt to use a code received by text, by an authentication application, or token devices. Those with higher

education are also more likely to say they use passphrases. Parents, along with those with higher income are apt to use facial recognition or fingerprints.

For nearly half (42%), operating system updates happen automatically. For others, updates are typically enabled within a day (15%), week (17%), month (10%) or year (5%). A small proportion (3%) claims that they never enable updates. Results do not vary notably from 2020.

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=2050; 2020: n=2710

- Those more likely to rely on automated schedules to update their operating system are aged 35 or older compared with other age groups. Younger Canadians are more likely to update weekly.
- Residents of Quebec are more likely to rely on automatic updates. Those in Saskatchewan are apt to say they update daily.
- Canadians with a university education, and higher income, are more likely to update weekly.

Nine in ten (92%) Canadians secure their home Wi-Fi with a unique password, although 25% used the default password. Seven in ten (68%) created the password. Only 17% use a guest network with a separate password for visitors. Results are fairly consistent with 2020.

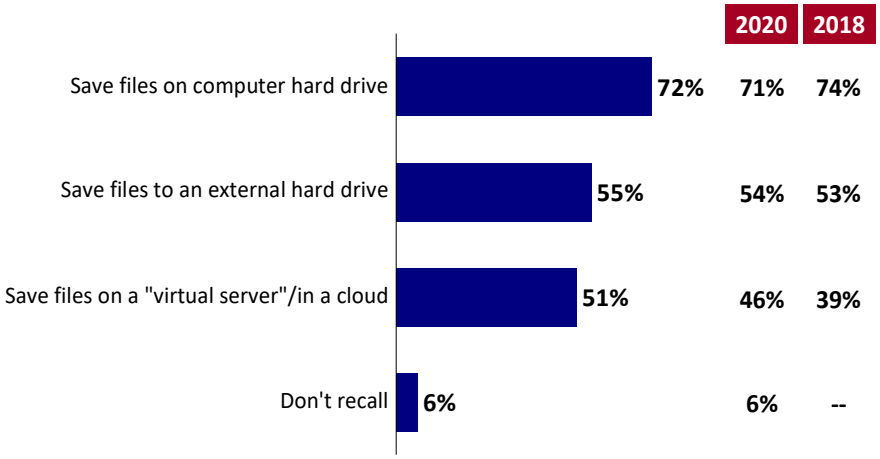
Table 3: Securing WiFi

--	Total 2022	Total 2020	Total 2018
QB2B. Do you secure your home Wi-Fi with a unique password?	*n=2050*	*n=2710*	*n=2072*
Yes	92%	90%	96%
No	3%	4%	3%
Do not have Wi-Fi at home	2%	3%	--
Do not know	1%	2%	1%
No response	1%	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=1889*	*n=2430*	
Yes, default password	25%	29%	
No, I created it myself	72%	68%	
Do not know	2%	2%	
No response	2%	1%	
Q10. Do you use a guest network with a separate password for your smart devices and/or for visitors?	*n=2050*	*n=2710*	
Yes	17%	17%	
No	78%	77%	
Do not know	3%	4%	
No response	3%	3%	

- Although almost everyone secures their home Wi-Fi, this is most prevalent among Canadians under age 45, along with parents, and those with higher education and income. Those aged 65 and over are more likely to say they do not secure their home Wi-Fi, or that they do not have Wi-Fi.
- The default password is used somewhat more commonly among those aged 55 to 64 compared with other age groups. It is also more prevalent in Manitoba compared with other regions, those with lower income, as well as among women compared with men.
- While relatively few use a guest password, this is somewhat more common among those 35 to 54, and particularly among parents, compared with other Canadians

Nearly three in four (72%) Canadians save their files on a computer hard drive. Over half (55%) store their data on an external hard drive and/or (51%) have implemented a virtual server or cloud. Results were very similar in 2020 and 2018, although the proportion of Canadians rely on the cloud has been increasing steadily since 2018.

Chart 10: Data Storage

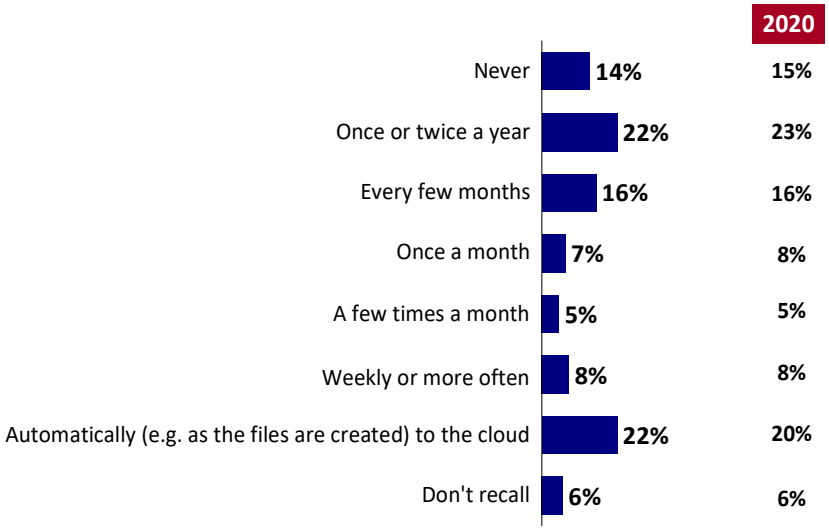


QD1B. Thinking about data storage of information for personal use, do you save information on your computer hard drive, an external hard drive (i.e., extra storage / back up), or on a "virtual server" (i.e., cloud computing)?
Base: n=2050; 2020: n=2710; 2018: n=2,072

- Education, age, income, and gender are strong predictors of whether any type of the above data storage options is used. Canadians age 44 or under are more likely than older counterparts to use a cloud, which is also more common among parents with children aged 6-12. 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 (22%), data and personal files stored on a computer, smartphone, or other mobile device are automatically saved to the cloud. A similar proportion (22%) 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 (7%), a few times a month (16%) or weekly or more (8%). A portion of Canadians never (14%) backs up their files. Results are consistent with those reported in 2020.

Chart 11: Frequency of Backing Up Devices



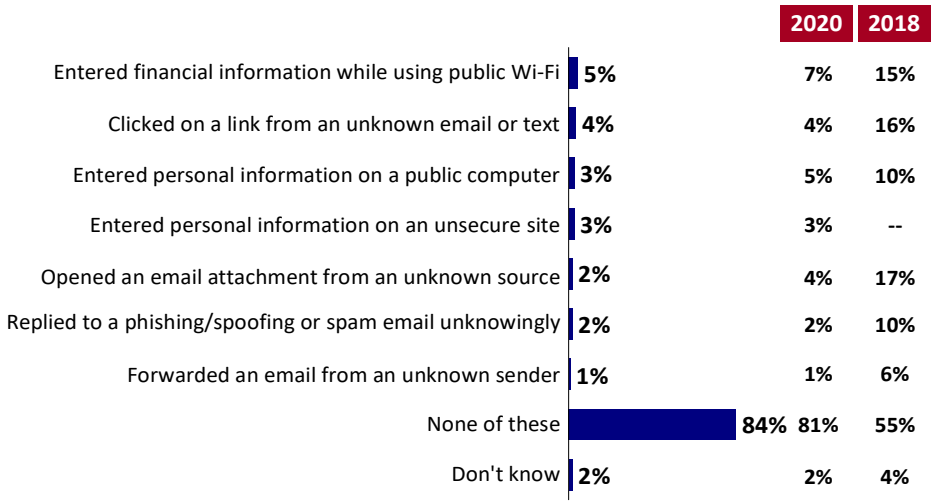
QB5X. How often do you back up data/personal files stored on your computer, smartphone or other mobile device?
Base: n=2050; 2020: n=2710; 2018: n=1,880

- Canadians under age 45, along with parents, and those with at least $80,000 in annual household income are more likely to say they automatically back up files to the cloud. Those age 65 and over are apt to never back up their files. Those with a high school education, or lower education, are also likely to say they never back up their files.

