Government of Canada Gouvernement du Canada

Get Cyber Safe Awareness Tracking Survey:
2024 Final Report

Prepared for the Communications Security Establishment

Supplier name: Phoenix Strategic Perspectives Inc.
Contract Number: CW2346933
Contract Value: $81,085.41 (including applicable taxes)
Award Date: 2024-01-23
Delivery Date: 2024-03-31
Registration Number: POR # 119-23

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 Study
Final Report

Prepared for the Communications Security Establishment
Supplier name: Phoenix Strategic Perspectives Inc.
April 2024

This public opinion research report presents the results of an online of 2,222 Canadians, aged 18+, conducted by Phoenix SPI on behalf of the Communications Security Establishment (CSE) between February 29 to March 19, 2024.

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

media@cse-cst.gc.ca

Catalogue number:
D96-17/2024E-PDF

International Standard Book Number (ISBN):
978-0-660-72842-1

Related publications (registration number: POR #119-23):
Catalogue number: D96-17/2024F-PDF
ISBN: 978-0-660-72843-8

Table of Contents

List of Figures

Executive Summary

Phoenix Strategic Perspectives Inc. (Phoenix SPI) was commissioned by the Communications Security Establishment (CSE) to conduct the biennial online Get Cyber Safe Awareness Tracking Survey.

Background and objectives

CSE is Canada's national cryptologic agency, providing the Government of Canada with information technology security and foreign signals intelligence. As part of its cyber security focus, CSE operates the Canadian Centre for Cyber Security (the Cyber Centre) which is the single unified source of expert advice, guidance, services, and support on cyber security for Canadians. Since 2018, CSE leads the Get Cyber Safe national public awareness campaign, which was created to inform Canadians about cyber security and the simple steps they can take to protect themselves online.

In support of Get Cyber Safe, CSE has conducted public opinion research (POR) focussed on Canadians' online attitudes and behaviours. POR was first conducted in the form of a national telephone survey in 2020, followed by a national online survey in 2022 (to track changes over time). Prior to that, Public Safety Canada conducted POR for the Get Cyber Safe campaign in 2011, 2017 and 2018. Both surveys were designed to collect data on online Canadians' knowledge and attitudes towards cyber security and cyber safety in the context of the Get Cyber Safe public awareness campaign.

In the spring of 2022, CSE also conducted a separate survey as a contribution to a report entitled *Oh Behave! The Annual Cybersecurity Behaviours and Attitudes Report* which had previously only been conducted in the US and UK. *Oh Behave!* is an annual research report that aims to better understand people's security attitudes and behaviours. A Canadian component was added for the 2022 survey, which focussed on the human factor of cyber risk—specifically, core cyber security behaviours, such as creating and managing passwords, applying multi-factor authentication (MFA), installing the latest updates, checking message legitimacy, recognizing and reporting phishing, and backing up data.

For this iteration of the survey, CSE's 2022 Get Cyber Safe survey and the 2024 *Oh Behave!* Survey were merged to create one comprehensive survey questionnaire designed to undertake the following:

- Assess performance of the public awareness campaign
- Help identify shifts in knowledge, behaviours, and attitudes
- Track awareness, attitudes and behaviour relating to cyber security activities
- Identify and track motivators and barriers to behaviour change
- Identify and track the best ways of communicating information
- Track public expectations in terms of the involvement of the federal government

This year's POR will inform the direction of the Get Cyber Safe campaign, as well as other communications and public messaging from CSE. The use of findings will be two-fold. Research findings will help the Get Cyber Safe campaign to raise the Canadian public awareness about staying safe online, and it will support future policy and communications activities of the Cyber Centre and CSE.

Methodology

A 15-minute online survey was conducted with 2,222 online Canadians aged 18 and older. This included 619 surveys with parents of children under 18 years of age, and 301 surveys 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 was drawn from Advanis' proprietary General Population Random Sample (GPRS) which has been developed using probability-based recruitment; specifically, random digit dialling (RDD) via Interactive Voice Response (IVR) and via live Computer Assisted Telephone Interviewing (CATI). This panel of more than 600,000 individuals can be considered representative of the general public in Canada.

The results were weighted to reflect the actual distribution of Canadians based on region, age, and gender. The margin of error for a sample of this size is ±2%, 19 times out of 20. The margins of error are greater for results pertaining to subgroups of the total sample. The fieldwork was conducted from February 29 to March 19, 2024. More information on the methodology can be found in the Appendix: Technical Specifications.

Key findings

Cyber security practices of online Canadians

The large majority of online Canadians (86%) said they take precautions to protect their online and social media accounts, devices and networks, and two-thirds (65%) do not assume their devices are automatically secure.

Starting with software updates, eight in 10 (81%) know how to install the latest software and app updates across their devices. Among those who know how to install the latest updates, almost nine in 10 (88%) do so regularly, including nearly half (48%) who always do so when notified that updates are available. Those who regularly install updates tend to do so immediately: 51% have automatic updates turned on and 19% run the update upon receipt of the notification.

In addition to installing updates, online Canadians are aware of measures to secure their accounts and tend to use them. Nine in 10 (90%) have heard of multi-factor authentication (MFA), and most of those aware of MFA (87%) know how to enable it and report using it regularly. Those who do not use MFA regularly need to be convinced of the value of this extra layer of security. Four in 10 (39%) non-users do not believe MFA will stop cybercriminals, 24% do not see any benefits to using multi-factor authentication, 21% consider it unnecessary if their device works, and 19% simply do not understand how to use it. Among those who no longer use multi-factor authentication, the single largest proportion (29%) attributed their lack of use to their perception that multi-factor authentication takes too long.

When it comes to their passwords, just over three-quarters (76%) of online Canadians make their passwords complex with a combination of letters, numbers, and symbols. Smaller proportions use a unique password for each account (35%), a password manager (30%), and a password with at least four to 15 characters (27%). For important online accounts, half of online Canadians use unique passwords all (31%) or a majority (27%) of the time.

While many online Canadians are engaging in practices that will help to keep their online accounts safe, some reported taking actions that *could* put their accounts at risk: 39% allow browsers or apps to autofill their passwords, 36% write down their passwords, 31% use the same password for multiple accounts, 10% keep passwords simple and easy to remember, and 2% share their password.

Additionally, when online, Canadians take steps to verify the legitimacy of a website. The majority analyse the overall look of the website (58%) or check for "https" in the address bar (54%). Many also check for a padlock symbol in the website's address bar (45%) or conduct research to validate that a website is legitimate website (42%). Most online Canadians also recognize the signs of phishing messages, including claims about accounts they do not have or unexpected deliveries (89%), requests for sensitive information (88%), and messages containing incorrect email addresses, unfamiliar links, or spelling or grammar mistakes (86%). Almost as many recognize that messages containing offers too good to be true (83%) and unexpected or unnecessary attachments (79%) are also signs of phishing messages.

Cybercrime and threats

More than three-quarters (78%) of online Canadians have *never* been a victim of an online scam where they lost money or data. That said, up to about one-quarter of Canadians have been a victim of other types of cyberattacks: 28% an email scam, 25% a malware attack, 24% a text scam, 20% a phishing scam, 15% a social media account hack, and 6% identity theft. While the incidence of cyberattacks is not high, two-thirds (65%) of online Canadians are worried about artificial intelligence (AI) related cybercrime, half (51%) are worried about falling victim to cybercrime in general, and one-quarter (24%) think it is likely they will be affected by at least one of several cyber threats over the next year: a cyber threat causing their personal information to be compromised (19%), loss of files or photos (8%), or financial loss (7%).

When asked what kinds of cyber threats they are *most* concerned about, 76% of online Canadians mentioned identity theft. Following identity theft, about six in 10 are most concerned about financial loss (63%) and viruses, spyware or malware (59%). Half (49%) are concerned about privacy violations, 44% about ransom attacks, 43% about personal data loss, and 39% about loss of information or files. Canadians are less likely to be concerned about phishing scams—35% said this is the type of threat they are most concerned about. Lower levels of concern may reflect online Canadians' confidence in their ability to identify a phishing message or a malicious link. Almost three-quarters (73%) are confident they can identify phishing threats.

Focusing on ransom attacks, 2% have been a victim of a ransomware attack, 4% think it is likely over the next year that they will be affected by an attack where their data will be held for ransom, and 24% think they are vulnerable to a ransomware attack. If ever a victim of a ransomware attack, the majority of online Canadians would reset their passwords (56%), take a photo of the ransomware message (54%), and report it to local police (52%).

The majority of online Canadians reported being somewhat (44%) or well (27%) prepared to face cyber threats. One-quarter (26%) said they feel unprepared. Among those feeling unprepared for a cyber threat, two main reasons were offered: futility (protecting themselves online is not possible) and lack of knowledge (not knowing where to obtain this information, not knowing the different threats, and not having straightforward information available).

Communications and the Get Cyber Safe campaign

Seven in 10 (70%) online Canadians feel confident that they could protect themselves online as long as they have trustworthy information on the steps to take. Almost two-thirds (63%) feel confident that they know how to find practical information to protect themselves online and exactly half (50%) feel they have enough information on how to take steps to protect against cyber threats.

Sixty-one percent of online Canadians would prefer to get information to protect themselves from cyber threats via websites. In addition to websites, four in 10 expressed a preference for check lists on what to do (41%) and instructional videos (41%). About one-third (35%) would be interested in fact sheets or infographics.

Very few (4%) have heard of the Get Cyber Safe campaign. Of the one in ten (11%) who were aware of the campaign with prompting, just over one-third (36%) read about it on social media. Approximately one-quarter saw a segment on the news or in the newspaper (27%), heard about it on a radio show or podcast (25%), or saw an online video (25%). Fewer visited the GetCyberSafe.ca website (16%) or heard about the campaign from someone else (8%).

Businesses and cyber security

More than three-quarters of business owners and managers or supervisors (78%) said their company has taken some steps to protect itself against cyber threats. Half or more of those surveyed reported that their business requires password protection on all devices (57%), keeps security software up to date on all machines (55%), and uses a password or user authentication for wireless and remote access (51%).

When it comes to protecting their company against cyber threats, about four in 10 said that their organization would benefit from guidelines for reacting to a cyberattack (44%), from a list of the types of threats that exist and clues to look out for (42%), or from steps to protect mobile devices in a public setting (38%).

When thinking about the daily operations of their company, nearly one-quarter of business respondents are concerned about work disruptions (23%) and almost as many are concerned about damage to the organization’s reputation (22%) or financial loss (22%). Sixteen percent said they are concerned about their company’s data being held for ransom.

Six in 10 companies are at least moderately prepared to defend against ransomware attacks. The measures implemented by at least one-third of companies to safeguard against this type of attack include using anti-virus software (52%), keeping operating systems, software, and apps updated (50%), using MFA (46%), backing up files (46%), and storing back-ups offline (36%). Despite being somewhat prepared, just over half of business owners and managers anticipate that it would take some effort (38%) or would be difficult (17%) to recover from a ransomware attack.

Parents and cyber security

As mentioned, this survey included an oversample of parents. Parents tended to differ from online Canadians who do not have children in terms of self-assessed knowledge of online security and the role they play in supporting others online. Parents were more likely to describe themselves as being connected to the internet all the time, having an advanced level of online security knowledge, and being the person their family members rely on for help with online security.

Despite their knowledge, parents were less likely to report taking precautions to protect their online accounts, installing the latest software or application updates, and using a unique password for each account. That said, when it comes to avoiding unsafe websites and phishing messages, parents were more likely to check for a website trust seal and analyse the overall look of the website, as well as be aware that offers too good to be true, unexpected attachments, and unprofessional graphic design are signs of phishing messages. Not surprisingly, parents were also more confident in their ability to identify a phishing message or a malicious link and less likely to be worried about AI-related cybercrime.

Concluding observations

In general, a large majority of Canadians take precautions to keep themselves safe online, with most regularly installing updates and using multi-factor authentication, and many using unique passwords for important online accounts most of the time, as well as complex passwords. The following are offered as concluding observations:

- *A sizable minority of online Canadians continue to use practices that could make them vulnerable to cybercrimes.* In recent years, there has been a steady decline in the proportion of Canadians using the same password for multiple accounts and an increase in the use of longer passwords and password managers. That said, almost one-quarter of online Canadians rarely use unique passwords, with many attributing this to their perception that unique passwords are difficult to remember, while roughly a third allow their web browser or an app to store their passwords and/or use the same password for multiple accounts. While storing passwords in browsers and apps and reusing the same password increases ease of use for the account holder, it does so at the expense of security. Browsers and apps are vulnerable to security attacks, and one compromised password could put many online accounts at risk at the same time.
- *While there is room for improvement vis-à-vis password management, online Canadians appear quite adept at identifying phishing messages and validating the legitimacy of websites.* Indeed, this could be the result of the increasing volume of spam messages reaching Canadians, but the outcome is online users who are able to identify risk. The vast majority of Canadians recognize commons signs of phishing messages and many routinely scrutinize the overall look of a website, check the "https" and the padlock symbol, and/or conduct research to confirm the legitimacy of a website.
- *Fear is a motivator: online Canadians' concern about cybercrime outweighs the probability that they will be a victim.* Victimization rates were low with most Canadians saying they have *never* been a victim of an online scam where money or personal information was lost. In contrast, two-thirds said they are concerned about AI-related cybercrime, and half worry about cybercrime in general, with many thinking they may be affected by at least one cyber threat over the next year--something unlikely to occur based on reported instances.

- *The Get Cyber Safe Campaign is well-suited to online Canadians' information preferences, but awareness of the campaign remains low***.** When it comes to information needs, online Canadians primarily look for information on how to protect themselves online via websites, with a large minority preferring checklists or instructional videos, as well as fact sheets or infographics. These formats lend themselves well to digital information campaigns, like Get Cyber Safe. That said, awareness of the campaign continues to be low, suggesting a need for increased publicity and/or branding of Get Cyber Safe as a one-stop Canadian information source on cyber security. Additional campaign content that could be of value to Canadians is an instructional video or checklist on what to do in the event of a cybercrime. While the majority of cybercrime victims reported the incident, more than one in 10 did not do so and one of the top reasons was not knowing what to do (who to report it to or how to do so).
- *Several sub-groups of online Canadians are more vulnerable than others when it comes to cyber safety —specifically, women, Canadians aged 65+, and Canadians aged 18 to 34.*
    - When it comes to keeping themselves safe online, women were more likely to feel unprepared to face a cyber threat, rely on others for help, and find most information on how to be secure online is confusing. In addition, they reported online practices that could leave their accounts and devices at risk of compromise. Women were less likely to know how to install the latest software and app updates and more likely to only install an update after clicking "remind me later". In addition, they are more likely to rarely use unique passwords, to keep their passwords simple, to reuse passwords, and to allow browsers or apps to store their passwords. The findings suggest a need for clear, concise information products on securing devices and online accounts to help keep this population safe online and prepared for cyber threats.
    - While many Canadians aged 65+ are taking steps to keep their accounts and devices secure, they are more likely than younger Canadians to require support for basic computing tasks, such as creating online accounts, installing the latest software, and backing up data. In addition, they are less likely than younger Canadians to know the common signs of phishing and to take steps to verify the legitimacy of a website and they are more likely to *not* know if they are vulnerable to a ransomware attack. Based on the research findings, online Canadians aged 65+ may benefit from checklists on how to identify cyber risks and what steps to take to protect themselves and secure their information.
    - Canadians under 35 exhibited several points of vulnerability in their online behaviour. They were less likely than older Canadians to always install the latest updates and more likely to click 'remind me later' a few times before installing the updates or to install the updates only when away from, or not using, their device. In addition, they were more likely than older Canadians to rarely use unique passwords for important online accounts and they were the most likely of all age groups to allow their browser or apps to store their passwords. Reminders of the importance of using complex passwords and keeping devices and apps up to date could be valuable for this age group, especially given they are less likely to see themselves falling victim to a cybercrime or being affected by a cyber threat in general.

Notes to reader

- Detailed findings are presented in the sections that follow. Results are presented in the main portion of the narrative and are typically supported by a graphic or tabular presentation of results.
- All results are expressed as percentages, unless otherwise noted. Throughout the report, percentages may not always add to 100 due to rounding and/or multiple responses being offered by respondents.
- At times, the number of respondents changes in the report because questions were asked of sub-samples of the survey population. Accordingly, readers should be aware of this and exercise caution when interpreting results based on smaller numbers of respondents.
- Subgroup differences are identified in the report, typically following the topline results.
  - Where subgroup differences are not discussed for certain questions, it can be assumed that there were no significant differences between the subgroups of respondents.
  - When reporting subgroup differences, if one or more categories in a subgroup is not mentioned in a discussion of differences (for example, if two out of three age groups are compared), it can be assumed that significant differences were found only among the categories reported.
  - Only subgroup differences that are statistically significant at the 95% confidence level, pertain to a subgroup sample size of more than n=30 are, or are part of a pattern or trend are discussed in the report.
- Where relevant, results are compared to similar surveys conducted in 2018, 2020 and 2022.
- The survey questionnaire is appended to the report.

Contract value

The contract value was $81,085.41 (including applicable taxes)

Statement of political neutrality

I hereby certify as a Senior Officer of Phoenix Strategic Perspectives that the deliverables fully comply with the Government of Canada political neutrality requirements outlined in the *Communications Policy* of the Government of Canada and Procedures for Planning and Contracting Public Opinion Research. Specifically, the deliverables do not contain any reference to electoral voting intentions, political party preferences, standings with the electorate, or ratings of the performance of a political party or its leader.

aWoods

Alethea Woods
President
Phoenix Strategic Perspectives Inc.

Survey Findings

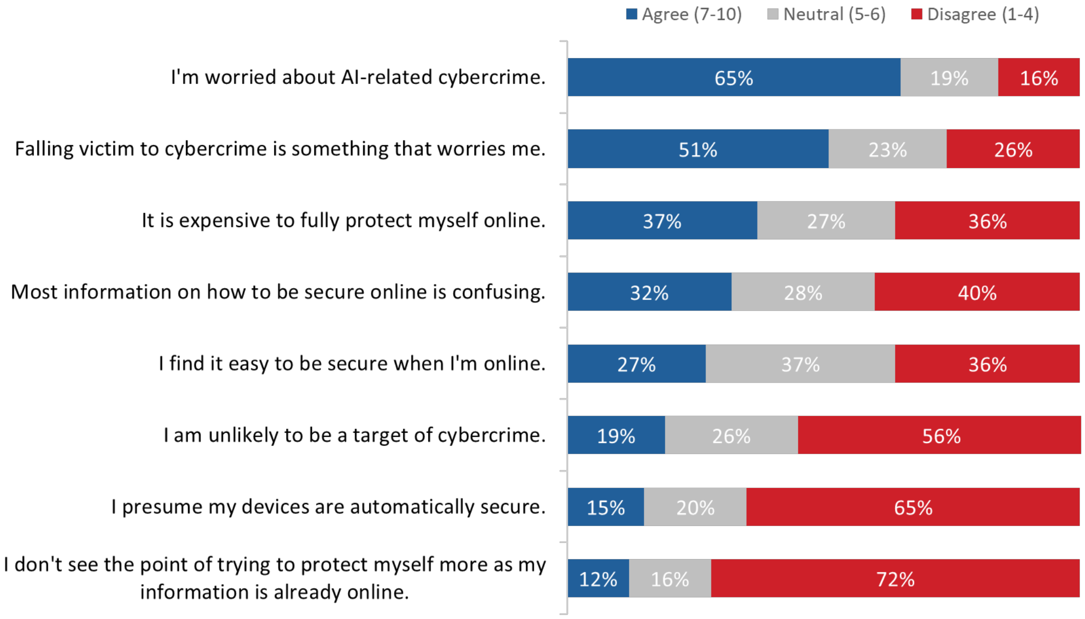
Views and attitudes towards cyber security

Majority of Canadians are worried about AI and cybercrime.

Respondents were asked to rate their level of agreement or disagreement with eight statements about cyber security concerns using a 10-point scale, where '1' is strongly disagree and '10' is strongly agree. In response, two-thirds (65%) of online Canadians agreed that they are worried about artificial intelligence (AI) related cybercrime (scores of 7 to 10 on the 10-point scale) and half (51%) are worried about falling victim to cybercrime in general. In addition, many consider themselves a likely target for cybercrime (56% disagreed with the statement *I am unlikely to be a target of cybercrime*).

When it comes to protecting themselves online, Canadians offered mixed assessments of the following: whether it's expensive to fully protect themselves online (37% agree, 27% neutral, and 36% disagree), whether information on how to be secure online is confusing (32% agree, 28% neutral, and 40% disagree), and whether it's easy to be secure when online (27% agree, 37% neutral, and 36% disagree). Relatively few presume their devices are automatically secure (15%) and do not see a point in trying to protect their information as it is already online (12%).

Figure 1: Attitudes toward online security



QCS1a-k. How much do you agree with the following statements about online security? Base: n=2,222; all respondents.

Notable subgroup differences include the following:

- As age increases, so does concern about AI being used for cybercrime, concern about falling victim to a cybercrime, and confusion about online security information. Those 18 to 34 were more likely than older Canadians to feel it is unlikely that they will be a target of cybercrime and to find it easy to be secure online.

- Gender differences were apparent. Women were more likely than men to be concerned about AI being used from cybercrime, to find that protecting themselves online is expensive, and to be confused by online security information. In contrast, men were more likely than women to feel it is easy to be secure online.
- As household income increased, the likelihood of agreeing that it is expensive to fully protect oneself online decreased.
- Residents of Quebec were more likely to doubt they will be targets of cybercrime compared to those who reside in Ontario.
- Those who are always online and those who rated their online security knowledge as advanced were more likely to find it easy to be secure when online and more apt to disagree with the premise that most information on how to be secure online is confusing. Canadians with advanced knowledge of online security were more likely to *not* worry about falling victim to cybercrime. Those with a basic or novice level of knowledge were more likely to think it is expensive to fully protect themselves online, to assume their devices are secure, to think it is pointless to try to be safe online, to find information about online security confusing, and to worry about becoming a victim of a cybercrime.

Relatively few rely on others to be secure online, but many turn to others for cyber security advice.