In the past month, eight in ten (84%) 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 (5%), clicked on a link from an unknown email or text (4%), entered personal information on a public computer (3%), entered personal information on an unsecure site (3%), opened an email attachment from an unknown source (2%), replied to a phishing, spoofing or spam email unknowingly (2%), or forwarded an email from an unknown sender (1%).

Results do not vary notably from 2020. 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



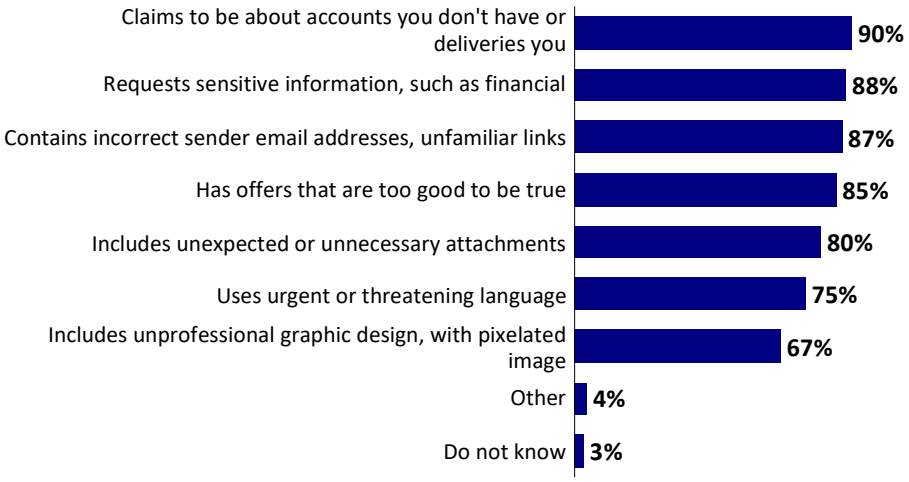
2018 question: To your knowledge, have you ever done any of these things?

QB11. In the past month, have you...?
Base: n=2050; 2020: n=2710; 2018: n=2,072

- Those under age 25 are more likely than others to have entered personal information 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.

Survey results suggest that most generally recognize the signs of phishing email, including claims that are unlikely (90%), requests for financial or other sensitive information (88%), contains incorrect email information or unfamiliar links (87%) or features offers that are too good. Eight in ten also recognize that suspect attachments or use of urgent threats (75%) point to phishing email. Use of a less that professional looking graphic is another indication noted by two in three.

Chart 13: Signs of Phishing



Q11b. As far as you know, what are signs of phishing?
Base: n=2135

- Those between 25 and 45 are generally more likely to recognize the signs of phishing emails, while those who are 65 or older are least likely to do so. This is also the case among those with a high school level of education, compared with those with post-secondary, and in particular those with a university level of education. This is echoed in the pattern based on household income.

D. INFORMATION

Two in five Canadians have looked up information about types of cyber security threats (42%) or information on how to tell if an email is a scam (39%). About one-third have looked for information on securing home Wi-Fi (36%) or how to protect mobile devices (33%). One in four have looked for information on steps to take to use public Wi-Fi safely (25%), to protect other internet connected devices (such as smart TVs, home security systems, fitness monitors, voice activated devices (25%), or using social networking sites safely (23%). About one in ten have looked for cyber security advice for children (13%) or seniors (10%). One in four (28%) have not looked for any cyber security information.

Results are similar to 2020, with slightly fewer searching information on how to tell if an email is a scam, and slightly more saying they have not searched for 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).

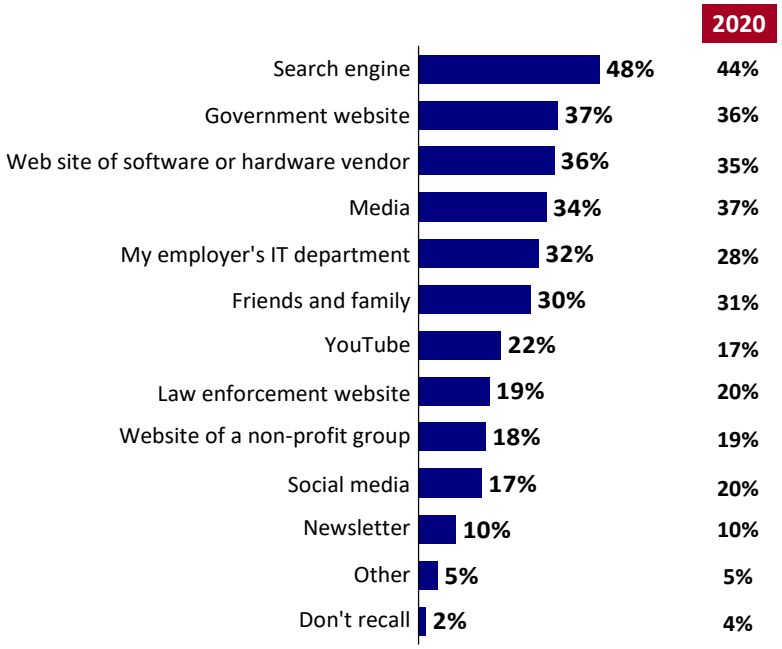
Chart 14: Type of Information Looked For

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=2050; 2020: n=2710; 2018: n=2,072

- Younger Canadians (under age 35) are more likely to have looked for information on steps you can take to use public Wi-Fi safely. Those aged 25-34 are apt to look for steps to use social networking sites safely, protecting other internet connected devices, mobile devices, or cyber security threats. Canadians who are 65 or older are more likely than others to have searched for information on internet safety for seniors. Those aged 45-54 are comparatively more likely to have looked for information on securing home Wi-Fi, and, along with those 35-44, are more likely to look for cyber security advice for children.
- Parents are more likely than those with no children under 18 at home to say they have looked for cyber security advice for children.
- Men, along with those with higher education and income, are more likely than women and those with less education and income to report searching for information on most areas. Canadians with high school or college education are more likely than those with a university education to say they have not searched for any information.
- Residents of British Columbia and the Territories are more likely than those in other regions to look up steps to take to use public Wi-Fi safely.

For 48% of Canadians, information on cyber security was found by using a search engine. About three in ten found information through a government website (37%), a software or hardware vendor's website (36%), the media, including a news organization's website (34%), through their employer's IT department (32%), or through friends and family (30%). One in five sourced information through YouTube (22%), a law enforcement website (19%), the website of a non-profit group (19%), or social media (17%). Ten percent found information in a newsletter. Results do not vary notably from 2020.

Chart 15: Information Source



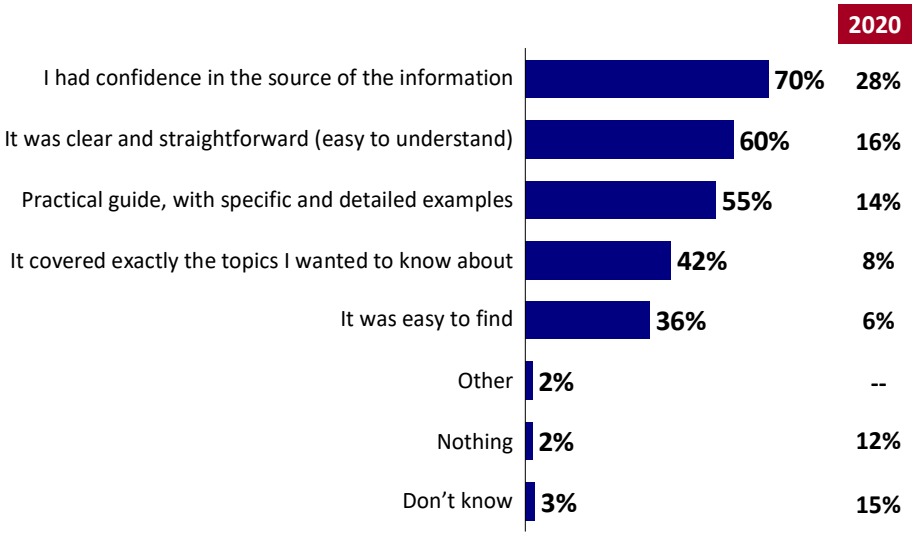
QIC5b. Where did you find that information?
Base: n=1394 (2022); n=1977 (Anyone searching for information topics listed in Chart 13)

- 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 those with higher education and income, 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 65 and over have a higher tendency than younger age segments to look for information on a website of a vendor or the media.
- 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.

- Residents of Ontario, along with Canadians with lower income, are more apt than those in other regions to have used YouTube.

Seven in ten (70%) found the information helpful because of their confidence in the source of the information. Over half say the information was helpful because it was clear and straightforward (60%), or because it offers a practical guide with specific steps and detailed examples (55%). Roughly two in five had confidence because the information covered precisely the topics they wanted to know about (42%) or that the information was easy to find (36%). Multiple responses could be selected in the question, although this was not the cases in 2020 making comparisons difficult; however, it still useful to note that the ordering from higher magnitude to lower is the same as found in 2020.

Chart 16: Reasons Information is Helpful

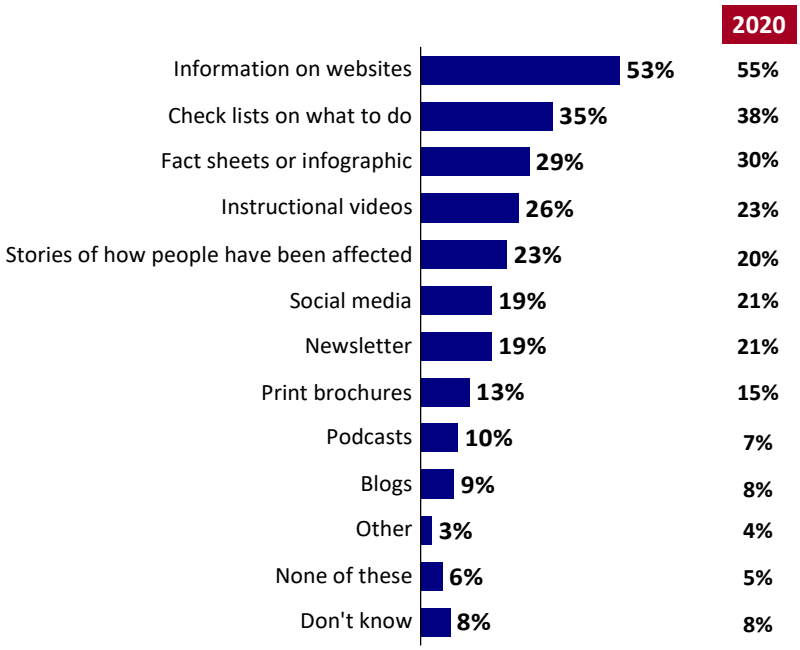


QIC8b. What was it about this information that made it helpful?
Base: n=1394 (2022); n=1977 (Anyone searching for information on one of the listed topics in Chart 13)

- Younger Canadians are more likely than those 25 or older to say the information was easy to find (this group was more apt to have used social media or YouTube).
- Parents of younger children (aged 6-12) are less likely to say any of the reasons.
- Those with a university education or higher income are more likely than individuals with less education and income to say they were confident in the source of the information. Those with higher income are also more likely to say the helpful information was a practical guide.

Over half (53%) of Canadians prefer to get information on cyber security protection through websites. Three in ten prefer check lists on what to do (35%) or fact sheets or infographics (29%). One in four say they prefer instructional videos (26%), or stories of how people have been affected (23%). One in five indicate social media (19%), or newsletters such as email subscriptions (19%). Fewer cite print brochures (13%), podcasts (10%) or blogs (9%) as their preferred vehicle for getting the information. Results do not vary considerably from 2020.

Chart 17: Preferred Type/Method of Information



Q20. How do you prefer to get information to protect yourself from cyber threats?
Base: n=2050; 2020: n=2651

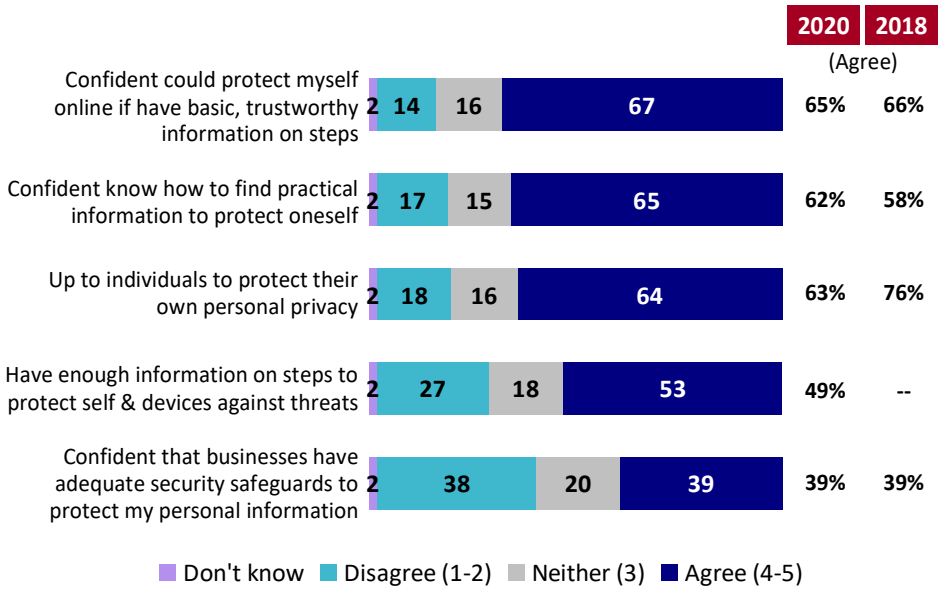
- Younger Canadians (under 25) are more likely than other age groups to prefer instructional videos or social media. Older Canadians (55 and over) are more likely than those who are younger to prefer check lists of what do to, print brochures or newsletters.
- Individuals who are between 25 and 34 are more likely to prefer podcasts or blogs, while those 35-44 are the group most likely to indicate fact sheets or infographics.
- Residents of Manitoba are more likely to prefer print brochures, while those in Quebec are apt to prefer checklists and newsletters.
- Men are more likely than women to prefer information on websites and blogs. Women prefer checklists or fact sheets.