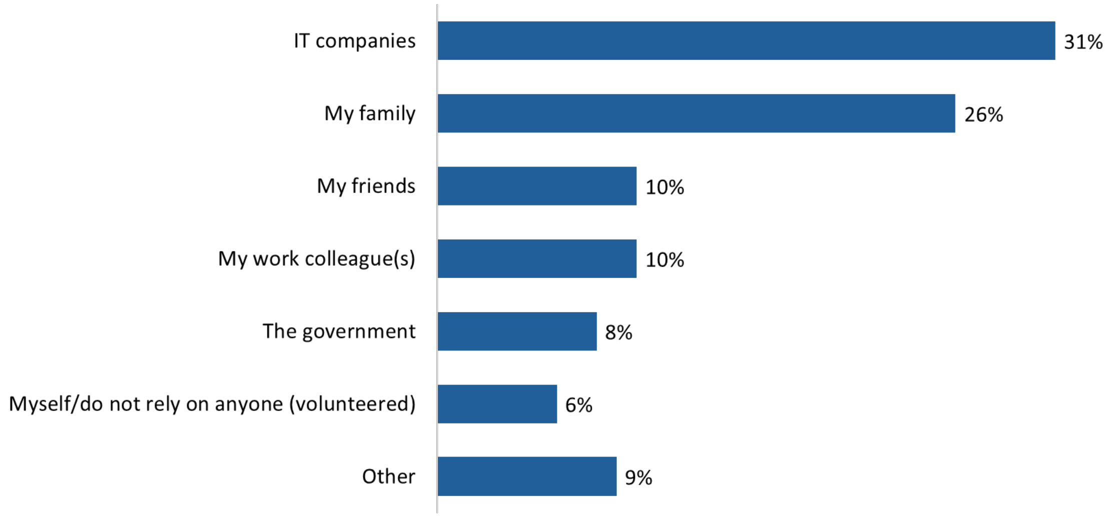
Slightly more than one in 10 (15%) online Canadians indicated that they rely on others, such as family or colleagues, to keep them secure online.[1] Respondents were asked to agree or disagree using a 10-point scale with the statement, *I rely on others (e.g. my family, my colleagues) to keep me secure online*.

When it comes to cyber security help or advice more generally, just over half of online Canadians rely on IT companies (31%) or their family (26%). Two in 10 rely on friends (10%) or work colleagues (10%), while fewer than one in 10 (8%) rely on government, such as government websites. Six percent volunteered that they manage their own cyber security and do not rely on anyone for help or advice.

Nine percent mentioned other sources of help or advice. The types of responses in the 'other' category included security experts, security apps, social media (YouTube, Reddit), radio and television programming, anti-virus software, Google, the internet (not specified) and various online resources, among other things.

[1] QCS1m. How much do you agree with the following statements about online security? Base: n=2,222; all respondents.

Figure 2: Source of help or advice on cyber security



QCS2. Who do you rely on most for cyber security help or advice? Base: n=2,222; all respondents.

Those aged 65 and older were the most likely to report that they rely on their family most for cyber security help or advice, while those aged 18 to 34 were the most likely to rely on friends for such advice and the least likely to turn to IT companies.

When looking at generational differences, Gen Z were the most likely to report that they rely on their friends, while Millennials and Gen X were more likely than Gen Z and Baby Boomers to reply on work colleagues. Gen X and Baby Boomers were more apt than Millennials and Gen Z to rely most on IT companies for cyber security help or advice.

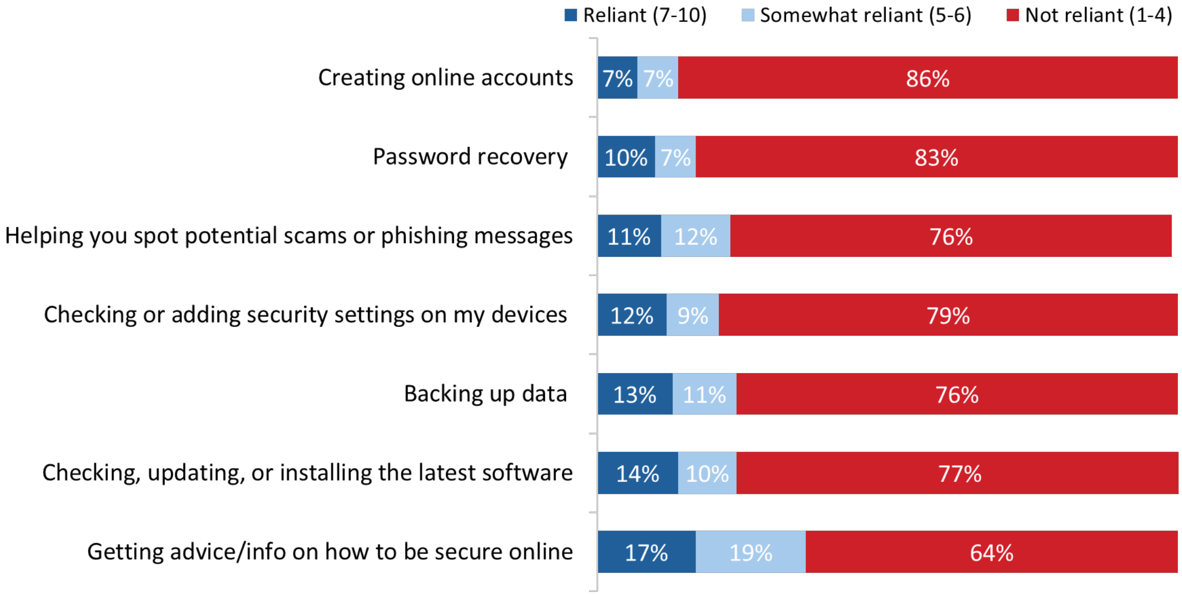
Those with a basic or beginner level of knowledge about online security were more likely to say they rely on their family.

More than half of online Canadians are not reliant on others for cyber security support.

Respondents were asked how much they rely on other people for help to perform different computing and cyber security tasks using a 10-point scale, where ‘1’ is not at all reliant and ‘10’ is fully reliant. More than half of online Canadians said they do not rely on other people to perform computing and cyber security tasks (scores of 1 to 4 on a 10-point scale). The rest are at least somewhat reliant on others (scores of 5 to 10).

In terms of support, 36% are at least somewhat reliant on others for advice and information on how to be secure online, 24% for checking, updating, or installing software updates, 24% for backing up their data, 23% for spotting potential scams or phishing attempts, 21% for checking or adding security features to their device(s), 17% for password recovery, and 14% for help creating online accounts.

Figure 3: Reliance on others for help with cyber security



QCS3. How much do you rely on other people for help (e.g. family, friends or colleagues) to perform the following things?
Base: n=2,222; all respondents.

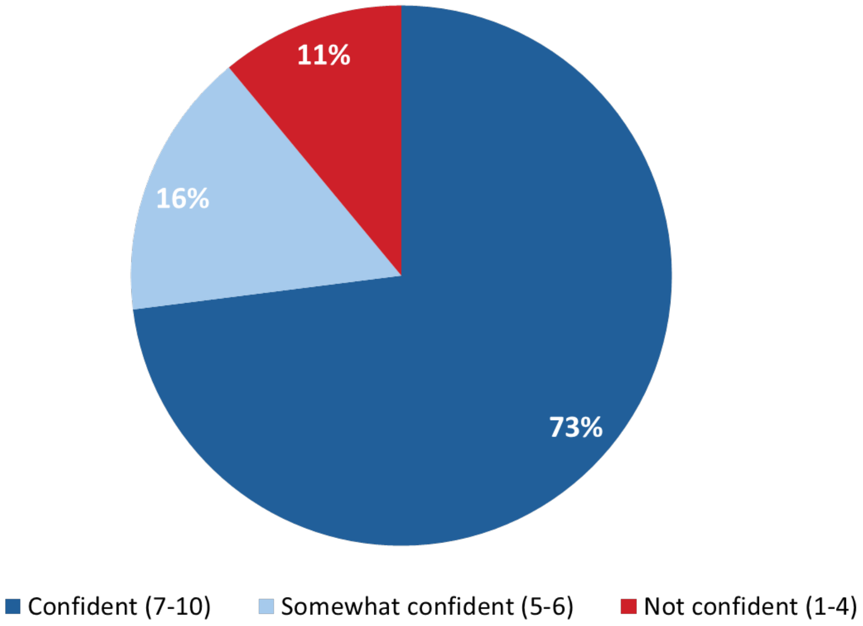
Notable subgroup differences include the following:

- Differences based on region tended to set Quebec, followed by Atlantic Canada, apart from the rest of Canada. Specifically, residents of Quebec were the most likely to be reliant on other people for advice and information on how to be secure online, and together with those from Atlantic Canada, they were more likely to rely on others for checking or adding security features on their devices, checking, updating, or installing the latest software, and password recovery.
- As age increased, so too did the likelihood of being reliant on others for support performing all of these cyber security tasks. The same trend was generally observed among the different generations: Baby Boomers and the Silent generation were typically more likely than Gen Z, Millennials and Gen X to rely on others for support in this area.
- Similarly, women were more likely than men to report being reliant on others for help with all these items.
- In general, those who are always connected and those who have an advanced level of knowledge when it comes to online security were more likely to *not* be reliant on anyone to perform these tasks.

Most Canadians are confident they can spot a scam message.

Three in four (73%) online Canadians feel confident in their ability to identify a phishing message or a malicious link. An additional 16% feel somewhat confident. In contrast, one in 10 (11%) are not confident they would be able to identify a phishing message or malicious link.

Figure 4: Confidence in identifying phishing messages or malicious links



QCS5. How confident are you in your ability to identify a phishing message or a malicious link? Base: n=2,222; all respondents.

Notable subgroup differences include the following:

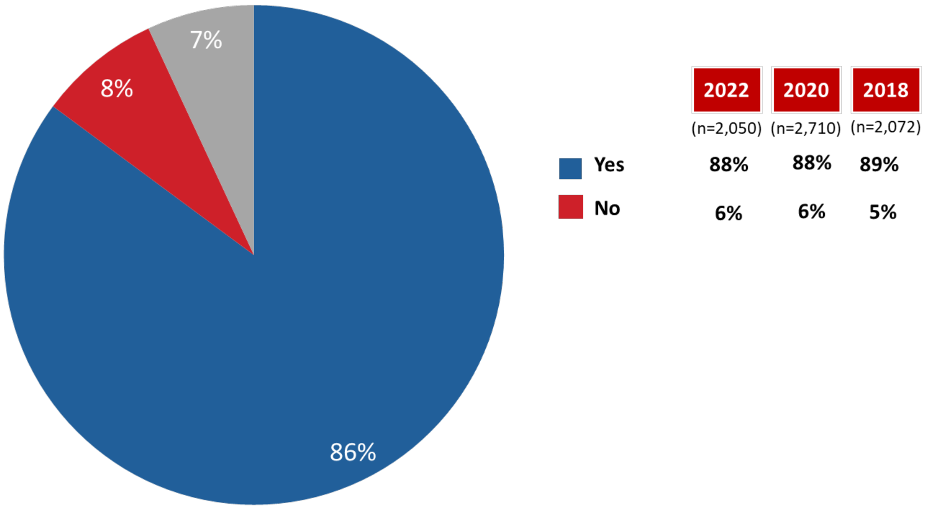
- Respondents from Manitoba were the most likely to be confident of their ability to identify a phishing message or malicious link.
- As age increased, confidence in spotting these messages or links decreased. Gen Z, Millennials and Gen X were more confident than Baby Boomers and the Silent generation.
- More men than women reported being confident they can identify a phishing message or malicious link.
- Confidence in one's ability to spot a phishing message or malicious link increased with household income.
- Those who are always connected and those who have an advanced level of knowledge when it comes to online security were more likely to be confident in their ability to identify a phishing message.

Cyber security practices of online Canadians

More than eight in 10 Canadians take precautions to protect their online accounts.

More than eight in 10 online Canadians (86%) reported that they take precautions to protect their online accounts, social media accounts, devices, and networks. Very few (8%) do not. The proportion of online Canadians taking precautions has changed very little since the baseline survey was conducted in 2018.

Figure 5: Take actions to protect online accounts



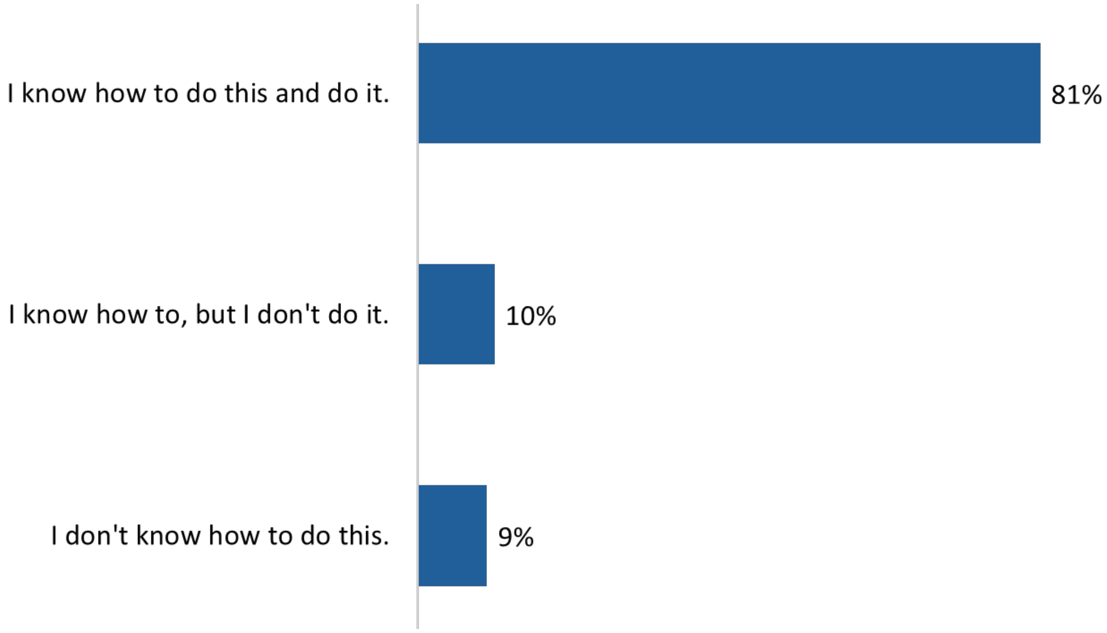
QBEH1. Do you take precautions to protect your online accounts, social media accounts, devices, or networks? Base: n=2,222; all respondents.

The likelihood of taking precautions to protect their online accounts, social media accounts, devices, and networks was higher among residents of Manitoba and Saskatchewan compared to residents of Quebec and Alberta; those aged 45+ compared to 18- to 34-year-olds; Baby Boomers; university graduates; and those earning more than $40,000 per year. Parents were less likely than online Canadians who do not have children under 18 to report taking precautions to protect their online accounts, social media accounts, devices, or networks.

Most online Canadians know how to install software and app updates and do so.

In addition to taking precautions to protect their online accounts, eight in 10 (81%) Canadians know how to install the latest software and app updates across their devices and report doing so. An additional 10% know how to install updates, but do not do so. Very few (9%) said they do not know how to install the latest software and app updates across their devices.

Figure 6: Knowledge of installing latest software or app update



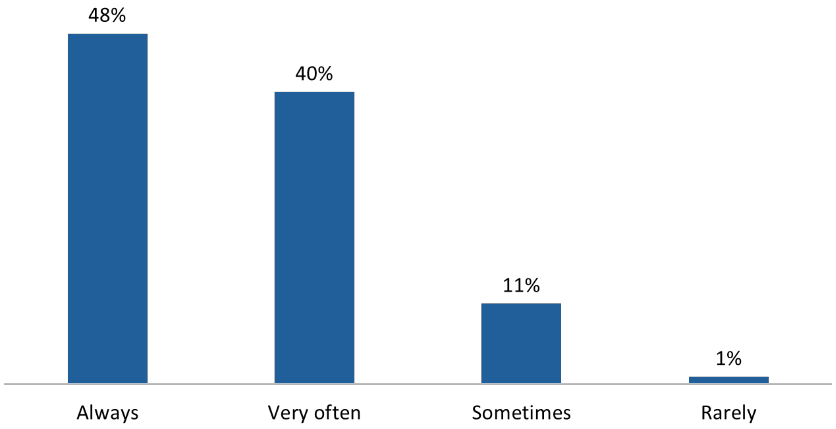
QBEH2. Do you know how to install the latest software and app updates across your devices (e.g. computer and mobile phone)? Base: n=2,222; all respondents.

The following groups of online Canadians were *less* likely to know how to install updates and to do so: those aged 65 and older, women, those from households with an annual income of under $40,000, those with a secondary school or college education, those who use the internet a few times a week or less, and those who have a basic or beginner level of online security knowledge. Gen Z were the most likely to say they know how to install the latest software and app updates, but do not actually do so.

The vast majority regularly install the latest software or application updates.

Among those who know how to install the latest software and app updates (n=1,813), the vast majority (88%) do so regularly, including almost half (48%) who do so 'always' when notified that updates are available. Relatively few (11%) 'sometimes' install updates to their devices, and almost no-one (1%) reported doing so 'rarely'.

Figure 7: Frequency of installing latest software or app updates



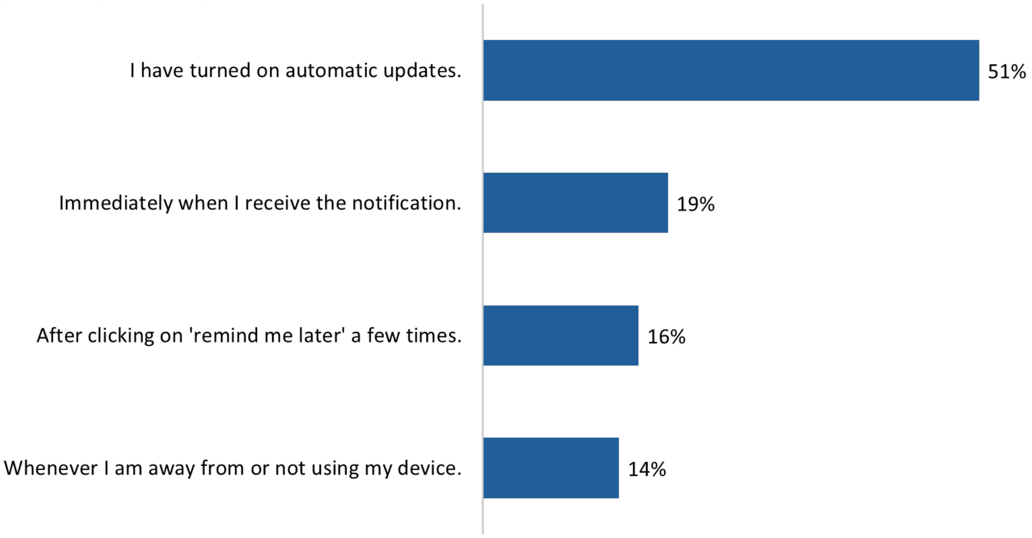
QBEH3. How often do you install the latest software or application updates to your devices when notified that they are available? Base: n=1,813; respondents who know how to install the latest software and app updates.

The likelihood of 'always' installing the latest software or application updates when notified generally increased with age and annual household income and was highest among those with advanced online security knowledge. Gen Z were the least likely to always install updates. In addition, parents were less likely than non-parents to always install updates when they receive a notification.

Seven in 10 online Canadians install updates immediately.

Among those who 'often' install software updates on their devices (n=1,800), seven in 10 (70%) install these updates immediately. Specifically, 51% have turned on automatic updates and 19% install updates immediately upon receipt of the notification. Among the rest, 16% install the updates only after clicking on 'remind me later' a few times and 14% do so only when they are away from, or not using, their device.

Figure 8: Typical timing for installing software updates



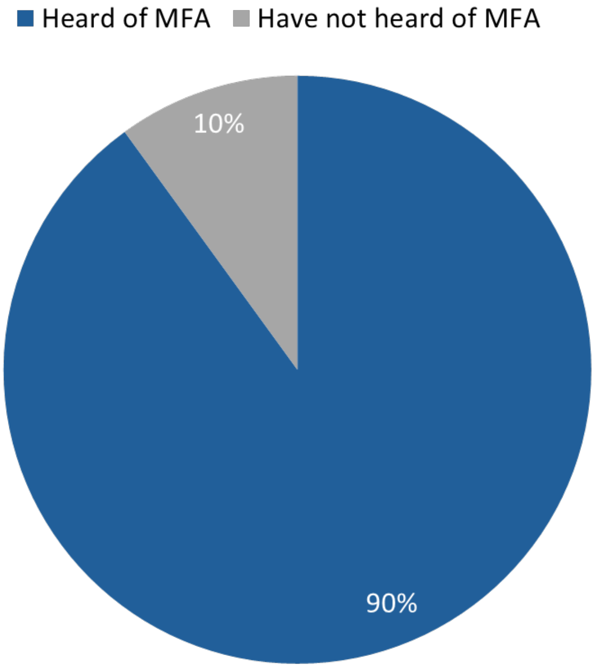
QBEH4. When do you typically install software updates on your devices? Base: n=1,800; respondents who install updates often.

Differences in behaviour based on age were evident. Specifically, as age increases, so too does the likelihood that online Canadians have turned on automatic updates. Conversely, 18- to 34-year-olds were more likely than those aged 35+ to report that they install updates after using the 'remind me later' feature a few times or whenever they are away from, or not using, their device. Gen Z was the most likely to say they install updates only after clicking 'remind me later' a few times.

Nine in 10 online Canadians know about MFA and use it regularly.

Nine in 10 (90%) surveyed Canadians have heard of multi-factor authentication (MFA), also known as Two-Factor or Two-Step Verification.