- Those with a university education are more likely than others to cite information on websites, checklists, or fact sheets. Those with higher income (over $150,000) are more likely to prefer fact sheets or workplace training. Canadians with lower income are more likely to prefer print brochures.

Two-thirds (67%) 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 feel confident that they know how to find practical information to protect themselves online (65%) or agree that it is up to individuals to protect their own personal privacy (64%). Only half (53%), 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 are similar to 2020; however, compared to 2018, more Canadians are confident they know how to find practical information (up to 65% from 58% in 2018), and less apt to agree that it is up to individuals to protect their own personal privacy (down to 64% compared with the 76% who agreed in 2018).

Chart 18: Attitudes about Information



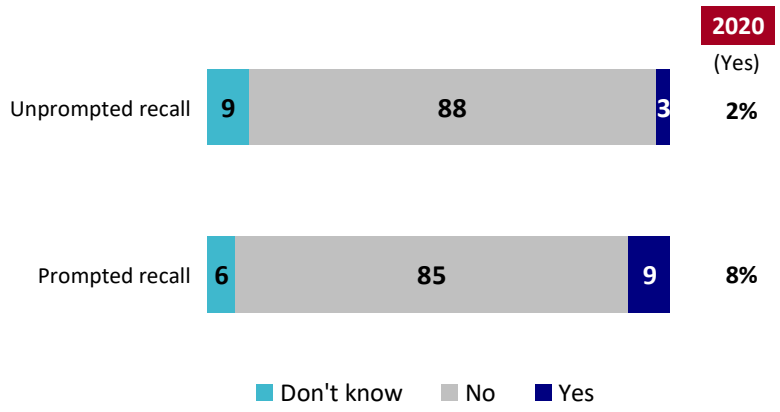
QA13, A11B, A118, Q120, A110. Please rate the degree to which you agree or disagree with the following statements.

Base: n=2050; 2020: n=2710; 2018: n=2,072

- Those with a university education are least likely to agree that it is up to individuals to protect their own personal privacy. Those with higher income ($150,000 and over) are apt to agree that they have enough information to protect themselves and devices, or they are confident they know how to find practical information.
- Canadians aged 18-54 are more likely to agree that they have enough information on how to take steps to protect themselves against cyber threats; those 55 and over are apt to disagree. Younger Canadians, under age 35, are more likely to express confidence that they could protect themselves online as long as they have basic, trustworthy information, or that they know how to find practical information.
- Men are more likely than women to be confident they can find practical information to protect themselves online.

Very few (3%; 2% in 2020) 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 (9%; 8% in 2020) reported familiarity with the Get Cyber Safe campaign from the Government of Canada.

Chart 19: Awareness of Get Cyber Safe Campaign



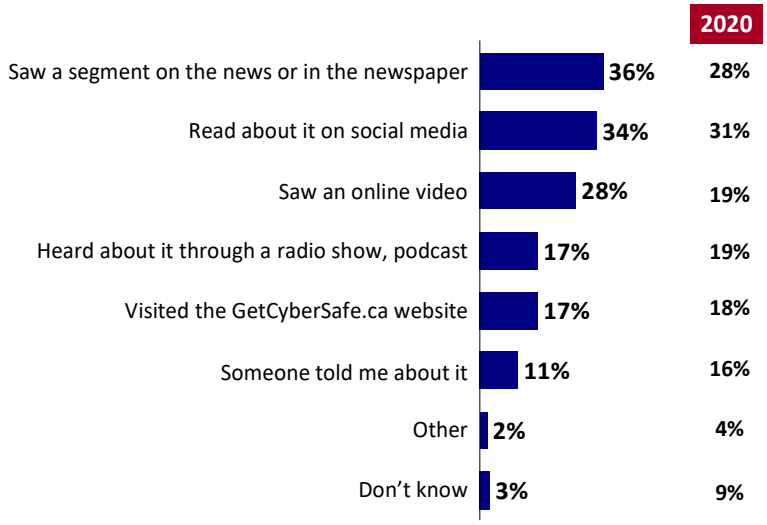
Q23. There is a Government of Canada awareness campaign created to inform Canadians about cyber security and the simple steps they can take to protect themselves online. Can you name this campaign?
Base: n=2050; 2020: n=2683

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=2050; 2020: n=2683

- When prompted, younger Canadians (under age 25), are more likely than those over age 25 to say they heard of Get Cyber Safe.

Of those who indicated familiarity with the Get Cyber Safe campaign, 36% saw a segment on the news or in the newspaper and 34% say they read about Get Cyber Safe on social media. Just over one in four (28%) saw an online video. Fewer than one in five heard about it through a radio show or podcast (17%), visited the GetCyberSafe.ca website (17%), or heard from someone else (11%). More Canadians who are aware of the campaign said they saw a segment in the news or newspaper, an online video, or that someone told them about it than in 2020.

Chart 20: Reason for Awareness of Get Cyber Safe Campaign



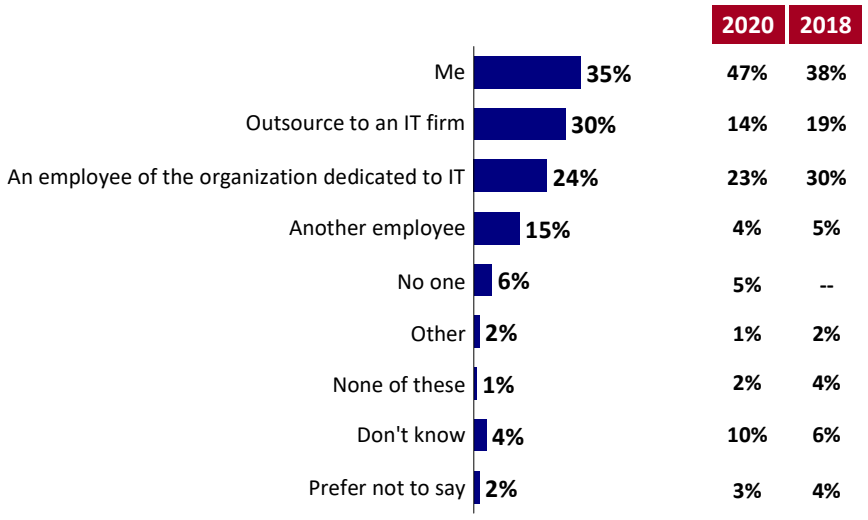
QGOCADA. Where did you see, hear, or read this?
Base: n=180; 2020: n=210

E. EXPERIENCE OF BUSINESSES

Over one in three (35%) of business owners or managers are responsible for their company's IT. Three in ten (30%) outsource to an IT firm. One in four (24%) cite an employee of the organization dedicated to IT and another 15% indicate another general employee is responsible. Six percent do not have anyone responsible for IT.

Notably more owners and managers indicating that they outsource to an IT firm (30%) more than in 2020 (14%) or 2019 (19%). There is also an apparent increase in of business owners or managers responding who have another employee (not dedicated to IT) responsible; and increase of about 10% from 4% in 2020 and 5% in 2018.

Chart 21: Responsibility for IT

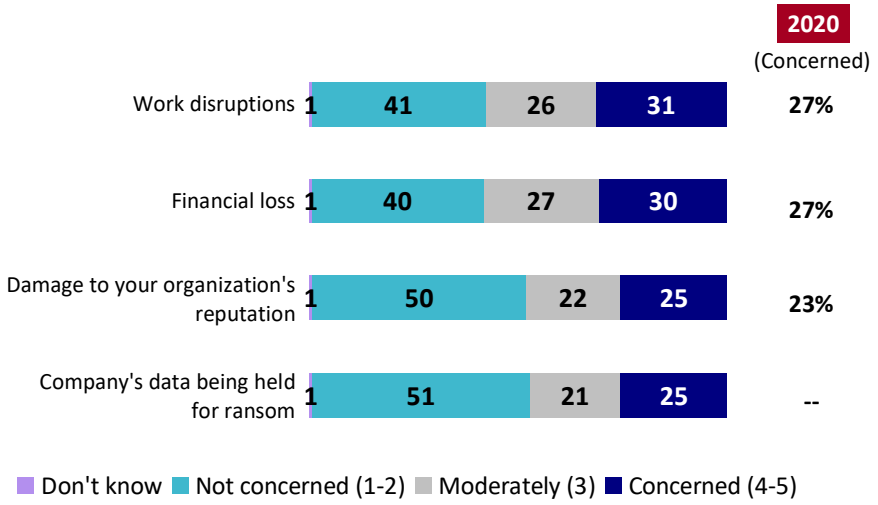


QBUS4. Who is responsible for your company's IT?
Base: n=301; 2020: n=356; 2018: n=533

- Smaller companies with 10 or fewer employees more often say that they are responsible for IT compared with those with more employees. Representatives of the larger organizations (11+ employees) are considerably more likely to point to another employee in the organization or outsourced management to an IT firm.
- Older business owners or managers (age 65+) are more likely than younger representatives to say they are responsible for their company's IT.

When thinking about the various concerns of daily operations, three in ten business owners or managers are concerned about work disruptions (31%) or financial loss (30%) in the event of a cyber threat. One in four are concerned about damage to the organization's reputation (25%) or the company's data being held for ransom. Concern in each of the three areas measured in 2020 are only marginally greater in 2022.

Chart 22: Level of Concern

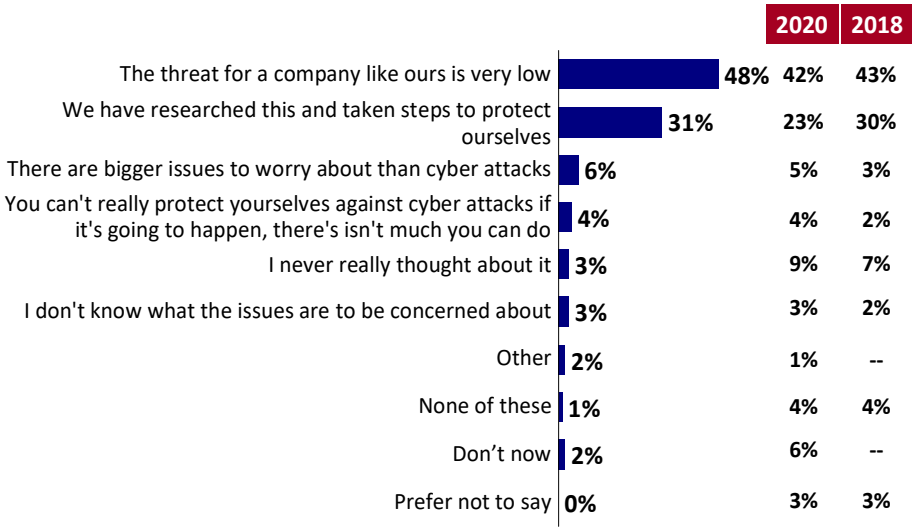


QBUS5A1-A3. Thinking about the various concerns of daily operations of your organization, how concerned are you that a cyber threat will cause...?
Base: n=301; 2020: n=360

- Smaller organizations, with 10 or fewer employees, are less likely to be concerned about work disruptions, or having their company's data held for ransom, where as a third of organizations with more than 10 employees said they are concerned.
- Results do not vary significantly by demographic groups.

Among those who are not concerned, nearly half (48%) cite their perception of minimal threat for their type of company (also listed as the top factor by a similar proportion in 2020 and 2018). Almost one in three (31%) say they have conducted research and taken steps to protect their business. Far fewer say they have bigger issues than cyber attacks to worry about (6%), feel they can't really protect themselves against cyber attacks (4%), report they have never really thought about cyber security (3%), or don't know what the issues are to be concerned about (3%).

Chart 23: Reasons for Lack of Concern



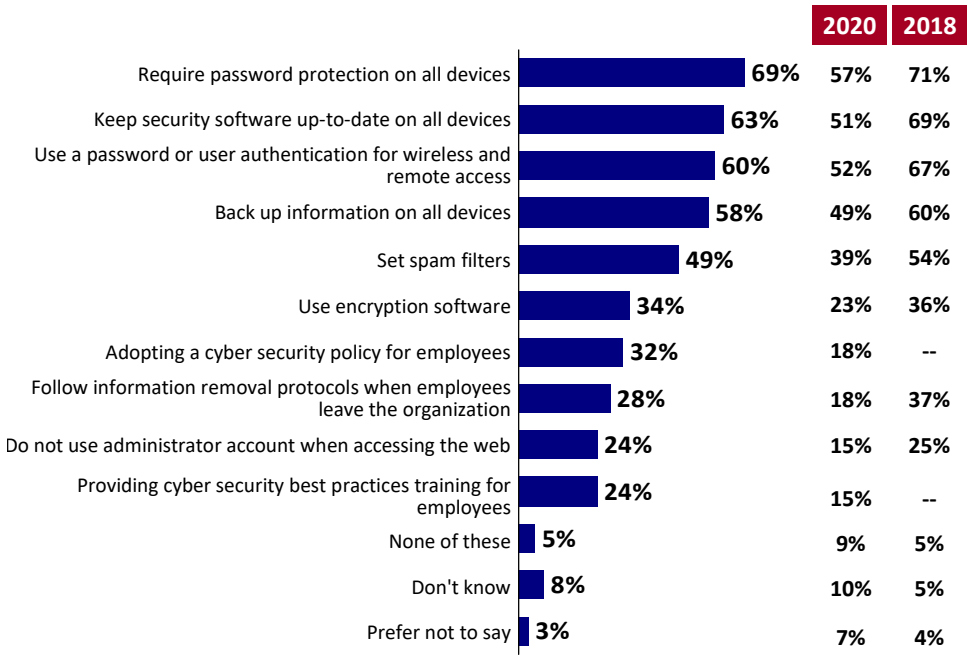
QBUS5B. Why is this?