Figure 9: Awareness of MFA

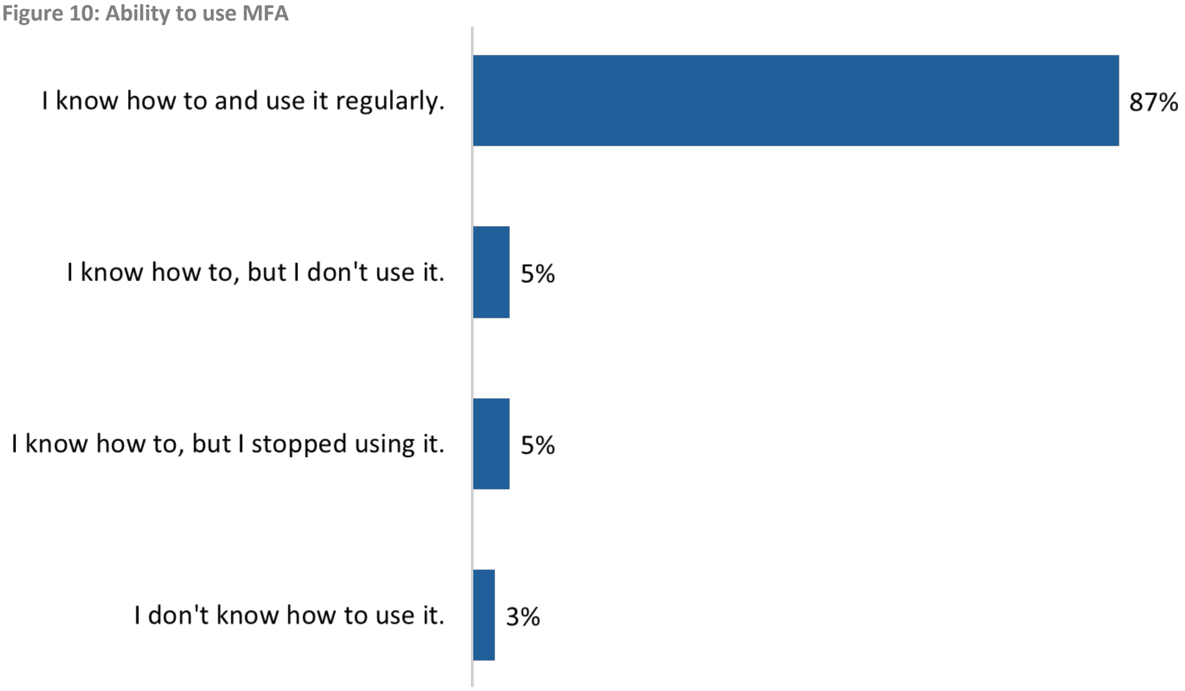


QBEH6. Have you ever heard of multi-factor authentication (MFA)? Also known as Two-Factor or Two-Step Verification. Base: n=2,222; all respondents.

Residents of Quebec were the most likely to report having *never* heard of MFA. Awareness of MFA increased with education and annual household income, and it was higher among younger Canadians and parents. The likelihood of *not* being aware of MFA was higher among those with a basic or beginner level of online security knowledge.

Of those aware of MFA (n=1,987), most (87%) know how to use it and do so regularly. An additional 10% know how to use MFA but do not use it (5%) or have stopped using it (5%). Very few (3%) reported not knowing how to use MFA.

Figure 10: Ability to use MFA



QBEH7. You mentioned you have heard about multi-factor authentication (MFA). Do you know how to use it? Base: n=1,987; respondents who have heard of MFA.

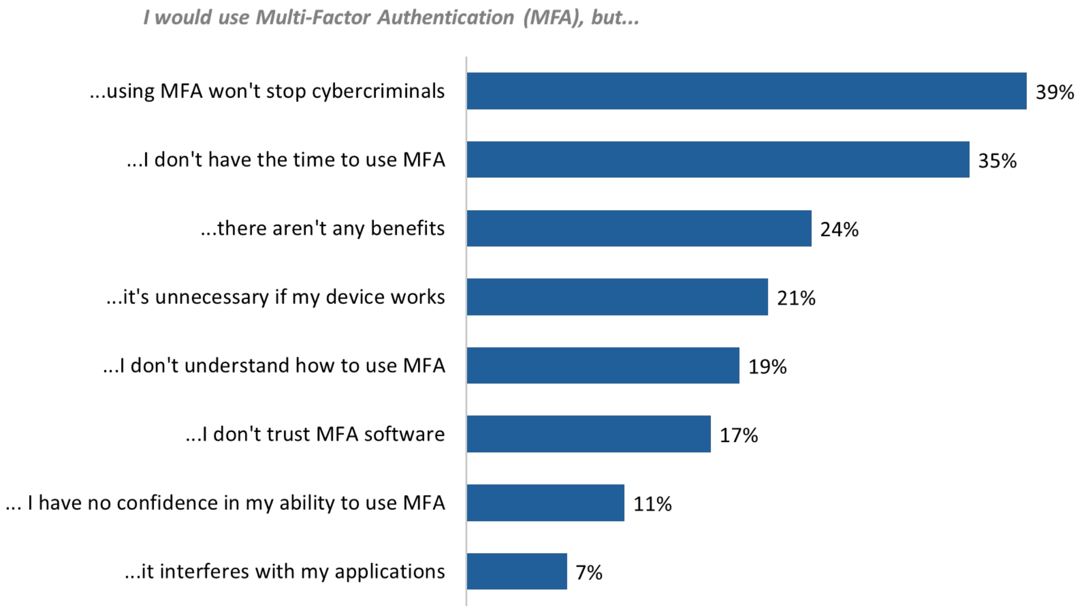
Those aged 18 to 34 and aged 35 to 44 were more likely than those aged 65+ to report knowing how to use MFA and to use it regularly. In addition, as education and household income increased, so too did the likelihood of knowing how to use MFA and using it regularly. Canadians with advanced knowledge of online security were the most likely to know how to use MFA and to use it regularly.

Lack of utility and time are the top reasons for not regularly using MFA.

Those who do not use multi-factor authentication regularly (n=255) do not believe it will stop cybercriminals (39%) and do not have the time to use it (35%). One-quarter (24%) do not see any benefits to using multi-factor authentication, while two in 10 consider it unnecessary if their device works (21%) or do not understand how to use multi-factor authentication (19%). Beyond this, 17% do not trust multi-factor authentication software, 11% have no confidence in their ability to use it, and 7% think it interferes with their applications and worry it will ‘break’ their device.

Respondents were asked to rate their level of agreement or disagreement with various statements about MFA using a 10-point scale, where ‘1’ is strongly disagree and ‘10’ is strongly agree. Presented in the graph below are the percentage of respondents who agreed with each statement (scores of 7 to 10 on the scale).

Figure 11: Reasons for not using MFA on a regular basis



QBEH9a-j. Please rate your agreement with the following statements: "I would use Multi-Factor Authentication (MFA), but..." Base: n=255; respondents who do not use MFA regularly.

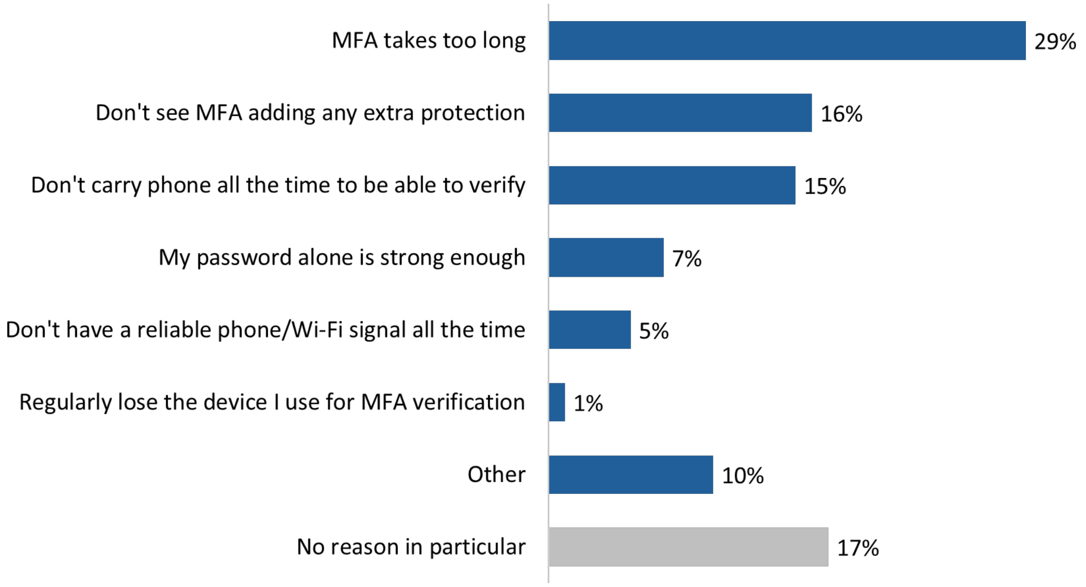
A variety of reasons were offered for not (or no longer) using MFA.

Those who do not, or no longer, use multi-factor authentication (n=194) attributed their lack of use to a number of reasons. The reason mentioned by the single largest proportion—29%—is that multi-factor authentication takes too long. Following this, 16% do not think multi-factor authentication adds any extra protection, and 15% do not carry their phone with them all the time, a requirement to use multi-factor authentication.

Reasons offered by smaller proportions included the perception that their password is strong enough (7%), not having a reliable phone or Wi-Fi signal all the time (5%), and regularly losing the device set up for multi-factor authentication (1%).

Close to two in 10 (17%) have no reason in particular for not using (or no longer using) multi-factor authentication.

Figure 12: Reasons for not using MFA



QBEH8. What is the main reason you don't use (or stopped using) multi-factor authentication (MFA)? Base: n=194; respondents who know how to use MFA but choose not to.

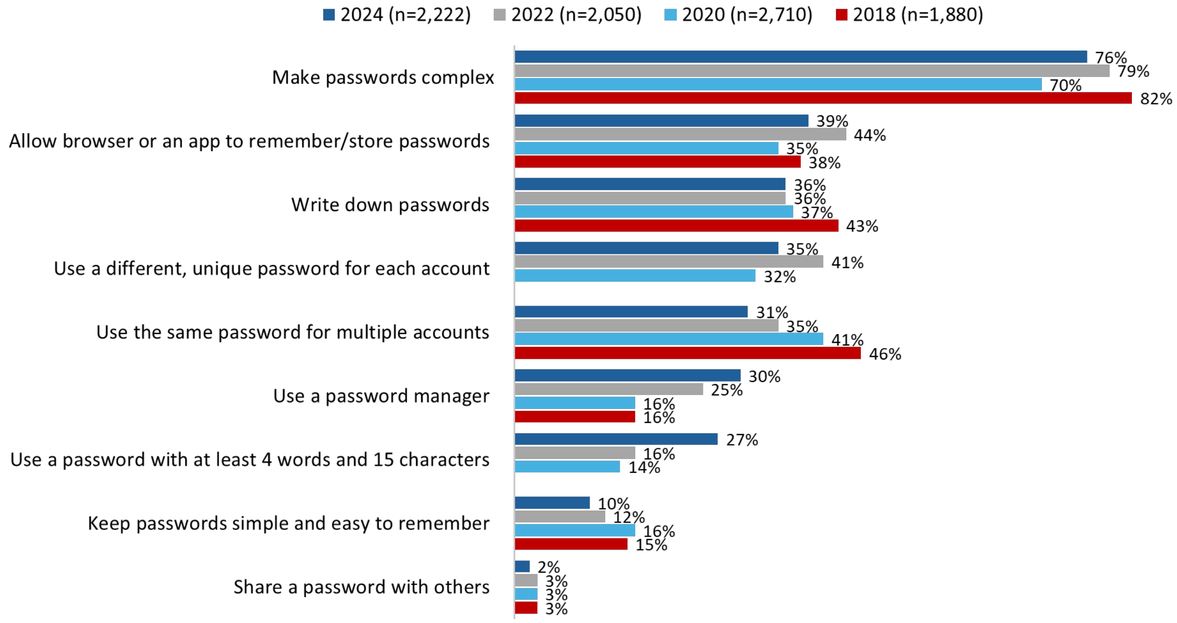
Three-quarters make their passwords complex.

When it comes to their passwords, just over three-quarters (76%) of online Canadians said they make their passwords complex with a combination of letters, numbers, and symbols. Following this, 35% (down from 41% in 2022) use a different, unique password for each account, 30% (up from 25% in 2022) use a password manager, and 27% (up from 16% in 2022) use a password with at least four to 15 characters.

Other respondents take actions that *could* put their accounts at risk: 39% (down from 44% in 2022) allow browsers or apps to 'remember' or auto-fill their passwords, 36% write down their passwords, 31% (down from 35% in 2022) use the same password for multiple accounts, 10% keep passwords simple and easy to remember, and 2% share their password.

Comparing year-over-year, making passwords complex continues to be reported by the greatest proportion of online Canadians. In addition, this year, fewer online Canadians are allowing browsers or apps to remember their passwords and use the same password for multiple accounts, while significantly more Canadians are using a password with at least four to 15 characters.

Figure 13: Actions taken regarding passwords



QBEH15. When it comes to your passwords, which of the following actions do you take? [multiple answers accepted] Base: all respondents; n=2,200. Don't know: 1%.

Differences based on age were pronounced and followed a clear pattern. Those aged 18 to 44 were more likely than older Canadians to allow their browser or app to remember or store their password, use a password manager, use the same password for multiple accounts, use a password with four to 15 characters, and make their passwords complex with a combination of letters, numbers, and symbols. Those aged 65+ were the *most* likely to report writing down their passwords.

Turning to gender, men were more likely than women to report using a password manager and unique passwords, while women were more likely to keep their passwords simple and easy to remember, use the same password for multiple accounts, write down their passwords, and allow browsers or apps to store their passwords.

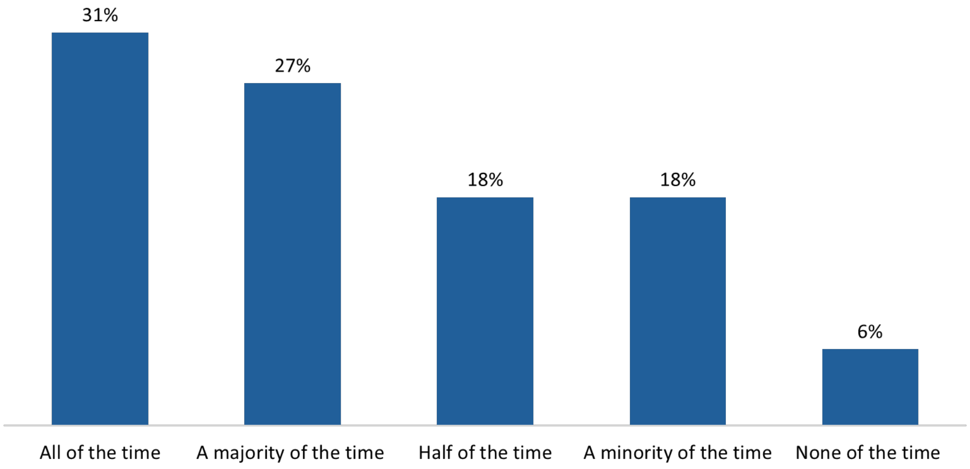
Other noteworthy subgroup differences include the following:

- The likelihood of using a password manager increased with household income.
- University graduates were more likely to use best practices for keeping passwords secure: complex passwords, passwords with four to 15 characters, unique passwords for each account, and password managers.
- Parents were more likely than those who do not have children under the age of 18 to use a password with four to 15 characters, but they were less likely than their counterparts to use a different password for each account.
- Use of a password manager was higher in Ontario compared to Atlantic Canada and Quebec.

Half of Canadians use unique passwords most of the time.

Half of online Canadians said they use unique passwords for their important online accounts 'all of the time' (31%) or a 'majority of time' (27%). In addition, one-third do so 'half of the time' (18%) or a 'minority of the time' (18%). Very few (6%) said they do not use unique passwords.

Figure 14: Use of unique passwords



QBEH17. How often do you use unique passwords for your important online accounts? Base: n=2,222; all respondents.

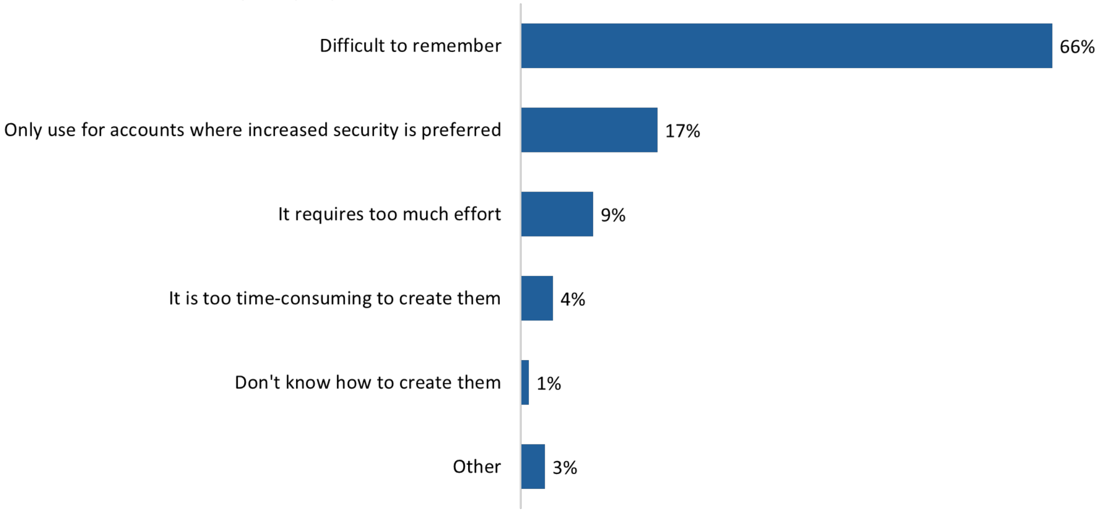
Those aged 45+ were more likely than online Canadians aged 18 to 34 to say they use unique passwords 'all of the time' or a 'majority of the time'. Gen Z was the generation most likely to use unique passwords for their important accounts 'half of the time'. Men were more likely to use unique passwords 'all of the time' compared to women. Online Canadians with up to a secondary school education were more likely to say they use unique passwords a 'minority of the time' for their important online accounts. Those with advanced knowledge of online security were more likely to use unique passwords 'all of the time'.

The length of passwords varied, with two-thirds reporting that they use between seven and eight characters (20%) or between nine and 11 characters (47%). Among the rest, one-third use longer passwords (26% use passwords that are 12 to 15 characters in length and 7% use passwords that are 16+ characters). To remember multiple passwords, approximately one-quarter each write them down in a notebook (23%) or use a password manager application, such as 1Password, LastPass, or iCloud keychain (24%). One in five (21%) said they remember their passwords without writing them down.

The main reason Canadians reuse passwords is to avoid having to remember them.

Two-thirds (66%) of those who rarely, if at all, use unique passwords for their online accounts (n=512) attributed this to the fact that they find it difficult to remember different passwords. Others said they do not use unique passwords because it requires too much effort (9%), is too time-consuming (4%), or they do not know how to (1%). Seventeen percent use unique passwords only for specific accounts where increased security is preferred.

Figure 15: Reasons for not using unique passwords

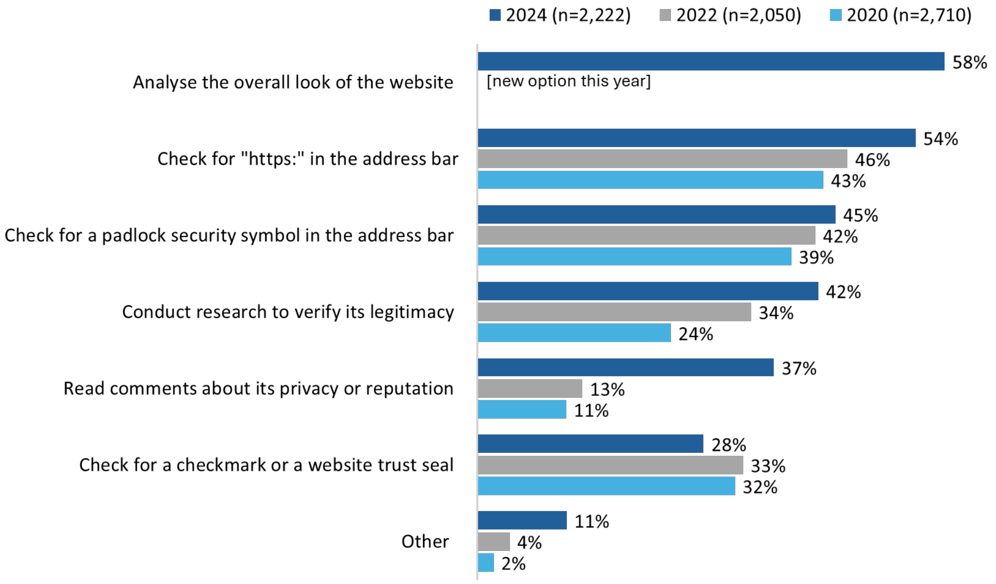


QBEH18. You mentioned that you rarely, if at all, use unique passwords for your online accounts. What is the main reason you don't do this? Base: n=512; respondents who do not create unique passwords.

Online Canadians use several strategies to verify a website.

To verify that a website is legitimate, just over half of online Canadians analyse the overall look of the website (58%) or check for “https” in the address bar (54%; up from 46% in 2022). Approximately four in 10 check for a padlock symbol in the website’s address bar (45%; up from 42% in 2022), conduct research to verify the legitimacy of the website (42%; up from 34% in 2022), or read comments about the website’s privacy or reputation (37%; up from 13% in 2022). Just over one-quarter check for a checkmark or website trust seal (28%; down from 33% in 2022).

Figure 16: Steps to verify website is secure



QBEH12. What steps do you take to verify that a WEBSITE is legitimate? [multiple answers accepted] Base: all respondents.

Canadians under the age of 65 were more likely than those aged 65+ to report taking all the steps listed to verify the legitimacy of a website. Gender differences were limited to two steps: men were more likely than women to conduct their own research to verify a webpage and to check for 'https'. Notable regional differences included the following: those in Quebec were the *most* likely to check for the padlock symbol and more likely than those in Atlantic Canada and British Columbia to check for 'https' in the address bar. Those with advanced knowledge of online security and those always connected to the internet were more likely to take all of these steps to verify the legitimacy of a website.