Base: n=188; 2020: n=203; 2018: n=533

- Individuals representing smaller organizations, with 10 or fewer employees, more often said they are not concerned about these potential impacts because the threat for their company is low.
- The same pattern holds for those with a college education.

Roughly two in five business owners or managers report that their business has implemented password protection on all devices (69%), kept security software up to date on all machines (63%), or use password or user authentication for wireless and remote access (60%). Over half (58%) have taken the steps to back up information on all devices while fewer (49%) have set spam filters to protect against online threats. About one in three have implemented encryption software (34%) or adopted a cyber security policy for employees (32%). About one in four followed information removal protocols when employees have left the organization (28%), refrain from using an administrator account when accessing the web (24%), or provided cyber security training for employees (24%). All steps reported have increased since 2020, but remain lower than findings in 2018.

Chart 24: Steps Taken to Prevent/Protect Against Attacks



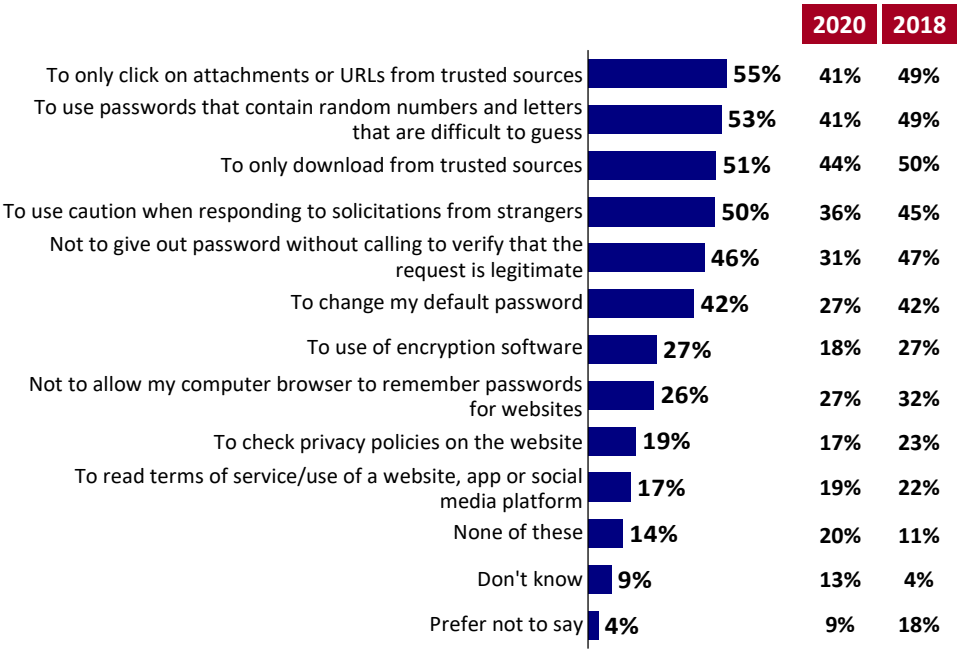
QBUS1. Turning to your work as a business owner/manager, which of the following steps has your business taken to protect itself against online threats?
Base: n=301; 2020: n=360; 2018: n=533

- Those using an IT firm are more likely to ensure devices have up-to-date software and spam filters, as well as use of password or user authentication for wireless remote access. Those using in-house IT staff are more likely than others to adopt a cyber security policy for employees, use encryption software, follow information removal protocols for employees who have left, and provide cyber security best practices training to employees. Those who are personally responsible for IT more often point to regular back ups on all devices.
- Larger organizations with more than 10 employees are more likely to point to many of these security measures (e.g., password protection requirement on devices and use of wireless, cyber security policies and training, encryption software)
- Those with higher income are more likely to say they provide cyber security best practices training, or adopt a cyber security policy for employees.

About two in five business owners or managers report that employees are instructed to only click on attachments or URLs from trusted sources (55%), to use passwords that contain random numbers and letters that are difficult to guess (53%), to only download from trusted sources (51%), or to use caution when responding to solicitations from strangers (50%). About two in five instruct employees to not give out passwords without calling to verify that the request is legitimate (46%) or to change default passwords (42%). One in four ask employees to use encryption software (27%) or to not allow computer browsers to remember passwords for websites (26%). Less than one in ten ask employees to check privacy policies of websites (19%) or read terms of service of a website, app, or social media platform (17%). Just over one in ten (14%) do not provide any instructions to employees to protect the organization against cyber threats.

Most instructions to employees are reported at higher levels than in 2020, with the top four are also an increase from 2018.

Chart 25: 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=301; 2020: n=360; 2018: n=533

- Larger organizations with more than 10 employees are more likely to instruct employees to only click on attachments or urls they trust and use caution when responding to solicitations from strangers. The latter is also more often instructed when there is an in-house IT staff.Those who are personally responsible for IT are more likely than others to instruct employees to use appropriate password rules and only download from trusted sources.

Half of business owners or managers say that their organization would benefit from guidelines for reacting to a cyber attack (50%) or from a list of the types of threats that exist and clues to look out for (49%). About two in five feel they would benefit from steps to protect mobile devices in a public setting (44%), best practise for employees on how to handle passwords (44%), information on best practices for safe cloud computing (43%), guidelines on use of personal devices for work (42%), resources on how to encrypt computers, laptops, and storage devices (41%), tips on the type of software/hardware to make networks secure (41%), or guidelines to establish rules for safe email usage policies (40%). Nearly as many say they would benefit from best practices for use of storage devices (39%) or best practices on a clear internet usage policy (38%). About one in three feel they could protect their organization with tips on communicating the importance of following cyber security to employees (35%) or information on steps for handling work-related information possessed by departing employees (33%). One in four identify the need for guidelines on how to establish strong social media policy (28%).