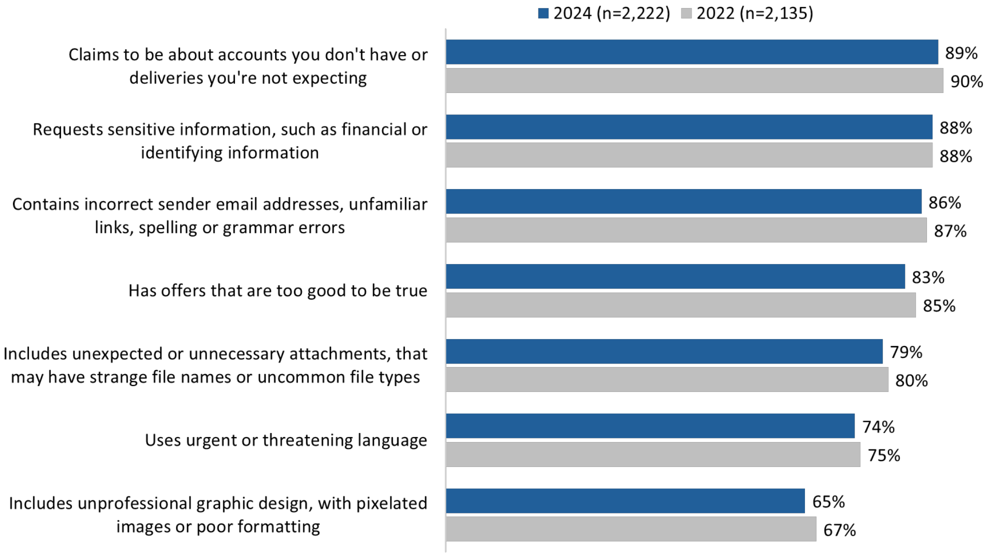
Comparing year-over-year, in general, more online Canadians report taking steps to verify websites. Specifically, the proportion conducting their own research has increased from 24% in 2020, to 34% in 2022, to 42% in 2024. Looking for comments on other websites to confirm reputation has increased significantly, from 11% and 13% in 2020 and 2022, to 37% in 2024. Looking for the padlock symbol has seen small increases year over year, from 39% in 2020, to 42% in 2022, to 45% in 2024. So too has the proportion checking for a 'https' protocol (from 43% in 2020, to 46% in 2022, to 54% in 2024).

Most online Canadians generally recognize the signs of phishing messages.

The vast majority of online Canadians recognize the signs of phishing messages, including claims about accounts they do not have or unexpected deliveries (89%), requests for sensitive information (88%), and messages containing incorrect email addresses, unfamiliar links, or spelling or grammar mistakes (86%). Almost as many recognize that messages containing offers too good to be true (83%) and unexpected or unnecessary attachments (79%) are also signs of phishing messages. Three-quarters (74%) recognize that the use of urgent or threatening language is indicative of phishing, while two-thirds (65%) said that messages using unprofessional graphic design are an indication of phishing.

Survey results are virtually identical to 2022.

Figure 17: Signs of phishing



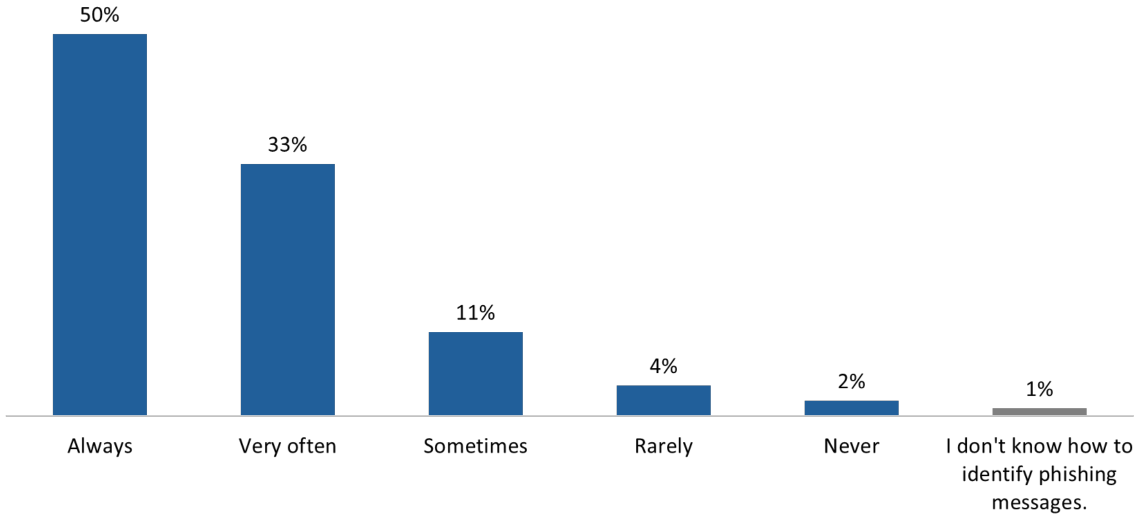
QBEH13. As far as you know, what are signs of phishing? [multiple answers accepted] Base: all respondents. Don't know: 2%.

Online Canadians under the age of 45 were more likely than older Canadians to point to all of these as potential signs of phishing. As education increased, so too did the likelihood of identifying these as signs of phishing. The opposite is the case when household income decreases—the likelihood of identifying these as signs of phishing decreased with annual household incomes and tended to be higher among those reporting to make under $40,000 a year. Parents were more likely than non-parents to point to offers being too good to be true, unexpected attachments, and unprofessional graphic design as signs of phishing. Those with advanced knowledge of online security and those always connected to the internet were more likely to be aware of many of these signs of phishing.

Most online Canadians frequently check messages for signs of phishing.

Most online Canadians 'always' (50%) or 'very often' (33%) check messages, including emails, texts, or social media, for signs of phishing before clicking any links or responding to them. An additional 11% check some of the time, while very few (6%) check messages 'rarely' or 'never'.

Figure 18: Frequency of checking for phishing messages



QBEH14. How often do you check messages (e.g. emails, texts, or social media) for signs of phishing before clicking any links or responding to them? Base: all respondents; n=2,222.

The following groups were more likely to report that they 'always' check messages for signs of phishing: residents of Ontario compared to Atlantic Canada and Quebec; men; Millennials; those with an annual household income of $100,000 to just under $150,000 compared to those earning under $100,000 annually; and university and college graduates. Those with advanced knowledge of online security and those always connected to the internet also were more likely to always check messages for signs of phishing.

Cybercrime and threats

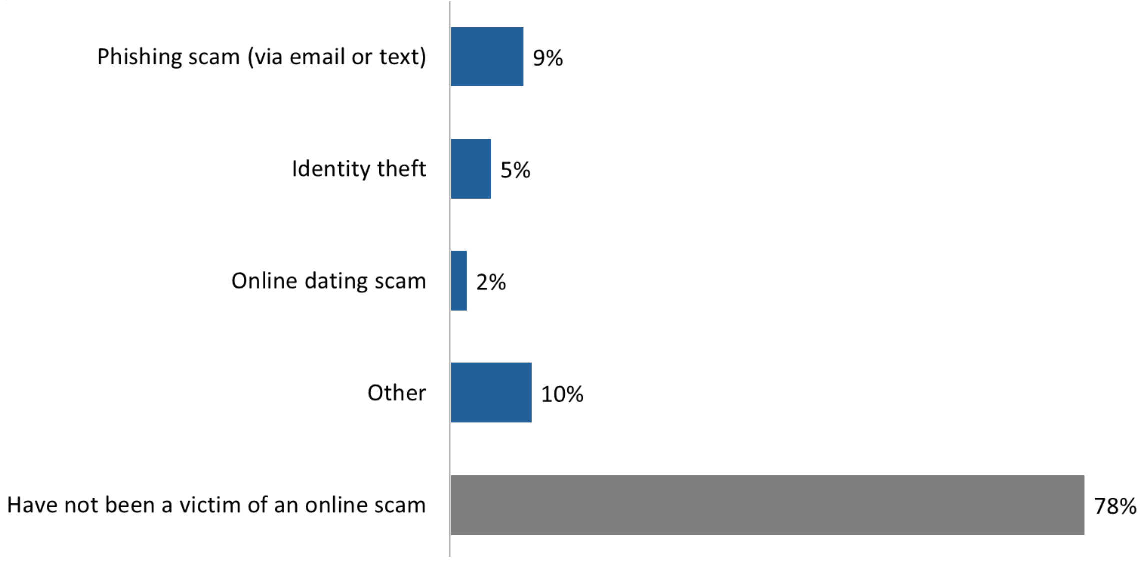
Most Canadians have never been a victim of online scams.

More than three-quarters (78%) of online Canadians said they have never been a victim of an online scam where they lost money or data. Relatively few have been a victim: 9% said they were the victim of a phishing scam, 5% have been the victim of identity theft, and 2% the victim of an online dating scam.

The following descriptions were available to respondents:

- "Phishing": Cybercriminals trick people into providing information or installing dangerous software in order to steal money or data from them. This is often done via fake emails that appear to be from trusted senders, which encourage people to click malicious links to fake websites, or to open malicious attachments.
- "Online dating scam": Scammers adopt a fake online identity to create an illusion of a romantic or close relationship to manipulate and/or steal from the victim. They often use highly emotive requests for money claiming they need emergency medical care, or to pay for transport costs to visit the victim if they are overseas.
- "Identity theft": Identity theft is when scammers access enough information about someone's identity (such as their name, date of birth, current or previous addresses) to obtain goods or services by deception, such as by opening a bank account or obtaining a credit card or loan.

Figure 19: Incidence of online scams



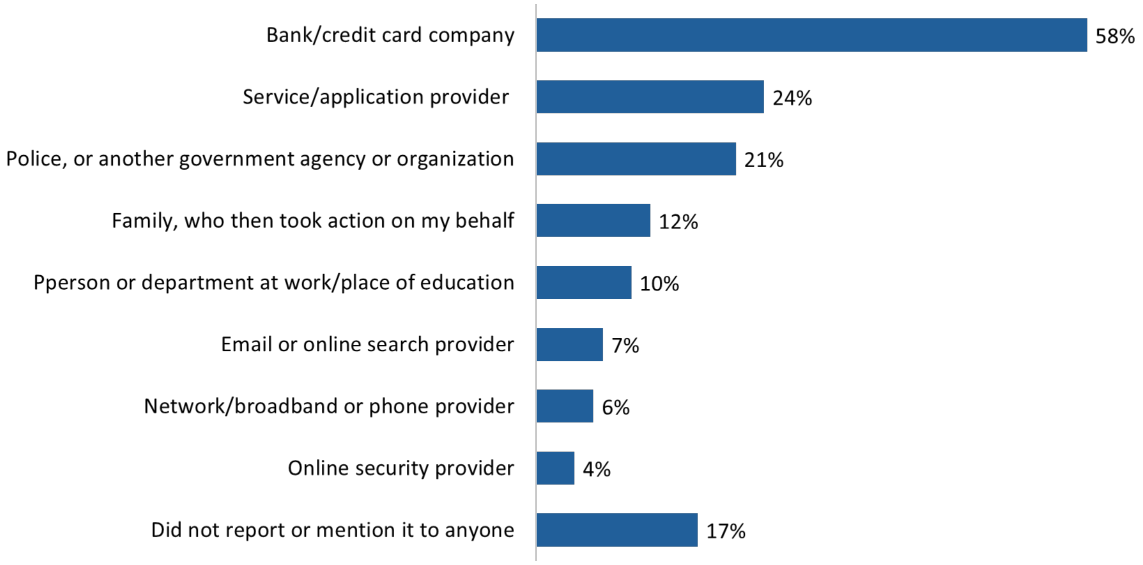
QCCE1. Have you ever personally been a victim of online scams where you have lost money or data? [multiple answers accepted] Base: n=2,222; all respondents.

The likelihood of being a victim of an online scam, either a phishing or online dating scam or identity theft, was higher among those from households with annual incomes of under $40,000 compared to those reporting an annual income of $100,000+.

Most victims of an online scam reported or mentioned it to someone.

More than eight in 10 (83%) of those who have been a victim of an online scam (n=193) reported or mentioned it to someone. The majority (58%) reported the scam to their bank or credit card company. Following this, 24% reported the scam to the service or application provider where they lost the money or data, and 21% reported it to the police or to another relevant government agency. Twelve percent told their family, who then took action on their behalf. The full range of actions can be found in figure 20.

Figure 20: Reporting on phishing scams



QCCE2. You mentioned that you have lost money or data through a phishing scam. Did you report this to anyone? [multiple answer accepted] Base: n=193; respondents who were victims of a phishing scam.

Those who were a victim of a phishing scam and reported it (n=161)[2] did so for two main reasons: to ensure it does not happen to them again or to other people (47%) or to get their money back (41%).

Among those who did not report the phishing scam (n=32)[3], reasons included uncertainty about who to report it to or how to do so, the perception that it would be pointless to report because no action would be taken, feelings of shame, and the view that amount of the loss was not significant enough, among others.

One-quarter of online Canadians think it's likely they will be affected by a cyber threat.

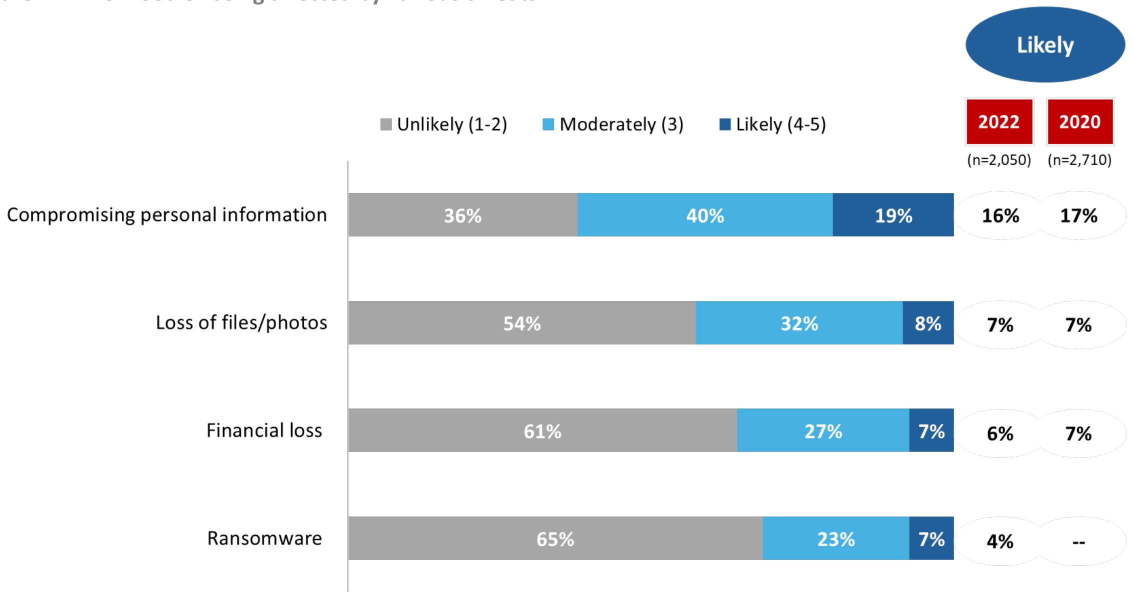
Up from 8% in 2022, 24% of online Canadians think it is likely they will be affected by at least one of four cyber threats over the next year. In terms of the specific threats, two in 10 (19%; up from 16% in 2022) think it is likely that they will be affected by a cyber threat causing their personal information to be compromised. Consistent with results from previous years, relatively few believe

[2] QCCE3. What is the main reason you reported a phishing scam? If you have lost money/data more than once, please think about the most recent time this happened. Base: respondents who reported phishing scam.

[3] QCCE4. What is the main reason you didn't report the phishing scam?

they will experience a threat that results in the loss of files or photos (8%), financial loss (7%), or where their data will be held for ransom (4%).

Figure 21: Likelihood of being affected by various threats



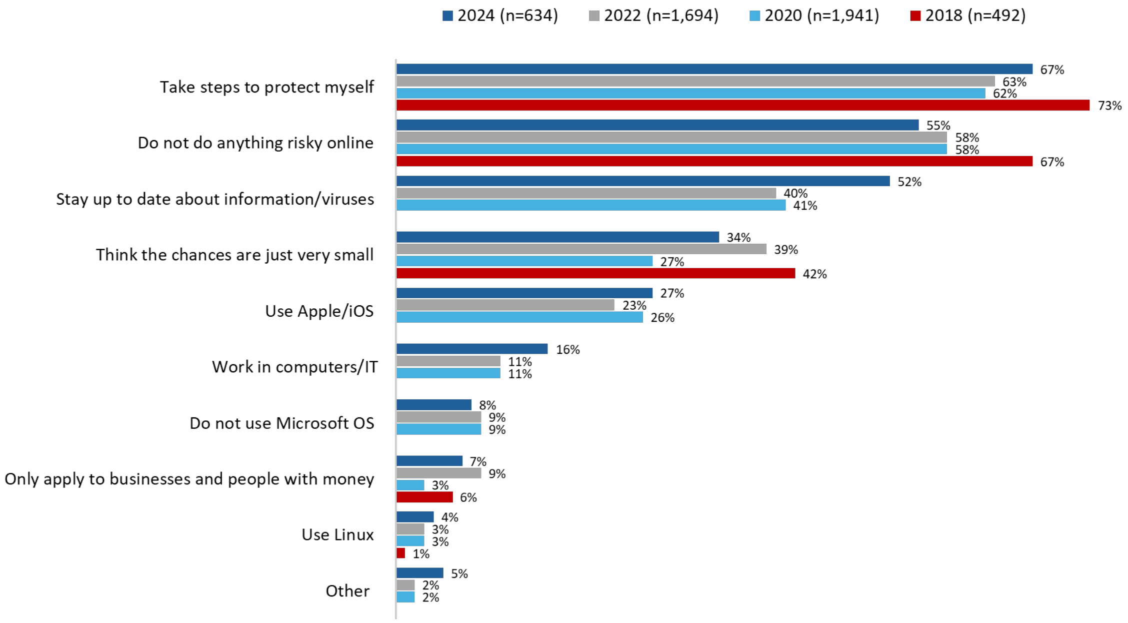
QCT1a-d. In the next year, how likely do you think it is that you will be affected by a cyber threat ...? Base: n=2,222; all respondents. Don't know: 5% to 6%.

As age decreased, the likelihood of thinking they would *not* be affected by one of these four types of cyber threats increased among online Canadians. Gen Z and Millennials were more likely than the other generations to think they will not be affected by any of these cyber threats. The same was true of those with advanced knowledge of online security.

Those who think they are unlikely to be affected by a cyber threat attributed this to actions they take or to their online behaviour.

The majority of those who think they are unlikely to be affected by a cyber threat (n=634) said it is because they take steps to protect themselves online (67%; up from 63% in 2024), avoid risky online behaviour (55%; down from 58% in 2022), or stay up to date about information and viruses (52%; up from 40% in 2022). One-third (34%; down from 39% in 2022) indicated they feel unlikely to be affected because the chances are just very small, while just over one-quarter (27%; up from 23% in 2022) think they are unlikely to be affected because they use Apple/iOS which is not as susceptible to viruses. The full range of reasons can be found in figure 22.

Figure 22: Why unlikely to be affected



QCT2. Why don't you think it is likely that you will be affected by a cyber threat? [multiple responses accepted] Base: respondents who think that they are unlikely to be affected by a cyber threat. Don't know: 1% to 2%.

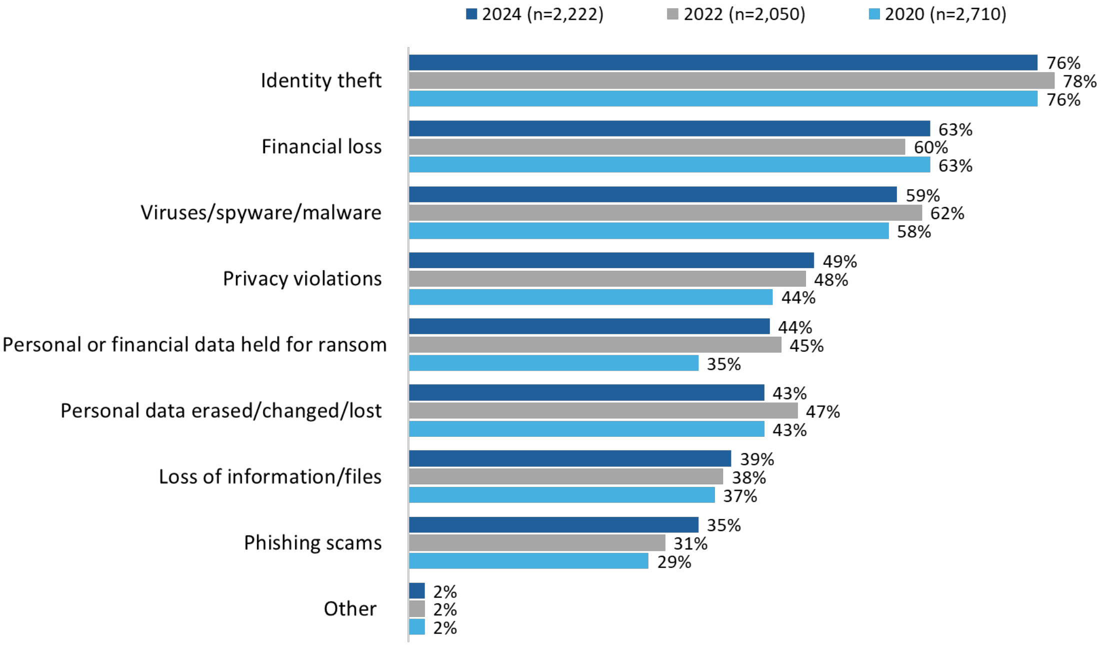
Younger respondents (i.e., those aged 44 and under), men, as well as college and university graduates were more likely to say they take steps to protect themselves. Those aged 44 and under were also more likely to say they do not do anything risky online and that the chances of being affected by a cyber threat are just small.

Identity theft, financial loss, malware top the list of threats that concern Canadians.

Consistent with previous years, three-quarters (76%) of online Canadians expressed concern about identity theft. Following identity theft, about six in 10 are most concerned about financial loss (63%) and viruses, spyware or malware (59%). Half (49%) are concerned about privacy violations, 44% about ransom attacks, 43% about personal data loss, and 39% about loss of information or files. Just over one-third (35%) are most concerned about phishing scams when thinking about cyber threats.