Table 4: Beneficial Information for Small and Medium Businesses

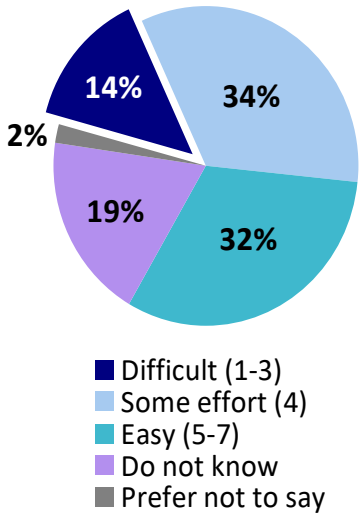
--	**Total 2022**	**Total 2020**	**Total 2018**
QBUS3. Which of the following types of information do you feel that your organization would benefit from having in order to protect itself against cyber threats?	*n=301*	*n=360*	*n=533*
Guidelines for reacting to a cyber attack	50%	40%	46%
A list of the types of threats that exist and cues to look for	49%	41%	47%
Steps to protect mobile devices in a public setting	44%	39%	40%
Best practices for employees on how to handle passwords	44%	29%	37%
Best practices for safe cloud computing (with definition of cloud computing)	43%	36%	35%
Guidelines on use of personal devices for work	42%	31%	40%
Resources on how to encrypt computers, laptops, and storage devices	41%	34%	37%
Tips/resources for the type of software/hardware to make networks secure	41%	29%	36%
Guidelines to establish rules for safe email usage policies	40%	28%	39%
Best practices for use of storage devices (e.g. USBs)	39%	34%	40%
Best practices for a clear internet usage policy	38%	27%	37%
Tips on communicating the importance of following cyber security policies to employees	35%	25%	32%
Steps for handling work-related information possessed by departing employees	33%	22%	33%

--	Total 2022	Total 2020	Total 2018
Guidelines on how to establish strong social media policy	28%	26%	37%
Other	4%	3%	4%
None of these	5%	9%	8%
Do not know	11%	13%	12%
Prefer not to say	4%	7%	7%

- Among those respondents who are personally responsible for IT the demand for each of these types of information is higher than it is among other respondents suggesting that the demand for this type of information may be 10 to 15 points higher than indicated.
- In smaller organizations, with 10 or fewer employees, the demand is comparatively higher for tips on the type of software or hardware to make networks secure.
- Compared with smaller organizations, the demand is higher in organizations with more than 10 employees for larger for guidelines for reacting to a cyber attack, and employees' use of personal devices for work, as well as best practices for employees regarding passwords, and tips on communicating the importance of cyber security policies.

Nearly half of business owners or managers anticipate that it would take some effort (34%) or be difficult (14%) to recover from a ransomware attack. About one in three (32%) believe it would be easy. One in five (19%) are not sure or prefer not to say (2%).

Chart 26: Recovery from a Ransomware Attack

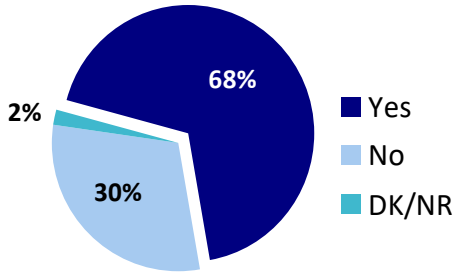


BUSBA42. How well would your organization be able to recover from a ransomware attack?
Base: n=301

- Representatives of organizations with 10 or fewer employees are more likely than their counterparts in larger companies to say it would be easy to recover from an attack. This pattern is also true among those with higher education

Two in three business owners or managers indicate they have employees who work from home, even some of the time.

Chart 27: Employees Working from Home

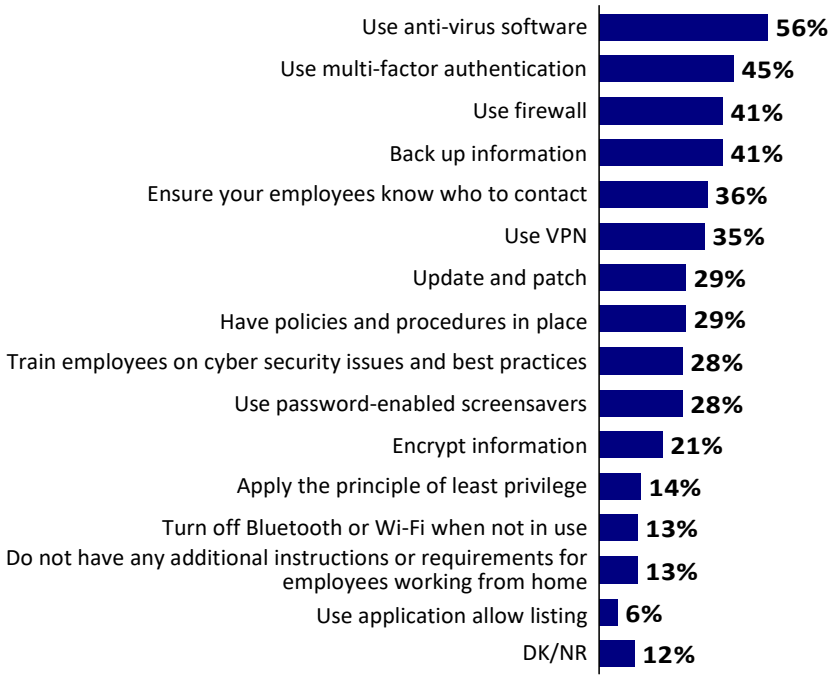


QBUS2B. Does your organization have employees who work from home, even some of the time?
Base: n=301

- Incidence of having employees who work from home at least some of the time is higher among organizations with more than 10 employees.
- Those with higher education are more apt to have employees who work from home, along with parents with children aged 6-12 or 13-15.

Over half (56%) of business owners or managers report requiring the use of anti-virus software for employees who work from home to protect the organization against cyber threats. About two in five indicate they require the use of multi-factor authentication (45%), a firewall (41%) or back up information (41%). Over one in three business owners or managers say they ensure their employees know who to contact (36%) or use a VPN. More than two in ten require an update and patch (29%), have policies and procedures in place (29%), train employees on cyber security issues and best practices (28%), use password-enabled screen savers (28%), or encrypt information (21%). Other instructions or requirements include applying the principle of least privilege (14%), turn off Bluetooth or Wi-Fi when not in use (13%), or use application allow listing (6%). Over one in ten do not have any additional instruction or requirements for employees working from home (13%) or are not sure (12%).

Chart 28: Protecting Home Workers against Cyber Threats



QBUS2C. What additional instructions or requirements do you have for employees who work from home to protect the organization against cyber threats?
Base: n=209

- Smaller organizations, as well as those where the respondent is responsible for IT, are more likely than others to say they instruct employees to back up their information.

- Those representing larger organizations are more likely than the smaller companies to instruct employees to use a VPN, ensure employees know who to contact about an IT issue, have policies and procedures in place and train employees on cyber security issues and best practices. These are particularly likely if the organization has IT staff.

APPENDICES

A. METHODOLOGY DETAILS

The sample consists of 2,050 completed interviews with Canadians 18 years of age or older who use the internet on a regular basis, including 553 interviews with parents of youth between the ages of 16 and 24, and 301 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 12,295 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 17 per cent[3]. The final survey sample of 2,050 yields a level of precision of +/-2.2 per cent for the sample overall and +/-3 to 6 per cent for most sub-groups that could be isolated in the analysis (including all regions, age, education, and income segments).