Over time, the proportion of online Canadians concerned about phishing scams has increased, from 29% in 2020 to 35% in 2024. After a small increase in 2022 (up to 47%), the proportion concerned about the lose of personal data has declined to the baseline level of 43%. All other concerns have not increased or decreased by more than 3% between 2022 and 2024.

Figure 23: Nature of concern



QCT3. What kinds of cyber threats are you most concerned about? Base: all respondents. Don't know: 2%.

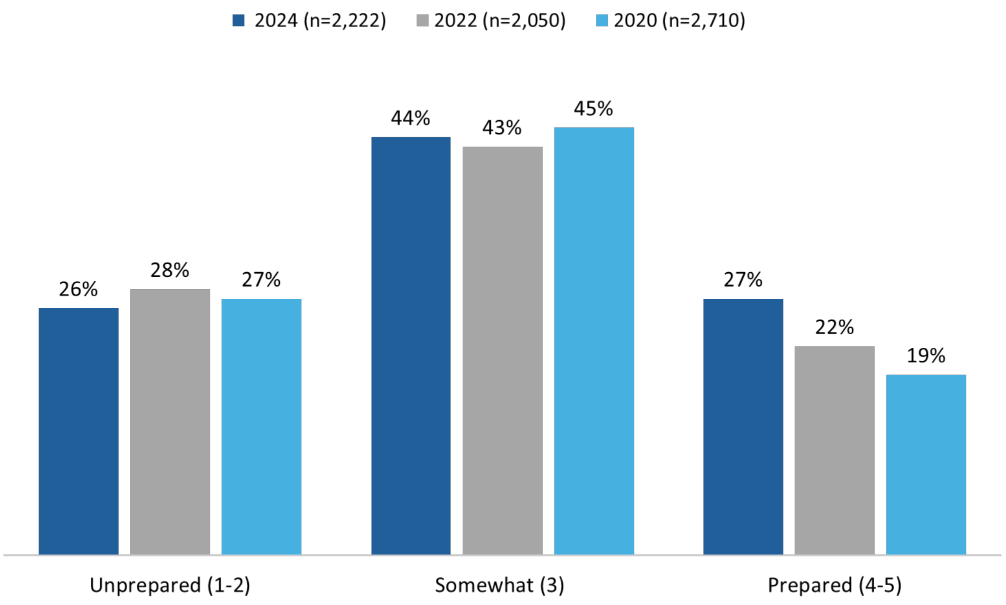
Noteworthy subgroup differences include the following:

- Respondents aged 45+ were more likely to be concerned about phishing scams, viruses, spyware or malware, and identity theft, while those aged 18 to 34 were more apt to be concerned about privacy violations.
- Gen Z was likely to be concerned about phishing scams and identity theft, and along with Millennials, more apt to be concerned about privacy violations. Concern about financial loss was higher among Millennials, Gen X, and the Silent generation than it was among Gen Z.
- The likelihood of being concerned about a ransomware attack was higher among those from households reporting an annual income of $150,000+, while those from households with an annual income of under $40,000 were less likely to be concerned about identity theft.
- Concern about identity theft and ransomware attacks increased with education levels. Those who reside in Quebec were the most likely to be concerned about identity theft.
- Canadians always connected to the internet were more likely than use who are online less often to be concerned about their personal or financial data being held for ransom.

Seven in 10 are at least somewhat prepared to face cyber threats.

The majority of online Canadians reported being somewhat (44%) or well (27%) prepared to face cyber threats. One-quarter (26%) said they feel unprepared. Over time, the proportion of online Canadians who feel they are well prepared has increased, from 19% in 2020, to 22% in 2022, to 27% in 2024.

Figure 24: Preparedness towards cyber threats



QCT4. How well prepared are you to face cyber threats? Base: all respondents. Don’t know: 4%.

Residents of Quebec were more likely than those in the rest of Canada to view themselves as unprepared to face cyberthreats. So too were those earning under $40,000 a year, women, those aged 65+, and online Canadians with a secondary school education.

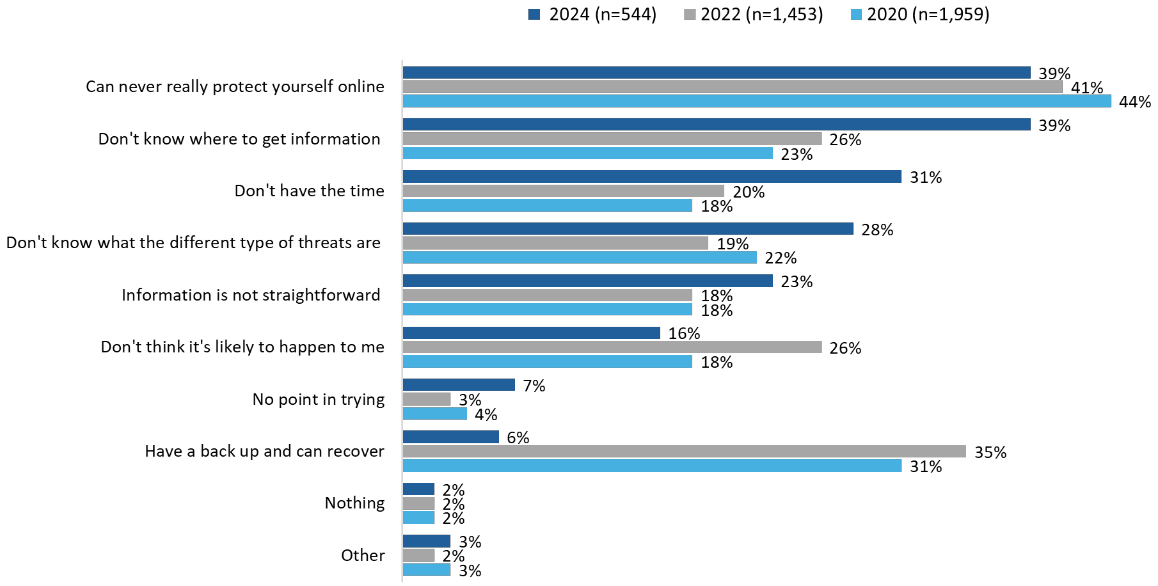
Reasons for feeling unprepared for a cyber threat varied.

Those who considered themselves not prepared to face a cyber threat (n=544) were most likely to attribute this to two reasons: the perception that you can never protect yourself online (39%) and not knowing where to get information (39%; up from 26% in 2022). Following this, approximately three in 10 mentioned lack of time (31%; up from 20% in 2022) and lack of knowledge of the different types of threats (28%; up from 19% in 2022). Nearly one-quarter said that the information is not straightforward (23%; up from 18% in 2022). The full list of reasons offered by respondents can be found in figure 25.

When the reasons for feeling unprepared are grouped together, two themes emerged: futility (protecting themselves online is not possible) and lack of knowledge (not knowing where to obtain this information, not knowing the different threats, and not having straightforward information available).

Over time, reasons related to lack of knowledge have been steadily increasing since the baseline survey in 2020.

Figure 25: Reasons for unpreparedness to face cyber threats



QCT5. Why do you feel not prepared to face cyber threats? [multiple responses accepted] Base: respondents who are not prepared to face cyber threats.

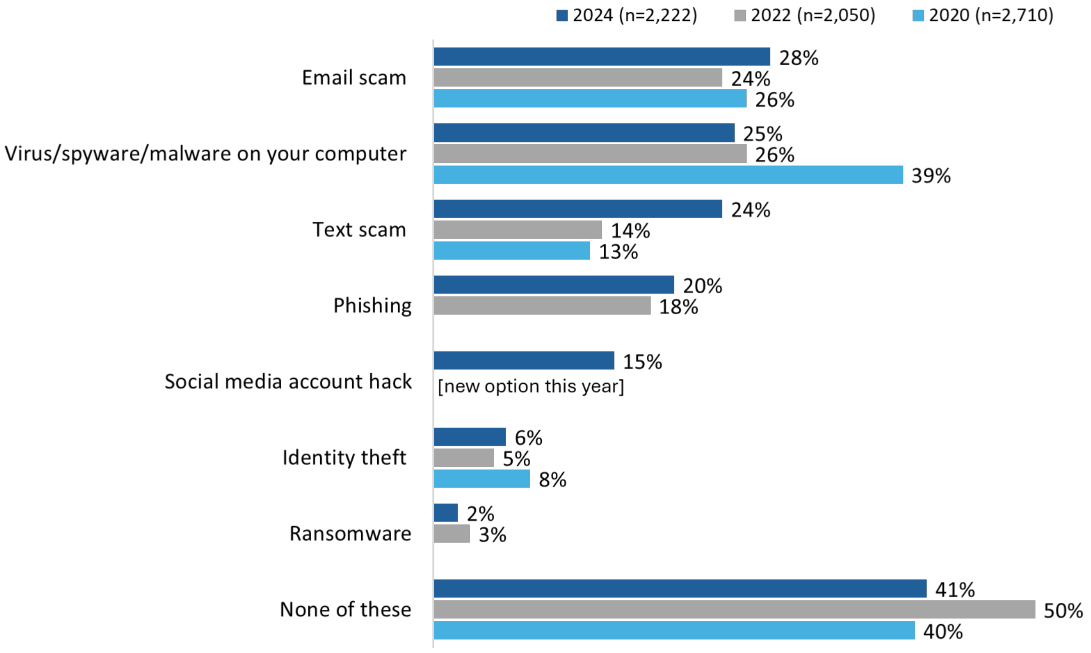
Respondents aged 65+ were more likely than younger online Canadians to attribute their lack of preparedness to a lack of resources or knowledge. Specifically, they feel unprepared because they do not know where to get this type of information, because they do not know what the different threats are, and because the information they find is not straightforward. Parents were more likely than those who do not have children under the age of 18 to say they are unprepared because they do not have the time to take steps to protect themselves.

Four in 10 online Canadians have never been a victim of a cyberattack.

Forty-one percent of online Canadians said they have never been a victim of a cyberattack (down from 50% in 2022). Those who have been a victim of a cyberattack were most likely to have experienced an email scam (28%; up from 24% in 2022), a malware attack on their computer (25%), or a text scam (24%; up from 14% in 2022). Two in 10 (20%) have been a victim of phishing scam and 15% have experienced a social media account hack. Relatively few have experienced identity theft (6%) or a ransomware attack (2%).

Over time, the incidence of email and text scams has increased, and in the case of text scams, it has increased significantly. The proportion of online Canadians who have been a victim of a virus, spyware or malware attack on their computer continues to be lower than the baseline survey, when 39% of respondents reported having experienced such an attack.

Figure 26: Incidence of Victimization



QCT6. Have you ever been a victim of any of the following cyberattacks? Base: all respondents. Don't know: 5%.

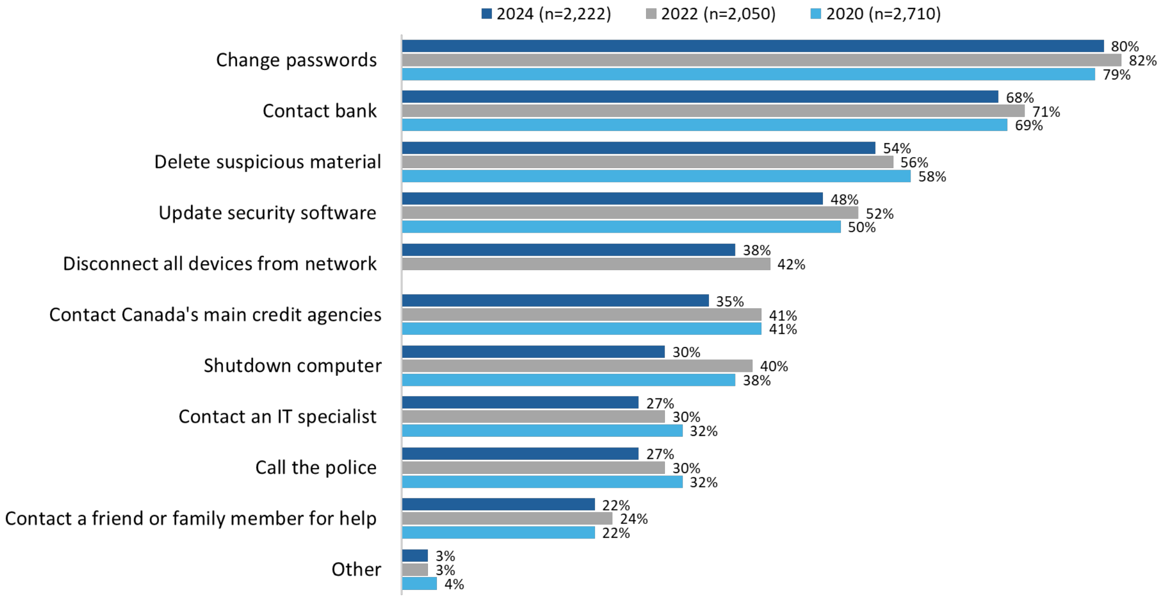
Residents of Quebec were more likely than those living elsewhere in the country to have been a victim of an email scam. The likelihood of being a victim of an email scam and phishing was higher among those aged 65+. Women were more likely than men to have been a victim of an email or text scam, and a social media account hack. Men were more apt to report being a victim of a virus, spyware or malware attack and identity theft. Canadians with advanced knowledge of online security were more likely to have never been a victim of a cyber attack.

Change password, contact the bank, delete suspicious material are the top steps that would be taken in the event of a cyberattack.

If respondents knew or suspected that they had been a victim of a cyberattack, the majority would change their passwords (80%), contact their bank (68%), and delete suspicious material (54%). Almost half (48%) would update their security software, 38% would disconnect all devices from their network, 35% would contact Canada's main credit agencies, and 30% would shut down their computer. Just over one-quarter would contact an IT specialist (27%) or call the police (27%) to protect themselves. Two in 10 (22%) would contact a friend or family member for help if they suspected they had been a victim of a cyber attack.

Over time, many of the steps that would be taken by online Canadians to protect themselves have seen minimal change. Notable exceptions this year include shutting down their computer, with far fewer pointing to this as a step they would take (30% versus 40% in 2022) and contacting Canada's main credit agencies (35% this year compared to 41% in 2020 and 2022). In addition, this year, the proportion of online Canadians who would contact an IT specialist or call the police continued to decline.

Figure 27: Steps taken to protect if victim of cyber attack



QCT7. If you knew or suspected that you'd been a victim of a cyberattack, what steps would you take to protect yourself? [multiple answers accepted] Base: all respondents. Don't know: 2%.

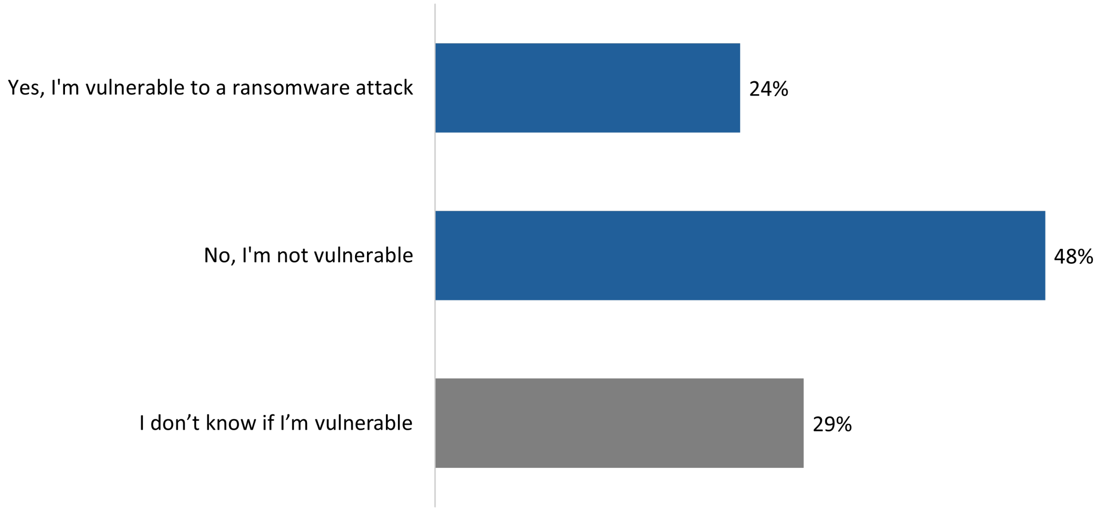
Notable subgroup differences include the following:

- Residents of Quebec were more likely than those living elsewhere in the country to contact Canada's main credit agencies. Conversely, compared to Ontarians, those living in Quebec were less likely to have said they would shutdown their computer, disconnect all connected devices, delete the suspicious material, update their security software, change their passwords, and contact their bank.
- Online Canadians aged 65+ were more likely than younger Canadians to shutdown their computer and delete the suspicious material and they were less likely to change their passwords.
- Women were more likely than men to turn to a third party for help—specifically, contacting the credit agencies, an IT specialist, or a friend or family member.
- Those with a secondary school education were less likely than their counterparts with a college or university education to update their security software, change their passwords, contact their bank, and contact an IT specialist.

One-quarter think they are vulnerable to a ransomware attack.

One-quarter (24%) of online Canadians think they are vulnerable to a ransomware attack, while almost half (48%) feel they are not vulnerable. The rest (29%) do not know whether they are vulnerable to a ransomware attack.

Figure 28: Vulnerability towards ransomware attacks



QCT8. Do you think you are vulnerable to a ransomware attack? Base: n=2,222; all respondents.

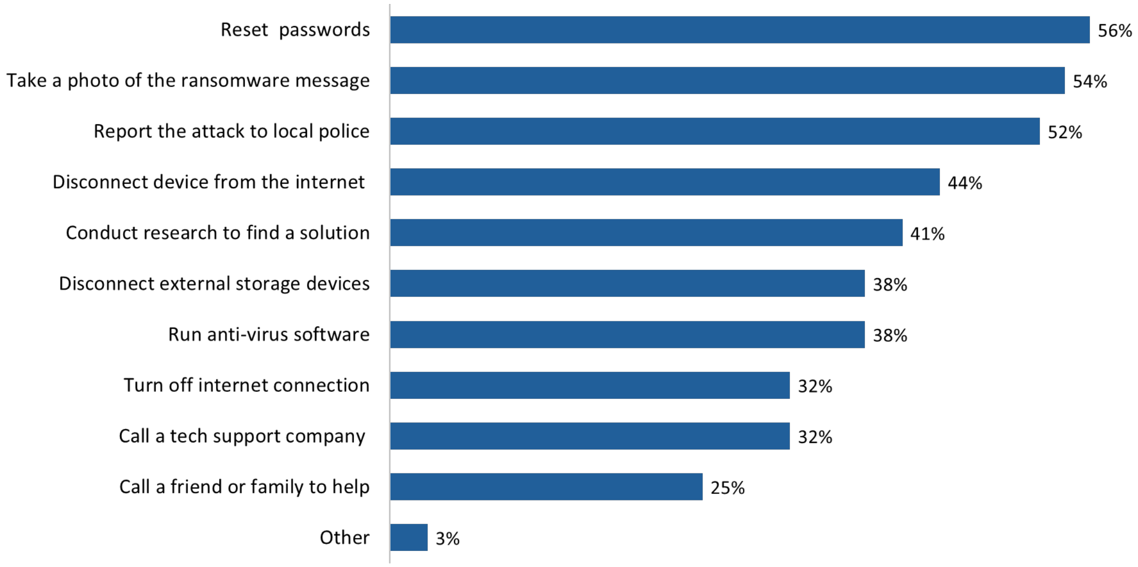
The following groups were more likely to think they are vulnerable to a ransomware attack: those who reside in Saskatchewan, men, those with an annual household income of $100,000+, and business owners. Canadians with advanced knowledge of online security were more likely than those less knowledgeable to believe they are *not* vulnerable to a ransomware attack.

When it comes to age, those between the ages of 35 and 64 were more likely than younger Canadians to think they are vulnerable to a ransomware attack, while those aged 65 and older were more likely to *not* know if they are vulnerable to such an attack.

In the event of a ransomware attack, the majority of online Canadians would reset their password, take a photo of the message, and report the attack to local police.

The majority of online Canadians would reset their passwords (56%), take a photo of the ransomware message (54%), and report it to local police (52%) if they were a victim of a ransomware attack. Following this, 44% would disconnect their device from the internet and 41% would conduct research to find a solution. Thirty-eight percent each would disconnect their external storage devices and run anti-virus software. About one-third would turn off their internet connection (32%) and call a tech support company (32%). One-quarter (25%) would call a friend or family member to help.

Figure 29: Actions one would take if a victim of a ransomware attack



QCT9. If you were a victim of a ransomware attack, what would you do? [multiple answers accepted] Base: n=2,222; all respondents. Don't know: 7%.

Those aged 45+ were more likely than younger Canadians to say they would report the attack to local police, turn off their internet connection, and call a tech company. Online Canadians aged 18 to 34 and those aged 65+ were more likely than 35–64-year-olds to say they would call a friend or family for help. The likelihood of conducting research on their own to find a solution was highest among those aged 18-34.

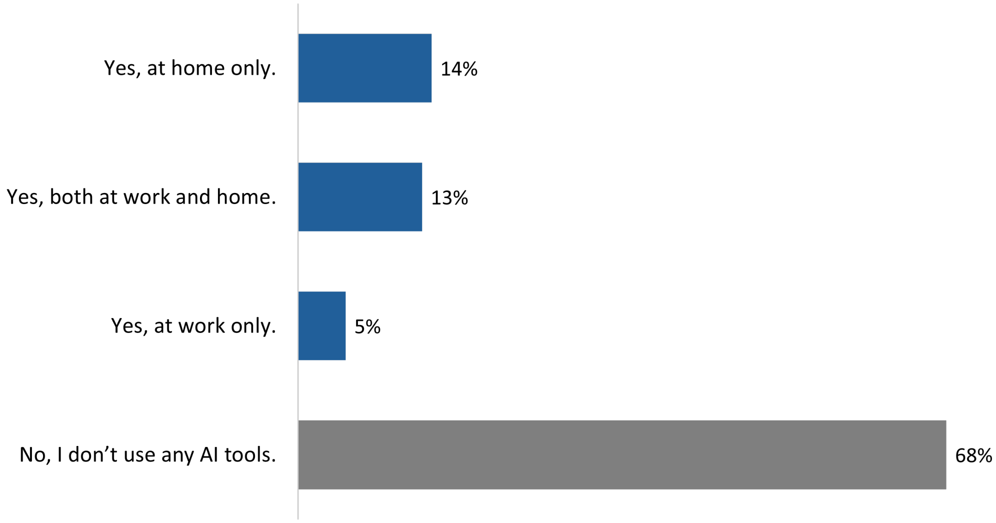
While men were more likely than women to conduct their own research, women were more likely to take a photo of the message, report it to the police, and call for help, either a friend or family (35% versus 18%) or a tech support company (38% versus 31%).

Views on artificial intelligence

One-third of online Canadians use AI tools.

One-third (32%) of online Canadians use Artificial Intelligence (AI) tools, such as ChatGPT, CoPilot, DALL-E, at home or work. Fourteen percent use AI tools at home only and 5% use them at work only. The rest (13%) use them at work and home. In contrast, two-thirds (68%) do not use any AI tools.

Figure 30: Use of AI



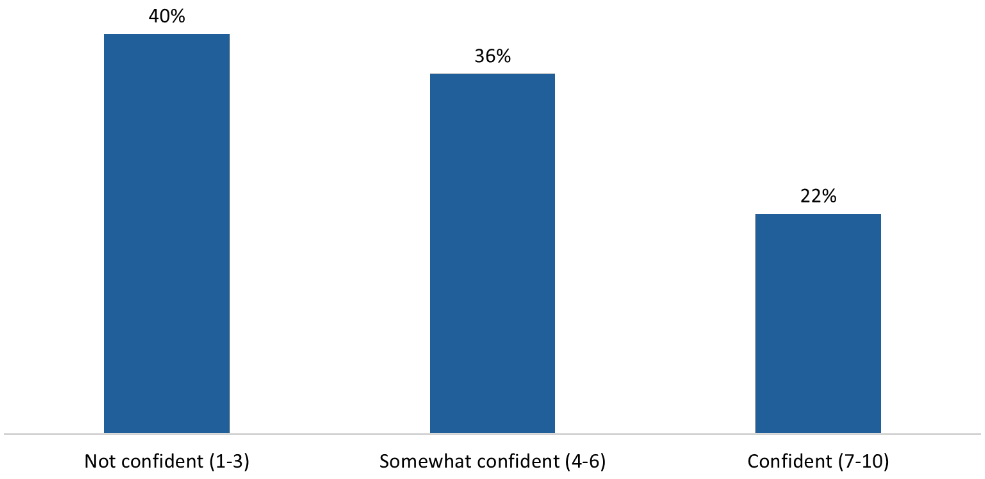
QAI1: Do you use any Artificial Intelligence (AI) tools at home or at work? Base: n=2,222; all respondents.

Use of AI tools decreased as age increased, and at-home use of AI tools was highest among 18–34-year-olds. Use of AI tools both at work and home was higher among those under the age of 45. Gen Z were the most likely to report using AI tools at home, while Baby Boomers and the Silent generation were more likely to not use AI tools. Those with a household income of over $150,000 were more likely to use AI at work and at home compared to those with a household income under $80,000.

Two-thirds are at least somewhat confident in their ability to recognize AI content.

Twenty-two percent of online Canadians reported feeling confident in their ability to recognize AI-generated content, such as messages, pictures, videos or deepfakes. An additional 36% were somewhat confident. The rest (40%) were not confident in their ability to identify content that is generated by AI.

Figure 31: Recognition of AI-generated content



QAI3. How confident are you in your ability to recognize AI-generated content (e.g. messages, pictures, videos, deepfakes)? Base: n=2,222; all respondents. Don't know: 3%.

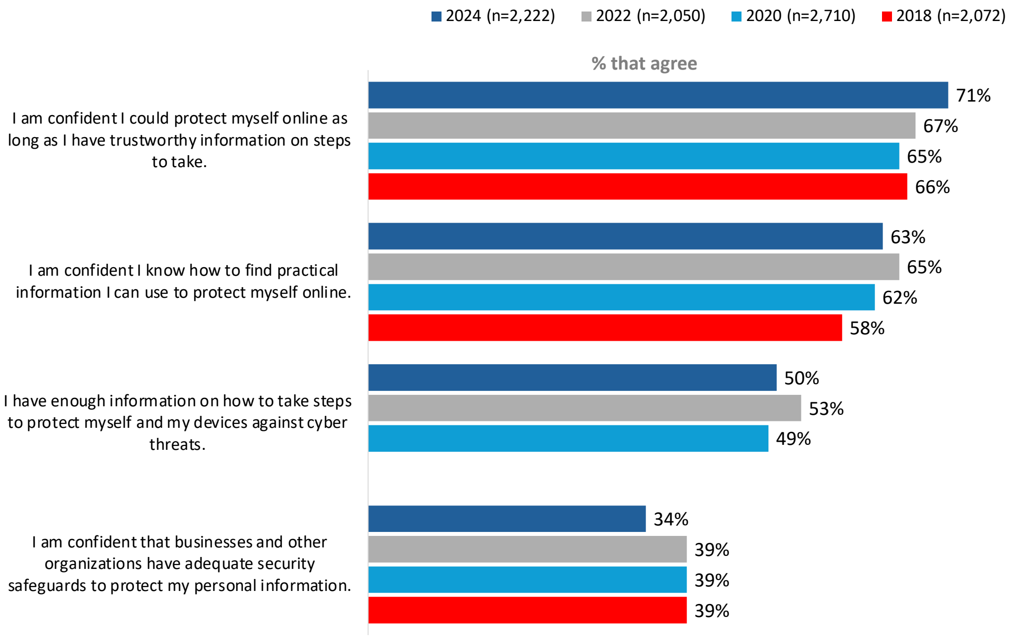
Younger online Canadians and men were more likely to be confident about their ability to recognize AI-generated content. So too were those with advanced online security knowledge. Confidence was highest among Gen Z, followed by Millennials, and then Gen X.

Communications and the Get Cyber Safe campaign

Many online Canadians are confident they can protect themselves online; far fewer are confident that businesses have adequate safeguards in place protect their personal information.

Seven in 10 (71%; up from 67% in 2022) online Canadians feel confident that they could protect themselves online as long as they have trustworthy information on the steps to take. Almost two-thirds (63%; down from 65% in 2022) feel confident that they know how to find practical information to protect themselves online and exactly half (50%; down from 53% in 2022) feel they have enough information on how to take steps to protect against cyber threats. Fewer (34%; down from 39% in 2022) are confident that businesses and other organizations have adequate security safeguards to protect personal information. This year's results are similar to 2022, with year-over-year differences not exceeding 5%.

Figure 32: Cyber threat prevention information



QINFO1. Please rate the degree to which you agree with the following statements. Base: n=2,222; all respondents. Don't know: 2%.

The likelihood of thinking they have enough information to take steps to protect themselves online was higher among online Canadians under the age of 45. Those under 45 were also more apt to be confident they could protect themselves online if they have trustworthy information and could find practical information to protect themselves online.

Men were more likely than women to agree that they have enough information on how to take steps to protect against cyber threats and to be confident they can find practical information to protect themselves online. Women were more likely to be confident that businesses and other organizations have adequate security safeguards to protect their personal information.

Those with a higher annual household income ($150,000 and over) were more apt to agree that they have enough information to protect themselves and their devices and to be confident they could protect themselves online as long as they have trustworthy information and could find practical information to use to protect themselves online.

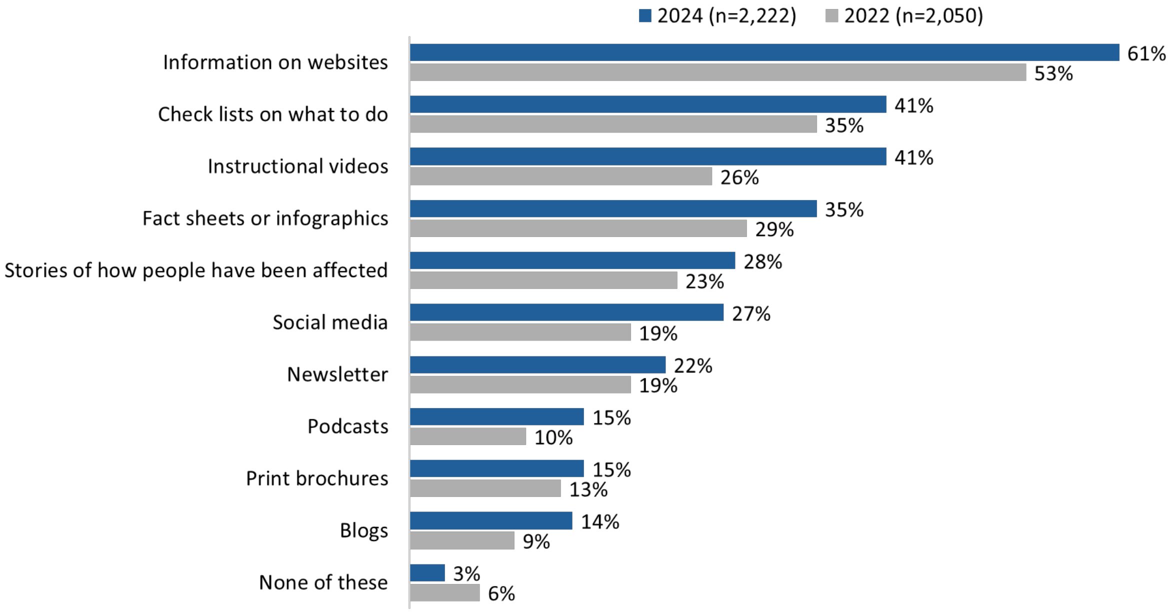
Baby Boomers and the Silent generation are most in need of information: they were more likely to lack confidence in their ability to find practical information and to protect themselves online with trustworthy information, and they were more apt to feel they do not have information to take steps to protect themselves online.

Six in 10 would prefer cyber safety information to be available on websites.

Sixty-one percent of online Canadians would prefer to get information to protect themselves from cyber threats via websites. In addition to websites, four in 10 expressed a preference for check lists on what to do (41%) and instructional videos (41%). About one-third (35%) would be interested in fact sheets or infographics. The full range of methods can be found in figure 33.

Over time, the same two methods top the list: information on websites and check lists on what to do. This year, however, more online Canadians indicated a preference for each: websites (61% versus 53%) and check lists (41% versus 35%). Indeed, across all methods, a greater proportion of online Canadians selected each one, with the most notable increase over time recorded for instructional videos: 41% expressed a preference for them this year compared to 26% in 2022. This was followed by social media: 27% expressed a preference for getting information through these platforms this year compared to 19% in 2022.

Figure 33: Preferred methods of getting information to protect against cyber threats



QINFO2. How do you prefer to get information to protect yourself from cyber threats? [multiple answers accepted] Base: n=2,222; all respondents. Don't know/refused: 6%.

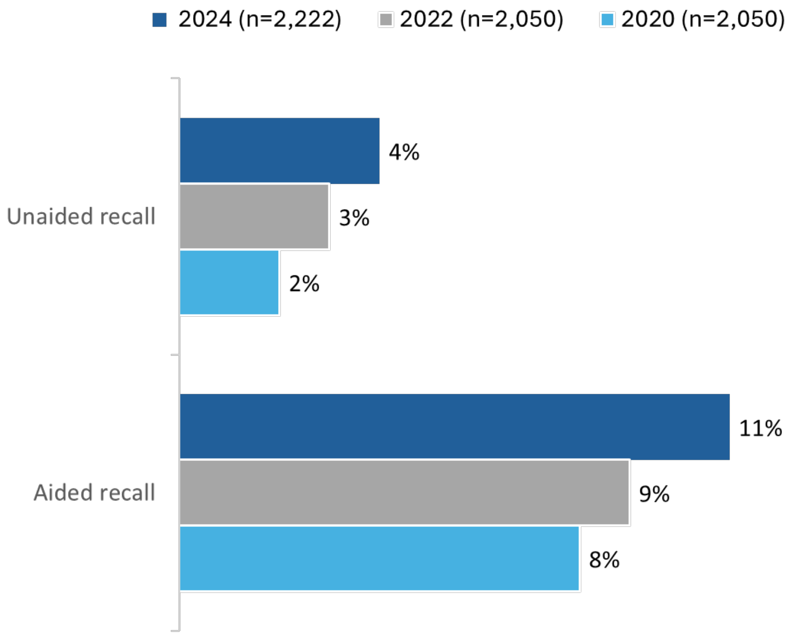
Notable subgroup differences include the following:

- Online Canadians aged 65+ were more likely to prefer check lists, print brochures, and newsletters (via an email subscription). In contrast, younger Canadians (those under 45) were more apt to prefer social media, information on websites, blogs, and fact sheets. Those 18 to 34 years of age were the most likely to express a preference for stories of how people have been affected.
- More men than women would prefer to get information to protect themselves from cyber threats via podcasts, blogs, and websites. Women, on the other hand, were more apt to prefer fact sheets or infographics, check lists, print brochures, and social media.
- College and university graduates were more likely to prefer fact sheets or infographics and check lists.

Relatively few have heard of the Get Cyber Safe campaign.

Very few (4%) respondents claimed to be able to 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. When those who said they could name the campaign were asked to provide the name, only 2% correctly named the campaign. Slightly more (11%) reported awareness of the Get Cyber Safe campaign when prompted with the name of the campaign.

Figure 34: Government of Canada cyber security campaign awareness



QGCS1. 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: all respondents. Don't know: 8%.
QGCS3. 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: all respondents. Don't know: 8%.

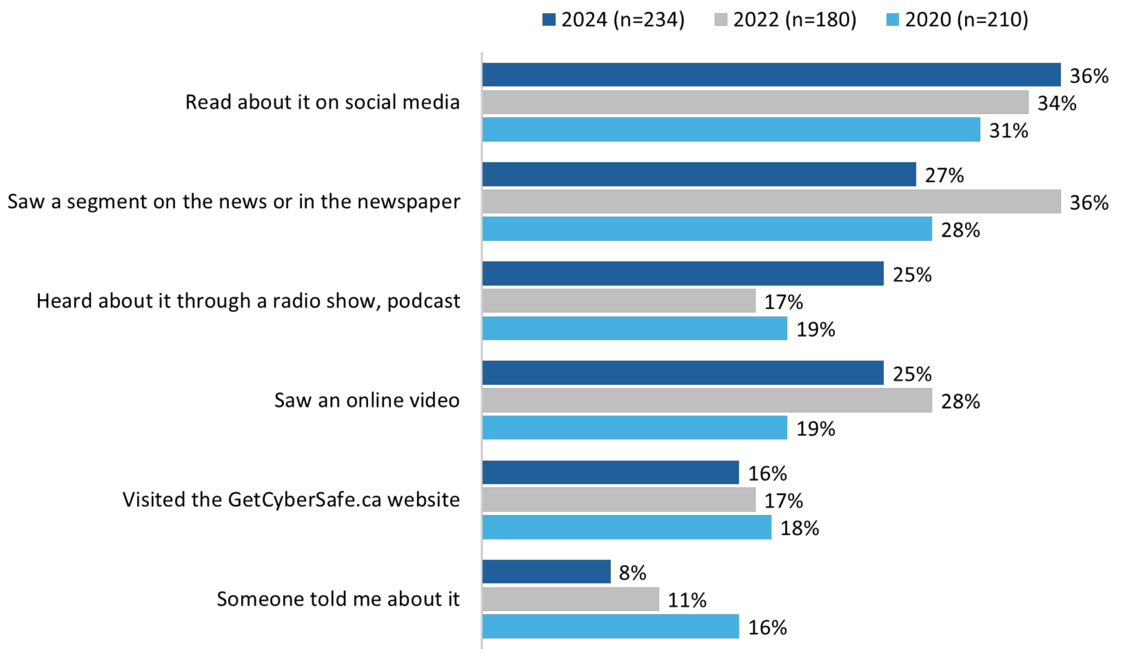
With prompting, Gen Z were more likely than Millennials, Gen X, and Baby Boomers to recall the campaign.

About one-third attributed their awareness of the campaign to social media.

Among those aware of the Get Cyber Safe campaign (n=234), just over one-third (36%) said they read about it on social media. Approximately one-quarter saw a segment on the news or in the newspaper (27%), heard about it on a radio show or podcast (25%), and saw an online video (25%). Smaller proportions visited the GetCyberSafe.ca website (16%) and heard about the campaign from someone else (8%).

More online Canadians aware of the campaign said they heard about it on a radio show or podcast in 2024 compared to 2022 (25% versus 17%), while the proportion who saw a segment in the news or newspaper has declined this year (from 36% in 2022 to 27% in 2024). All other changes over time did not exceed 3%.

Figure 35: Source of awareness of the Get Cyber Safe campaign



QGCS4. Where did you see, hear, or read this? [multiple answers accepted] Base: n=234; those aware of the Get Cyber Safe campaign. Don't know: 7%.

Businesses and cyber security

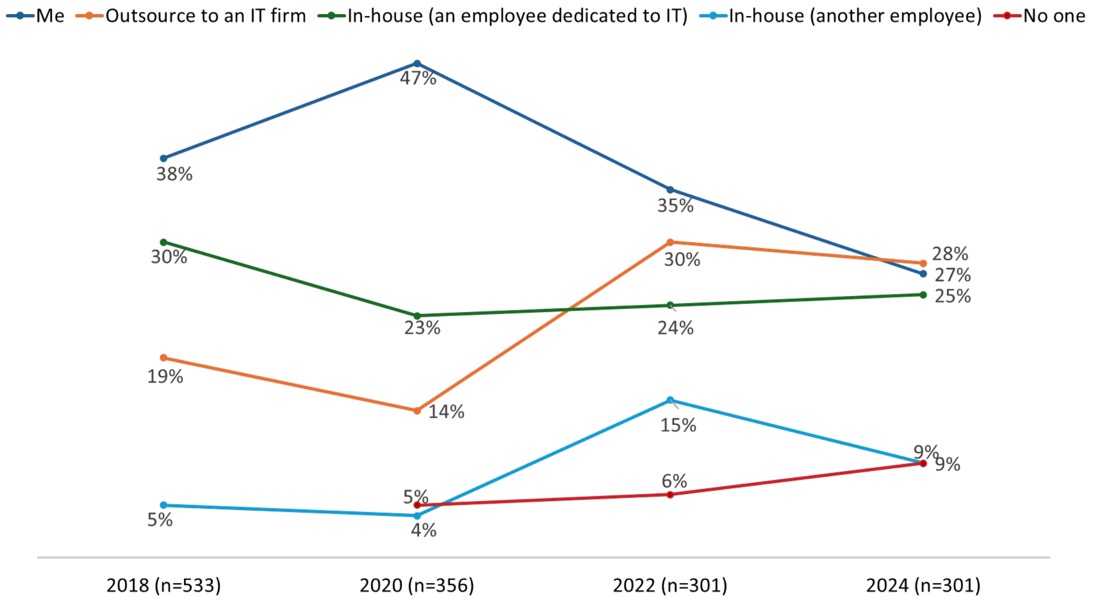
The questions in this section of the report were asked only of online Canadians who own a business or manage employees of a small business (n=301). In total, 39% of respondents were owners of a small business and 61% were managers or supervisors.

For the purpose of this survey, small businesses are considered establishments that employ up to 100 employees. Just over one-third (35%) of companies in the survey sample employ fewer than five employees. Among the rest, 14% employ five to nine employees, 35% 10 to 49 and 16% 500 to 100 employees.

In terms of IT responsibility, 28% of business respondents said their company outsources IT support, 27% are personally responsible for the company's IT, and 25% said there is a dedicated employee responsible for IT. One in 10 respondents reported that another employee (one not dedicated to IT) is responsible (9%) or that said no one at their organization is responsible for the company's IT (9%).

Over time, fewer business owners and managers are taking responsibility for their company's IT, from a high of 47% in 2020 down to 35% in 2022, and down further to 27% in 2024. Use of external service providers is virtually unchanged this year, after doubling between 2020 (14%) and 2022 (30%). Use of in-house IT support remains consistent since 2020, while the proportion of companies assigning IT support to another employee (not one dedicated to IT) has declined this year (from 15% in 2022 to 9% this year) after a significant increase from 2020 to 2022 (from 4% to 15%).

Figure 36: IT responsibility



QBUS1. Who is responsible for your company's IT? Base: business respondents; n=301. Don't know/refused: 7%.

More than three-quarters of those surveyed (78%) said their company has taken some steps to protect itself against cyber threats. Among the rest, 6% have not implemented any measures to safeguard against cyber threats and 16% did not know if their company has taken action to protect itself against cyber threats.

Half or more of the business owners and managers surveyed reported that their business requires password protection on all devices (57%), keeps security software up to date on all machines (55%), and uses a password or user authentication for wireless and remote access (51%). The full list of measures taken can be found in figure 37.

With one exception, the proportion of companies taking these steps has declined since 2022. This exception is providing cyber security best practices training for employees—there has been no change over time in the number of companies implementing this measure to protect themselves against cyber threats.

Figure 37: Measures implemented by companies to safeguard against cyber threats

	2024 (n=301)	2022 (n=301)	2020 (n=360)	2018 (n=533)
Require password protection on all devices	57%	69%	57%	71%
Keep security software up to date on all machines	55%	63%	51%	69%
Use a password or user authentication for wireless, remote access	51%	60%	52%	67%
Back up information on all devices	42%	58%	49%	60%
Set spam filters	40%	49%	39%	54%
Use encryption software	31%	34%	23%	36%
Use information removal protocols when employees leave	27%	28%	18%	37%
Adopting a cyber security policy for employees	25%	32%	18%	--
Providing cyber security best practices training for employees	24%	24%	15%	--
Do not use administrator account when accessing the web	14%	24%	15%	25%
None of these	*6%*	*5%*	*9%*	*5%*
Don't know	*16%*	*8%*	*10%*	*5%*

QBUS2. Which of the following steps has your company taken to protect itself against cyber threats? [multiple answers accepted] Base: business respondents; n=301. Refused: 2%.