Prior to conducting the survey, the instrument was tested with 14 cases in English and 10 cases in French. Additional questions were placed on the pretest version of the questionnaire asking

[3] Among the sample of 12,295 cases, 58 bounced as undeliverable (12,237 valid sample) and 31 were screened out as out of scope.

about length, flow, clarity of wording and so on to elicit feedback from respondents. Minimal changes were made as a result of the testing.

The survey was administered between January 21 and February 14, 2022, using a 15-minute 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 5: Demographic Table

Table 5a: Province / Territory (unweighted)

-	**Total**
n=	*2050*
British Columbia and Yukon	13%
Alberta and Northwest Territories	12%
Saskatchewan and Manitoba	10%
Ontario	36%
Quebec and Nunavut	21%
Atlantic	9%

Table 5b: Gender (unweighted)

-	**Total**
n=	*2050*
Male	48%
Female	50%
Prefer to self-identify	2%
Prefer not to say	1%

Table 5c: Age (unweighted)

-	**Total**
n=	*2050*
18-24	4%
25-34	18%
35-44	21%
45-54	19%
55-64	17%
65 up	21%

Table 5d: Children under the age of 18 in the home

--	**Total**
n=	*2050*
Yes	25%
No	74%
Prefer not to say	0%

Table 5e: Age of children in the home

-	**Total**
n=	*553*
Under 5	39%
6 to 12	47%
13 to 15	31%
16 or older	34%
Prefer not to say	1%

Table 5f: Level of education completed

-	**Total**
n=	*2050*
High school or less	13%
Some post secondary	12%
College, vocational or trade certificate or diploma	25%
Undergraduate university degree	27%
Graduate or professional degree	22%
Prefer not to say	1%

Table 5h: Annual household income

-	**Total**
n=	*2050*
<$20,000	4%
$20,000-$39,999	10%
$40,000-$59,999	12%
$60,000-$79,999	12%
$80,000-$99,999	11%
$100,000-$149,999	20%
$150,000 or more	17%
Don't know/No response	13%

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 underrepresented 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.

B. SURVEY QUESTIONNAIRE

WINTRO

Thank you for participating in this survey. Ekos Research Associates, a Canadian public opinion research company is conducting the survey on behalf of the Government of Canada about issues related to online security. Si vous préférez répondre au sondage en français, veuillez cliquer sur français. **Your participation is optional and your responses will be kept entirely confidential and anonymous.** The survey takes 15 minutes to complete. It is being directed by EKOS Research, and is being administered according to the requirements of the *Privacy Act*. To view our privacy policy, click here. This survey is registered with the Canadian Research Insights Council's (CRIC) Research Verification Service. Click here if you wish to verify its authenticity (project code 20220121-EK115) If you require any technical assistance, please contact online@ekos.com.

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
Prefer not to say	99

QEMP

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

Please specify	77
None	97
Do not know	98
No response	99

QEMPA

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

Over 100	1
Under 100	2
Do not know	98
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
Prefer not to say	99

QCHILDA [1,6]

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
Prefer not to say	99

D4

In what year were you born?

Year:	1
Prefer not to say	9999

QAGEA

Are you at least 18 years of age?

Yes	1
No	2
No response	99

QAGEY

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

No response	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

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 at 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 (please specify)	77
None of these	98
Do not know	99

Q6

MFA

Do you use <hover="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">multi-factor authentication>?

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
Do not know	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
Do not know	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 message	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

B11B [1,10]

As far as you know, what are signs of phishing?

Please select all that apply

Uses urgent or threatening language	1
Requests sensitive information, such as financial or identifying information	2
Has offers that are too good to be true	3
Claims to be about accounts you don't have or deliveries you're not expecting	4
Contains incorrect sender email addresses, unfamiliar links, spelling or grammar errors	5
Includes unexpected or unnecessary attachments, that may have strange file names or uncommon file types	6
Includes unprofessional graphic design, with pixelated images or poor formatting	7

Other (please specify)	77
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

Q11D

In the next year, how likely do you feel it is that you will be affected by a cyber threat where your data will be held for ransom?

1 Not at all likely	1
2	2
3 Moderately likely	3
4	4
5 Extremely likely	5
Do not know	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 or financial data held for ransom (Ransomware)	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 (please 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
Phishing	6
Ransomware	7
None of these	97
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
Disconnect all devices that are connected to your network	11
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 (please 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 (please specify)	77
None of these	97
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 (please 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
Do not know	99

IC8B [1,8]

1-9,77, IC5A

What was it about this information that made it helpful?

Please select all that apply

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 (please specify)	77
Nothing	97
Do not know	99

QEMPE

How often do you work from home?

Part time	1
Full time	2
As needed	3
Never	4
Do not know	8
No response	9

QEMPF

Have you been given any specific instructions or requirements by your employer to protect the organization from cyber threats?

Yes	1
No	2
Do not know	8
No response	9

QEMPFB [1,10]

If yes, what type of instructions or requirements have you been given by your employer?

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

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

IC6 [1,15]

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

Please select all that apply

Friends or family	1
Internet Service Provider	2
Security software company	3
Financial Institutions	4
Vendor website (e.g. online store where you are shopping, etc.)	5
Not-for-profit organization dedicated to electronic security	6
Government	7
Law enforcement organization	8
Other (please specify)	77
Do not know	98
No response	99

BUS1 [1,20]

FT/PT (D2) and responsible (EMPB) OR S-E (D2) AND Size <100 (QEMP / QEMPA)

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]

Which of the following instructions do you provide to employees to protect the organization against cyber threats and to protect 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

QBUS2B

Does your organization have employees who work from home, even some of the time?

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

QBUS2C [1,20]

What additional instructions or requirements do you have for employees who work from home to protect the organization against cyber threats?

Select all that apply

Use VPN	1
Use firewall	2
Use anti-virus software	3
Use application allow listing	4
Have policies and procedures in place	5
Ensure your employees know who to contact	6
Train employees on cyber security issues and best practices	7
Use multi-factor authentication	8
Use password-enabled screensavers	9
Update and patch.	10

Turn off Bluetooth or Wi-Fi when not in use	11
Back up information	12
Encrypt information	13
Apply the principle of least privilege	14
Do not have any additional instructions or requirements for employees working from home	97
Do not know	98
No response	99

BUS3 [1,20]

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 b> 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 (please specify)	77
None of these	97
Do not know	98
Prefer not to say	99

BUS4 [0,20]

Who is responsible for your company's IT?

Select all that apply

Me	1
Another employee (specify role in company):	2
An employee of the organization dedicated to IT	3
Outsource to an IT firm	4
No one	5
Other (please specify)	77
None of these	97
Do not know	98
Prefer not to say	99

BUS5A1

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

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

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

BUS5A4

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

...result in my company's data being held for ransom?

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 (please specify)	77
None of these	97
Do not know	98
Prefer not to say	99

BUSBA42

How well would your organization be able to recover from a ransomware attack?

1 With great difficulty and hardship	1
2	2
3	3
4 With some effort, but recover reasonably well	4
5	5
6	6
7 Easily, with limited impact	7
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 Get Cyber Safe 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 (please 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

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

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

<[THNKSP2 = 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.> 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.