When it comes to protecting their company against cyber threats, about four in 10 business owners and managers said that their organization would benefit from guidelines for reacting to a cyber attack (44%; down from 50% in 2022), from a list of the types of threats that exist and clues to look out for (42%; down from 49% in 2022) or from steps to protect mobile devices in a public setting (38%; down from 44% in 2022). The full range of information deemed beneficial by respondents can be found in the table below.

Figure 38: Beneficial information for businesses

	2024 (n=301)	2022 (n=301)	2020 (n=360)	2018 (n=533)
Guidelines for reacting to a cyber attack	44%	50%	40%	46%
A list of the types of threats that exist and cues to look for	42%	49%	41%	47%
Steps to protect mobile devices in a public setting	38%	44%	39%	40%
Guidelines to establish rules for safe email usage policies	35%	40%	28%	39%
Best practices for safe cloud computing	34%	43%	36%	35%

Tips/resources for software/hardware to make networks secure	33%	41%	29%	36%
Resources on encrypting computers, laptops, storage devices	33%	41%	34%	37%
Best practices for employees on how to handle passwords	32%	44%	29%	37%
Best practices for use of storage devices	31%	39%	34%	40%
Tips on communicating the importance of cyber security policies to employees	28%	35%	25%	32%
Steps for handling work information of departing employees	27%	33%	22%	33%
Guidelines on use of personal devices for work	27%	42%	31%	40%
Best practices for a clear internet usage policy	26%	38%	27%	37%
Guidelines on how to establish a social media policy	22%	28%	26%	37%
Other	3%	4%	3%	4%
None of these	*5%*	*5%*	*9%*	*8%*
Don't know	*12%*	*11%*	*13%*	*12%*

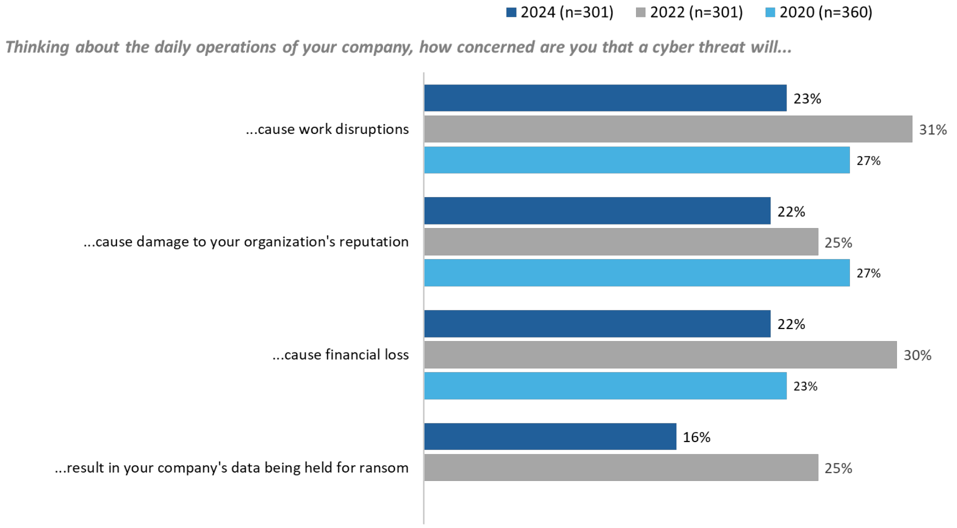
QBUS3. Which of the following types of information do you think your company would benefit from having in order to protect itself against cyber threats? Base: business respondents; n=301. Refused: 6%.

Concern about cyber threats has declined year-over-year.

When thinking about the daily operations of their company, nearly one-quarter of business owners and managers are concerned about work disruptions (23%) and almost as many are concerned about damage to the organization's reputation (22%) or financial loss (22%) (scores of 5-7 on a 7-point scale). Sixteen percent said they are concerned about their company's data being held for ransom.

Concern in each of these areas has declined since 2022. However, when factoring in those who said they are 'moderately' concerned (scores of 4), there is a small increase in the proportion of business owners and managers that are at least moderately concerned about work disruptions (62% in 2024 versus 57% in 2022).

Figure 39: Concerns regarding cyber threats

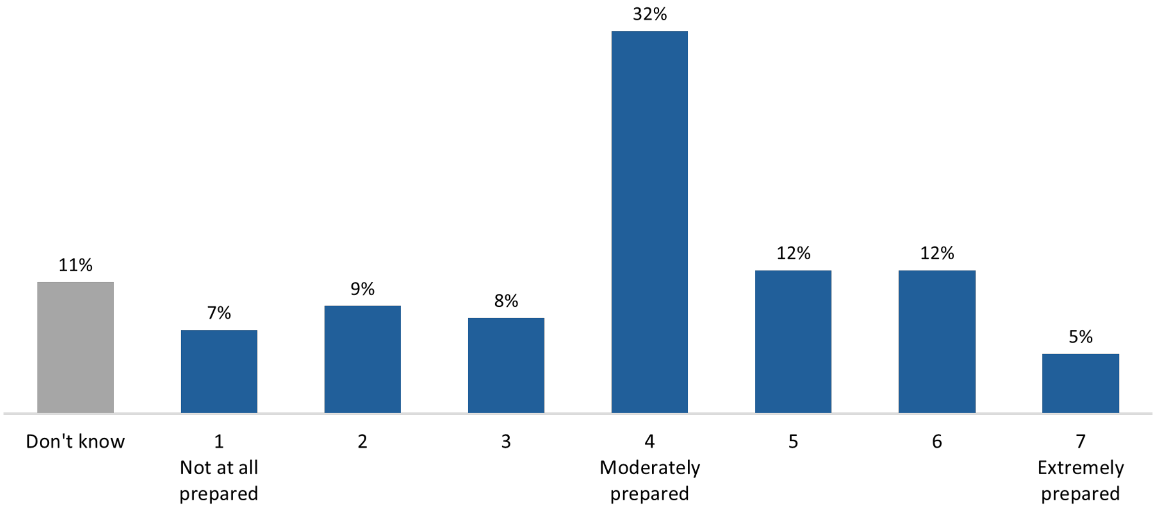


QBUS4. Thinking about the daily operations of your company, how concerned are you that a cyber threat will ... Use a 7-point scale, where '1' is not at all concerned and '7' is extremely concerned. Base: business respondents; n=301. Don't know/refused: 1% or less.

Six in 10 companies are at least moderately prepared to defend against ransomware attacks.

The majority of business owners and managers said their company is moderately (32%) or very (29%) prepared to defend against ransomware attacks. One-quarter (24%) are not prepared, and the rest (11%) did not know how to rate their company's current level of readiness when it came to defending against ransomware attacks.

Figure 40: Readiness to defend against ransomware attacks

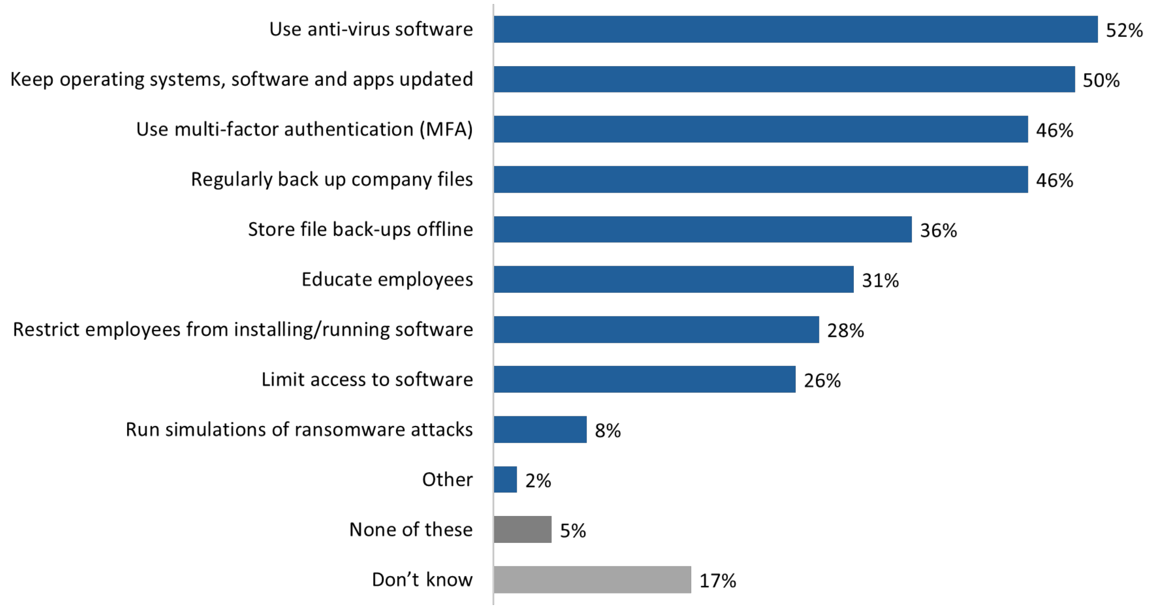


QBUS5. How would you rate your company's current level of readiness to defend against ransomware attacks? Base: business respondents; n=301. Refused: 4%.

Measures implemented by companies to safeguard against ransomware varied.

Half of business owners and managers said their company uses anti-virus software (52%) and keeps operating systems, software, and apps regularly updated (50%). Almost as many companies use MFA (46%) and regularly back up company files (46%). Just over one-third (36%) store file back-ups offline, while approximately three in 10 educate employees (31%) and restrict employees from installing and running software (28%). Roughly one-quarter (26%) limit employee access to software. Relatively few (8%) run simulations of ransomware attacks. Notably, 17% of business owners and managers did not know whether their company has done anything to protect itself from ransomware attacks.

Figure 41: Measures implemented by companies to safeguard against ransomware

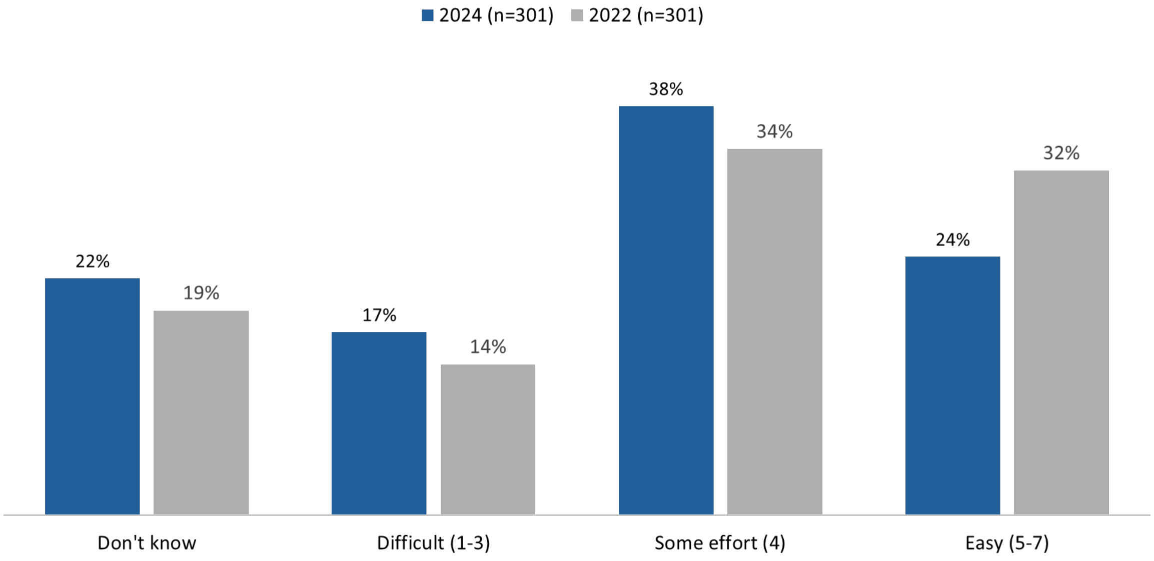


QBUS6. What, if anything, has your company done to protect itself from ransomware attacks? Base: business respondents; n=301. Refused: 6% or less.

For many companies, recovering from a ransomware attacked would take some effort.

Just over half of business owners and managers (55%; up from 48% in 2022) anticipate that it would take some effort (38%) or would be difficult (17%) to recover from a ransomware attack. One-quarter (24%; down from 32% in 2022) believe their company would recover with relative ease and with limited impact.

Figure 42: Ability to recover from a ransomware attack



QBUS7. How well would your company be able to recover from a ransomware attack? Base: business respondents; n=301. Refused: 3%.

Profile of Survey Respondents

Present in the tables below is a profile of survey respondents (using weighted data). In total, 80% of the surveys were completed in English and 20% in French.

Region	%
Atlantic Canada	7%
Quebec	23%
Ontario	39%
Manitoba	4%
Saskatchewan	3%
Alberta	11%
British Columbia and Territories	14%

Age	%
18-24	11%
25-34	17%
35-44	16%
45-54	17%
55-64	16%
65+	22%

Generation	%
Gen Z: 1997-2006	13%
Millennials: 1981-1996	25%
Gen X: 1965-1980	24%
Baby Boomers: 1946-1964	30%
Silent: 1928-1945	2%
No response	7%

Gender	%
Man	47%
Woman	49%
Another gender	2%
No response	2%

Education	%
Elementary school or less	<1%
Secondary school	8%
Some post-secondary	11%
College, vocational or trade school	25%
Undergraduate university program	27%
Graduate or professional university program	27%
No response	2%

Employment status	%
Working full-time	46%
Working part-time	8%
Self-employed	10%
Unemployed, but looking for work	2%
A student attending school full-time	6%
Retired	22%
Not in the workforce	3%
Other	2%
No response	1%

Household income	%
Under $20,000	4%
$20,000 to just under $40,000	9%
$40,000 to just under $60,000	9%
$60,000 to just under $80,000	12%
$80,000 to just under $100,000	14%
$100,000 to just under $150,000	21%
$150,000 and above	17%
No response	14%

Parent	%
Yes	28%
No	72%
No response	1%

Age of children	**%**
Under 5 years	39%
5 to 8 years	29%
9 to 12 years	32%
13 to 15 years	29%
16 to 17 years	21%

Frequency of using the internet	**%**
A few times per month	<1%
A few times per week	2%
A few times a day	2%
I'm always connected	69%

Average hours online per week	**%**
Less than 10 hours	15%
10 or more hours	83%
I don't know	3%

Level of online security knowledge	**%**
Advanced	20%
Intermediate	45%
Basic	31%
Novice/Beginner	4%
I don't have any knowledge about staying secure online.	1%

Appendix

Technical specifications

The following specifications applied to the survey:

- An online survey was administered to 2,222 Canadians, 18 years of age and older, who use the internet at least a few times a month. Quotas were in place for 300 business owners and managers/supervisors of companies with fewer than 100 employees (business sub-sample) and 300 households with children under 18 years of age (parent sub-sample). In total, surveys were completed with 301 business owners and managers/supervisors and 619 parents.
- Overall, the average survey length was 16.3 minutes with a median of 14.7 minutes.
- Based on a sample of this size, the overall results can be considered accurate within ±2%, 19 times out of 20.
- The sample was drawn from Advanis' proprietary General Population Random Sample (GPRS) which has been developed using probability-based recruitment. This panel of more than 600,000 individuals can be considered representative of the general public in Canada.
- A pre-test was conducted on February 27, 2024, with 24 individuals. Ten surveys were completed in French and the rest in English. The median length of the survey was 19 minutes. On February 28 and 29, changes to the questionnaire were implemented to reduce the survey length (the target length was 15 minutes). Changes involved the removal of questions only; there were no changes to the wording or structure of any questions. As a result, the pre-test data were retained as part of the final survey data.
- The fieldwork began in full on February 29 and was completed March 19, 2024.
- The fieldwork was conducted by Advanis using a phone-to-web methodology (which is standard for all surveys administered to GPRS panellists). All survey respondents were called at least once over the telephone. On contact, panellists they were asked if they would be willing to participate in the survey and (upon agreement) they were sent the survey invitation either by SMS or email (the method is based on the panelist's preference which is established with they join the panel). Two reminders were issued to those who had not responded to the survey. Reminders were sent three days apart.
- In total, 13,824 panellists were recruited to participant in the survey. A total of 2,222 panellists completed the survey, for a participation rate of 16%.

The survey data have been weighted by age, gender and region using population figures from Statistics Canada's 2021 census data. Any respondents who refused to provide their gender were given a neutral weight so as not to skew the weighting proportions. The tables below present the unweighted and weighted proportions for the variables used to create the weights.

Gender	% Weighted	% Unweighted
Man	49%	52%
Woman	51%	48%

Region	% Weighted	% Unweighted
Atlantic Canada	7%	7%
Quebec	23%	23%
Ontario	39%	36%
Manitoba	3%	4%
Saskatchewan	3%	3%
Alberta	11%	12%
British Columbia and Territories	14%	16%

Age	% Weighted	% Unweighted
18-24	11%	8%
25-34	16%	18%
35-44	16%	16%
45-54	17%	17%
55-64	16%	17%
65+	23%	23%

A non-response analysis was conducted to assess the potential for non-response bias. Survey non-response can bias results when there are systematic differences between survey respondents and non-respondents. The survey sample (the unweighted percentages in the tables above) very closely mirrored the distribution of the population (the weighted percentages in the tables above), so it is likely that non-response introduced very little or no bias at all.

Survey questionnaire

Survey Introduction Page

Thank you for agreeing to take part in this short survey being conducted on behalf of the Government of Canada by Phoenix SPI. Si vous préférez répondre au sondage en français, veuillez cliquer sur « Français » dans le coin supérieur droit.

This survey is designed to collect information on issues related to online security. The survey should take no more than 15 minutes to complete and is voluntary and completely confidential. The information provided will be administered according to the requirements of the *Privacy Act*. Your responses will not be used to identify you, and none of your opinions will be attributed to you personally in any way. To view Phoenix SPI's privacy policy, click <here>.

This survey is registered with the Canadian Research Insights Council's Research Verification Service. The project verification code is **20240202-PH841**. Click <here> to verify the legitimacy of this survey.

Eligibility and screening

S1. In what year were you born?
01. Year:
02. Prefer not to answer [SKIP TO S3]

S2. [IF S1=2006] Are you at least 18 years of age?
01. Yes
02. No [THANK AND TERMINATE]
03. Prefer not to answer [THANK AND TERMINATE]

S3. [IF S1=02] In which age category do you belong?
01. Less than 18 years old [THANK AND TERMINATE]
02. 18 to 24
03. 25 to 34
04. 35 to 44
05. 45 to 54
06. 55 to 64
07. 65 or older
08. Prefer not to answer [THANK AND TERMINATE]

S4. How frequently do you use the internet? This means being on an internet-connected device using apps or websites. [CAB24; Q1]
06. Less than a few times a month [THANK AND TERMINATE]
01. A few times per month
02. Once a week
03. A few times per week
04. A few times a day
05. I'm always connected

S5. On average, how many hours per week are you online? This means being on an internet-connected device using apps or websites.
01. Less than 10 hours
02. 10 or more hours
03. I don't know [THANK AND TERMINATE]

S6. In which province or territory do you currently live?
01. Alberta
02. British Columbia
03. Manitoba
04. New Brunswick
05. Newfoundland and Labrador
06. Northwest Territories
07. Nova Scotia
08. Nunavut
09. Ontario
10. Prince Edward Island
11. Quebec
12. Saskatchewan
13. Yukon
14. Prefer not to answer [THANK AND TERMINATE]

S7. Which of the following categories best describes your current employment status? Are you...?
01. Working full-time, that is, 35 or more hours per week
02. Working part-time, that is, less than 35 hours per week
03. Self-employed [SKIP TO S11]
04. Unemployed, but looking for work [SKIP TO S11]
05. A student attending school full-time [SKIP TO S11]
06. Retired [SKIP TO S11]
07. Not in the workforce [Full-time homemaker, unemployed, not looking for work] [SKIP TO S11]
08. Other [SKIP TO S11]
09. Prefer not to answer [SKIP TO S11]

S8. [IF S7=01,02] How many employees work for your company?
01. Less than 5
02. 5-9
03. 10-49
04. 50-100
05. 101-249 [SKIP TO S11]
06. 250-499 [SKIP TO S11]
07. 500 or more [SKIP TO S11]
08. Do not know
09. Prefer not to answer

S9. [IF S8=01-04] Are you the owner of the company?
01. Yes [BUSINESS QUOTA; SKIP TO S11]
02. No
03. Prefer not to answer

S10. [IF S9=02,03] Do you have any of the following responsibilities?
Please select all that apply

01. Employees report to you
02. You oversee the work of other employees
03. You're involved in decisions about processes or procedures followed by employees
04. None of these
05. Prefer not to answer

[BUSINESS QUOTA: IF S8=01-04 AND S9=01 OR S10=01-03]

S11. Are there any children under the age of 18 currently living in your household?
01. Yes [PARENT QUOTA]
02. No
03. Prefer not to answer

S12. [IF S11=01] What are the ages of children in the home?
Select all that apply

01. Under 5
02. 5 to 8
03. 9 to 12
04. 13 to 15
05. 16 to 17
06. Prefer not to answer

S13. What is your level of online security knowledge? [CAB24; Q3]
01. Advanced
02. Intermediate
03. Basic
04. Novice/Beginner
05. I don't have any knowledge about staying secure online.

Views and attitudes towards cyber security

[ALL]
These next questions are about online security, which is often referred to as cyber security.

QCS1. How much do you agree with the following statements about online security? [CAB24; Q4-Q7]
[RANDOMIZE ITEMS]
a) I find it easy to be secure when I'm online.
b) Most information on how to be secure online is confusing.
e) I presume my devices are automatically secure.
f) It is expensive to fully protect myself online.
g) I don't see the point of trying to protect myself more as my information is already online.
h) Falling victim to cybercrime is something that worries me.
i) I am unlikely to be a target of cybercrime.

k) I’m worried about Artificial Intelligence (AI)-related cybercrime.

[DO NOT RANDOMIZE; ALWAYS PRESENT LAST]
l) Family members rely on me to keep them secure online.
m) I rely on others (e.g. my family, my colleagues) to keep me secure online.

[RESPONSE OPTIONS]
1-Strongly disagree
2
3
4
5
6
7
8
9
10-Strongly agree

QCS2. Who do you rely on most for cyber security help or advice? [CAB24; Q8]
01. My family (e.g. spouse, child, relatives).
02. My friends.
03. My work colleague(s).
04. The government (e.g. government websites).
05. IT companies (e.g. tech support companies or the seller of the related device).
06. Other, please specify:____

QCS3. How much do you rely on other people for help (e.g. family, friends or colleagues) to perform the following things? [CAB24; Q10]
[RANDOMIZE ITEMS]
a) Getting advice and information on how to be secure online.
b) Creating online accounts.
c) Checking or adding security settings on my devices (e.g. PIN).
d) Checking, updating, or installing the latest software.
e) Password recovery (i.e. if you can’t access your online accounts).
f) Backing up data (e.g. files and photos).
g) Helping you spot potential scams or phishing messages (e.g., emails, texts, direct messages).

[RESPONSE OPTIONS]
1-Not reliant at all
2
3
4
5
6
7
8
9
10-Fully reliant

QCS5. How confident are you in your ability to identify a phishing message or a malicious link? [CAB24; Q25]

1-Not at all confident
2
3
4
5
6
7
8
9
10-Very confident

Cyber security measures

[ALL]
These next questions focus on cyber security measures.

QBEH1. Do you take precautions to protect your online accounts, social media accounts, devices, or networks? [Cyber22; Q1-KPI]

01. Yes
02. No
03. I don't know

QBEH2. Do you know how to install the latest software and app updates across your devices (e.g. computer and mobile phone)? [CAB24; Q29]

01. I don't know how to do this. [SKIP TO QBEH5]
02. I know how to, but I don't do it. [SKIP TO QBEH5]
03. I know how to do this and do it.

QBEH3. [IF QBEH2=03] How often do you install the latest software or application updates to your devices when notified that they are available? [CAB24; Q60]

01. Never [SKIP TO QBEH5]
02. Rarely [SKIP TO QBEH5]
03. Sometimes
04. Very often
05. Always

QBEH4. [IF QBEH3=03-05] When do you typically install software updates on your devices? [CAB24; Q61]

01. I have turned on automatic updates.
02. Immediately when I receive the notification.
03. After clicking on 'remind me later' a few times.
04. Whenever I am away from or not using my device (e.g. during the night).

QBEH6. Have you ever heard of multi-factor authentication (MFA)? [CAB24; Q17]
Also known as Two-Factor or Two-Step Verification.

01. Yes
02. No [SKIP TO QBEH10]

QBEH7. [IF QBEH6=01] You mentioned you have heard about multi-factor authentication (MFA). Do you know how to use it? [CAB24; Q18]

01. I don't know how to use it. [SKIP TO QBEH9]
02. I know how to, but I don't use it.
03. I know how to, but I stopped using it.
04. I know how to and use it regularly. [SKIP TO QBEH10]

QBEH8. [QBEH7=02, 03] What is the main reason you don't use (or stopped using) multi-factor authentication (MFA)? [CAB24; Q19]
[RANDOMIZE]
01. MFA takes too long.
02. I don't carry my phone with me all the time to be able to verify.
03. I don't see MFA adding any extra protection.
04. My password alone is strong enough.
05. I don't have a reliable phone/Wi-Fi signal all the time to be able to verify.
06. I regularly lose the device I use for MFA verification.
07. [ANCHOR] Other (please specify)
08. [ANCHOR] No reason in particular; I just don't.

QBEH9 [QBEH7=01, 02, 03]: Please rate your agreement with the following statements: [CAB24; Q23]
"I would use Multi-Factor Authentication (MFA), but..."
[RANDOMIZE ITEMS]
a) ...I don't understand how to use MFA.
b) ... I have no confidence in my ability to use MFA.
c) ...I don't have the time to use MFA.
d) ...it is unnecessary to use MFA if my device works as it should
f) ...using MFA won't stop cybercriminals.
g) ...there aren't any benefits for me to use MFA.
h) ...I don't trust MFA software.
j) ...it interferes with my applications and I worry it 'breaks' my device.

[RESPONSE OPTIONS]
1-Strongly disagree
2
3
4
5
6
7
8
9

10-Strongly agree

QBEH12. What steps do you take to verify that a WEBSITE is legitimate? [CAB24; Q27]
Please select all that apply

[RANDOMIZE]
01. Before accessing the website's address, I conduct research to verify its legitimacy.
02. I check for "https:" in the address bar.
03. I check for a padlock security symbol in the address bar.
04. I check for a checkmark or a website trust seal.
05. I analyse the overall look of the website (e.g. its appearance, whether it looks professional).
06. I read comments on other websites about its privacy or reputation.
07. [ANCHOR] Other, please specify:___

QBEH13. As far as you know, what are signs of phishing? [Cyber22; B11B]
Please select all that apply

[RANDOMIZE]
01. Uses urgent or threatening language
02. Requests sensitive information, such as financial or identifying information
03. Has offers that are too good to be true
04. Claims to be about accounts you don't have or deliveries you're not expecting
05. Contains incorrect sender email addresses, unfamiliar links, spelling or grammar errors
06. Includes unexpected or unnecessary attachments, that may have strange file names or uncommon file types
07. Includes unprofessional graphic design, with pixelated images or poor formatting
08. [ANCHOR] Other (please specify)
09. [ANCHOR] None of these
10. [ANCHOR] I don't know

QBEH14. How often do you check messages (e.g. emails, texts, or social media) for signs of phishing before clicking any links or responding to them? [CAB24; Q62]
01. Never
02. Rarely
03. Sometimes
04. Very often
05. Always
06. I don't know how to identify phishing messages.

QBEH15. When it comes to your passwords, which of the following actions do you take? [Cyber22; Q5-02,03,05,09=KPIs]
Please select all that apply

[RANDOMIZE]
01. Keep your passwords simple and easy to remember
02. Make your passwords complex with a combination of letters, numbers and symbols
03. Use a password with at least 4 words and 15 characters
04. [CANNOT BE SELECTED WITH 05] Use the same password for multiple accounts
05. [CANNOT BE SELECTED WITH 04] Use a different, unique password for each account

06. Share a password with others
07. Write down your passwords
08. Use a password manager
09. Allow your browser or an app to remember/ store your passwords
10. [ANCHOR] Other (please specify)
11. [ANCHOR] None of these
12. [ANCHOR] I don't know

QBEH17. How often do you use unique passwords for your important online accounts (e.g. emails, social media, payment-related sites)? [CAB24; Q52]
'Unique' means completely different, not just changing a character or two.

01. All of the time
02. A majority of the time
03. Half of the time
04. A minority of the time
05. None of the time

QBEH18. [IF QBEH17=04,05] You mentioned that you rarely, if at all, use unique passwords for your online accounts. What is the main reason you don't do this? [CAB24; Q53]
[RANDOMIZE]
01. It is too time-consuming to create them.
02. They are difficult to remember.
03. It requires too much effort.
04. I don't know how to create them.
05. I only use them for accounts where I want increased security.
06. [ANCHOR] Other, please specify: _

[BUSINESS QUOTA: IF S8=01-04 AND S9=01 OR S10=01-03, SKIP TO NEXT SECTION; EVERYONE ELSE, CONTINUE]

QBEH21. How long are the password(s) you usually create? [CAB24; Q59]
01. 6 characters or less
02. 7-8 characters
03. 9-11 characters
04. 12-15 characters
05. 16 characters or longer

QBEH22. What is your preferred method of remembering multiple passwords? [CAB24; Q66]
[RANDOMIZE]
01. I write them down in a notebook.
02. I write them down in a document on my computer (electronic format).
03. I store them in my phone.
04. I store them in my email.
05. I remember them (without writing them down).
06. I save passwords in the browser (e.g. Google Chrome or Firefox).
07. I use a password manager application (e.g. 1Password, LastPass, iCloud keychain).
08. I just reset them each time I need to log in.

Cybercrime

[ALL]
These next questions are about cybercrimes.

QCCE1. Have you ever personally been a victim of online scams where you have lost money or data? [CAB24; Q31]
Please select all that apply

[RANDOMIZE]
01. Phishing scam (via email or text).
02. Online dating scam [SKIP TO QCT1]
03. Identity theft [SKIP TO QCT1]
05. Other, please specify [SKIP TO QCT1]
04. [ANCHOR; EXCLUSIVE] No, I have not lost money or data due to online scams [SKIP TO QCT1]

Add mouseover/hover boxes:

- “Phishing”: Cybercriminals trick people into providing information or installing dangerous software in order to steal money or data from them. This is often done via fake emails that appear to be from trusted senders, which encourage people to click malicious links to fake websites, or to open malicious attachments.
- “Online dating scam”: Scammers adopt a fake online identity to create an illusion of a romantic or close relationship to manipulate and/or steal from the victim. They often use highly emotive requests for money claiming they need emergency medical care, or to pay for transport costs to visit the victim if they are overseas.
- “Identity theft”: Identity theft is when scammers access enough information about someone’s identity (such as their name, date of birth, current or previous addresses) to obtain goods or services by deception, such as by opening a bank account or obtaining a credit card or loan.

QCCE2. [IF QCCE1=01] You mentioned that you have lost money or data through a phishing scam. Did you report this to anyone? *If you have lost money/data more than once, please think about the most recent time this happened.* [CAB24; Q32]
Please select all that apply

[RANDOMIZE]
01. Yes, to my bank/credit card company.
02. Yes, to the police, or another government agency or organization.
03. Yes, to the designated person or department at my work or place of education.
04. Yes, to my network/broadband or phone provider.
05. Yes, to my email or online search provider (e.g. Gmail).
06. Yes, to the service/application provider where I lost money/data.
07. Yes, my online security provider (e.g. Norton, McAfee).
08. Yes, I told my family, who then took action on my behalf.
09. [ANCHOR; EXCLUSIVE] No, I didn’t report or mention it to anyone.

QCCE3. [IF QCCE2=01-08] What is the main reason you reported a phishing scam? If you have lost money/data more than once, please think about the most recent time this happened. [CAB24; Q33]
01. It is important to notify the relevant authorities so this doesn’t happen to me or other people.

02. I wanted to take action to get my money back.
03. I wanted the cybercriminals to be caught.
04. Other, please describe:

QCCE4. [IF QCCE2=09] What is the main reason you didn't report the phishing scam? [CAB24; Q34]
[RANDOMIZE]
01. I didn't have the time.
02. I didn't know who to report it to.
03. I didn't know how to report it.
04. The process was too much effort (couldn't be bothered).
05. There was no point as no action would have been taken.
06. I forgot.
07. I was too ashamed to have fallen for the scam.
08. The amount of money/data lost was too small or unimportant to me.
09. [ANCHOR] Other, please specify:

Cyber threats

[ALL]
These next questions are about cyber threats. A cyber threat is an activity intended to compromise the security of a computer system.

QCT1. In the next year, how likely do you think it is that you will be affected by a cyber threat ... [Cyber22; Q11A-D]
[ROTATE A-C AS A BLOCK]
a) ...causing your personal information to be compromised?
b) ...causing you financial loss?
c) ...causing you the loss of files, photos?
d) …where your data will be held for ransom?

1-Not at all likely
2
3- Moderately likely
4
5-Extremely likely
I don't know

QCT2. [IF QCT1A-D=01, 02] Why don't you think it is likely that you will be affected by a cyber threat? [Cyber22; K8A]
Please select all that apply

[RANDOMIZE]
01. Take steps to protect myself online
02. Do not do anything risky online
03. Think the chances are just very small
04. Online threats only apply to businesses and people with a lot of money
05. Stay up to date/knowledgeable/educated about information/viruses
06. Work in computer/information technology

07. Use Apple/iOS which is not as susceptible to viruses
08. Use Linux which is not as susceptible to viruses
09. Do not use Microsoft OS
10. [ANCHOR] Other (please specify)
11. [ANCHOR] I don't know

QCT3. What kinds of cyber threats are you most concerned about? [Cyber22; Q15]
Please select all that apply

[RANDOMIZE]
01. Phishing scams
02. Viruses/spyware/malware
03. Identity theft
04. Privacy violations
05. Financial loss
06. Personal or financial data held for ransom (Ransomware)
07. Loss of information/files
08. Personal data erased/ changed/ lost
09. [ANCHOR] Other (please specify)
10. [ANCHOR] None of these
11. [ANCHOR] I don't know

QCT4. How well prepared are you to face cyber threats? [Cyber22; Q16-KPI]
01. Not at all prepared
02. Not prepared
03. Somewhat prepared
04. Prepared
05. Very well prepared
06. I don't know

QCT5. [IF QCT4=01,02] Why do you feel not prepared to face cyber threats? [Cyber22; Q17]
Please select all that apply

[RANDOMIZE]
01. I don't think it's likely to happen to me
02. I don't have the time/ never get around to taking steps to protect myself
03. I don't know what the different type of threats are
04. I don't know where to get information about the steps to take
05. The information I find is not straightforward enough to help me
06. You can never really protect yourself online
07. There's no point in trying
08. I have a back up and can recover
09. [ANCHOR] Nothing
10. [ANCHOR] Other (please specify)
11. [ANCHOR] I don't know

QCT6. Have you ever been a victim of any of the following cyber attacks? [Cyber22; Q18]
Please select all that apply

[RANDOMIZE]
01. Email scam
02. Text scam
03. Virus/spyware/malware on your computer
04. Identity theft
05. Social media account hack
06. Phishing
07. Ransomware
08. [ANCHOR] None of these
09. [ANCHOR] I don't know

QCT7. If you knew or suspected that you'd been a victim of a cyber attack, what steps would you take to protect yourself? [Cyber22; Q19]
Please select all that apply

[RANDOMIZE]
01. Shutdown my computer
02. Disconnect all devices that are connected to my network
03. Delete suspicious material (email, text, downloaded content, etc.)
04. Update my security software
05. Change my passwords
06. Contact my bank
07. Contact Canada's main credit agencies (Trans Union, Equifax)
08. Contact an IT specialist
09. Contact a friend or family member for help
10. Call the police
11. [ANCHOR] Nothing
12. [ANCHOR] Other (please specify)
13. [ANCHOR] I don't know

QCT8. Do you think you are vulnerable to a ransomware attack? [NEW]
Add mouseover/hover box: "Ransomware attack": Ransomware is a type of malware that blocks access to the victim's personal data unless a sum of money (i.e., a ransom) is paid.

01. Yes
02. No
03. I don't know if I'm vulnerable to a ransomware attack

QCT9. If you were a victim of a ransomware attack, what would you do? [NEW]
Please select all that apply

[RANDOMIZE]
01. Take a photo of the ransomware message
02. Report the attack to local police
03. Disconnect my device from the internet
04. Turn off my internet connection
05. Disconnect external storage devices like hard drives, USBs, and cloud
06. Call a friend or family to help
07. Conduct research to find a solution

08. Run anti-virus software
09. Reset all my passwords
10. Call a tech support company to help me
11. [ANCHOR] Other (please specify)
12. [ANCHOR] I don't know

Artificial intelligence

[ALL]
These next questions are about Artificial Intelligence (AI).

QAI1: Do you use any Artificial Intelligence (AI) tools* at home or at work? [CAB24; Q72]
***For example: ChatGPT, CoPilot, DALL-E.**

01. Yes, at home only.
02. Yes, at work only.
03. Yes, both at work and home.
04. No, I don't use any AI tools.

QAI3. How confident are you in your ability to recognize AI-generated content (e.g. messages, pictures, videos, deepfakes)? [CAB24; Q77]
1-Not at all confident
2
3
4
5
6
7
8
9
10-Very confident
I don't know

Businesses and cyber security

[BUSINESS: IF S8=01-04 AND S9=01 OR S10=01-03]

Turning to your work,

QBUS1. Who is responsible for your company's IT? [Cyber22; QBUS4]
Select all that apply

[RANDOMIZE]
01. Me
02. Another employee (specify role in company):
03. An employee of the organization dedicated to IT
04. Outsource to an IT firm
05. [ANCHOR] No one
06. [ANCHOR] Other (please specify)
07. [ANCHOR] None of these

08. [ANCHOR] Do not know
09. [ANCHOR] Prefer not to answer

QBUS2. Which of the following steps has your company taken to protect itself against cyber threats? [Cyber22; BUS1]
Select all that apply

[RANDOMIZE]
01. Keep security software up-to-date on all machines
02. Set spam filters
03. Require password protection on all devices
04. Back up information on all devices
05. Use encryption software
06. Do not use administrator account when accessing the web
07. Use a password or user authentication for wireless and remote access
08. Follow information removal protocols when employees leave the organization
09. Providing cyber security best practices training for employees
10. Adopting a cyber security policy for employees
11. [ANCHOR] None of these
12. [ANCHOR] I don’t know
13. [ANCHOR] Prefer not to answer

QBUS3. Which of the following types of information do you think your company would benefit from having in order to protect itself against cyber threats? [Cyber22; QBUS3]
Select all that apply

[RANDOMIZE]
01. A list of the types of threats that exist and cues to look for
02. Tips on communicating the importance of following cyber security policies to employees
03. Best practices for a clear internet usage policy
04. Guidelines to establish rules for safe email usage policies
05. Guidelines on how to establish a social media policy
06. Tips/resources for the type of software/hardware to make networks secure
07. Best practices for employees on how to handle passwords
08. Steps to protect mobile devices in a public setting
09. Steps for handling work-related information possessed by departing employees
10. Guidelines for reacting to a cyber attack
11. Best practices for safe cloud computing (with definition of cloud computing)
12. Best practices for use of storage devices (e.g. USBs)
13. Resources on how to encrypt computers, laptops, and storage devices
14. Guidelines on use of personal devices for work
15. [ANCHOR] Other (please specify)
16. [ANCHOR] None of these
17. [ANCHOR] I don’t know
18. [ANCHOR] Prefer not to answer

QBUS4. Thinking about the daily operations of your company, how concerned are you that a cyber threat will ... [Cyber22; QBUS5A1-4]
[RANDOMIZE]

a) ...cause work disruptions?
b) ...cause damage to your organization's reputation?
c) ...cause financial loss?
d) ...result in your company's data being held for ransom?

[RESPONSE OPTIONS]
1-Not at all concerned
2
3
4-Moderately concerned
5
6
7-Extremely concerned
I don't know
Prefer not to answer

QBUS5. How would you rate your company's current level of readiness to defend against ransomware attacks? [NEW]
1-Not at all prepared
2
3
4-Moderately prepared
5
6
7-Extremely prepared
I don't know
Prefer not to answer

QBUS6. What, if anything, has your company done to protect itself from ransomware attacks? [NEW]
Select all that apply

[RANDOMIZE]
01. Educate employees
02. Keep operating systems, software and apps updated
03. Restrict employees from installing and running software
04. Limit access to software to employees who need the programs
05. Use anti-virus software
06. Use multi-factor authentication (MFA)
07. Regularly back up company files
08. Store file back-ups offline
09. Run simulations of ransomware attacks to practice the company response
10. [ANCHOR] Other (please specify)
11. [ANCHOR] None of these
12. [ANCHOR] I don't know
13. [ANCHOR] Prefer not to answer

QBUS7. How well would your company be able to recover from a ransomware attack? [Cyber22; BUSBA42]

1-With great difficulty and hardship
2
3
4-With some effort, but recover reasonably well
5
6
7-Easily, with limited impact
I don't know
Prefer not to answer

Information needs and communications preferences

[ALL]
You're almost finished this survey. Thank you for sharing your views.

QINFO1. Please rate the degree to which you agree with the following statements. [Cyber22; QA13, 111B, 118, A120; C=KPI]
[RANDOMIZE ITEMS]
a) I have enough information on how to take steps to protect myself and my devices against cyber threats.
b) I am confident I could protect myself online as long as I have trustworthy information on steps to take.
c) I am confident I know how to find practical information I can use to protect myself online.
d) I am confident that businesses and other organizations have adequate security safeguards to protect my personal information.

[RESPONSE OPTIONS]
1-Strongly disagree
2-2
3-3
4-Neither
5-5
6-6
7-Strongly agree
I don't know

QINFO2. How do you prefer to get information to protect yourself from cyber threats? [Cyber22; Q20]
Please select all that apply

[RANDOMIZE]
01. Podcasts
02. Blogs
03. Fact sheets or infographics
04. Check lists on what to do
05. Instructional videos
06. Stories of how people have been affected

07. Information on websites
08. Print brochures
09. Newsletter (e.g. an email subscription)
10. Social media
11. [ANCHOR] Other (please specify)
12. [ANCHOR] None of these
13. [ANCHOR] I don't know

Get Cybersafe campaign

[ALL]
QGCS1. 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? [Cyber22; Q23-KPI]
01. Yes
02. No [SKIP TO QGCS3]
03. I don't know [SKIP TO QGCS3]

QGCS2. [IF QGCS1=01] What is the name of the campaign?
[OPEN]

QGCS3. 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? [Cyber22; GOCAD-KPI]
01. Yes
02. No [SKIP TO D1]
03. I don't know [SKIP TO D1]

QGCS4. [IF QGCS3=01] Where did you see, hear, or read this? [Cyber22; GOCADA]
Select all that apply

[RANDOMIZE]
01. Visited the GetCyberSafe.ca website
02. Heard about it through a radio show, podcast
03. Read about it on social media
04. Saw an online video
05. Someone told me about it
06. Saw a segment on the news or in the newspaper
07. [ANCHOR] Other (please specify)
08. [ANCHOR] I don't know

Demographics

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

D1. How do you identify your gender?
01. Man

02. Woman
03. I identify as another gender
04. Prefer not to answer

D2. What is the highest level of formal education that you have completed to date?
01. Elementary school or less
02. Secondary school
03. Some post secondary
04. College, vocational or trade school
05. Undergraduate university program
06. Graduate or professional university program
07. Prefer not to answer

D3. Which of the following categories best describes your total household income last year, before taxes, from all sources for all household members?
01. Under $20,000
02. $20,000 to just under $40,000
03. $40,000 to just under $60,000
04. $60,000 to just under $80,000
05. $80,000 to just under $100,000
06. $100,000 to just under $150,000
07. $150,000 and above
08. Prefer not to answer

Closing page

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.