Government of Canada / Gouvernement du Canada

Get Cyber Safe Awareness Tracking Survey: 2026 Final Report

Prepared for the Communications Security Establishment Canada

Supplier name: Phoenix Strategic Perspectives Inc.
Contract Number: CW2426715
Contract Value: $79,075.00 (including applicable taxes)
Award Date: 2025-11-04
Delivery Date: 2026-03-11
Registration Number: POR 052-25

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 Canada
Supplier name: Phoenix Strategic Perspectives Inc.

This public opinion research report presents the results of an online survey of 2,330 Canadians, aged 18+, conducted by Phoenix SPI on behalf of the Communications Security Establishment Canada (CSE) between January 9 and January 29, 2026.

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

Catalogue number:

- D96-17/2026E-PDF

International Standard Book Number (ISBN):

- 978-0-660-98883-2

Related publications (registration number: POR 052-25):

- **Catalogue number:** D96-17/2026F-PDF
- **ISBN:** 978-0-660-98884-9

Table of Contents

List of Figures

Executive Summary

Phoenix Strategic Perspectives Inc. (Phoenix SPI) was commissioned by the Communications Security Establishment Canada (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 (Cyber Centre) which provides expert advice, guidance, services and support on cyber security for Canadians and businesses. Since 2018, CSE's Marketing team has managed the Get Cyber Safe national public awareness campaign[1], created to inform Canadians about cyber security and the simple steps they can take to protect themselves online.

Quantitative public opinion research (POR) has been conducted every two years since 2020 to gather information on Canadians' knowledge and attitudes towards cyber security in the context of the campaign. This POR complements research on cyber security undertaken by Public Safety Canada in 2011, 2017 and 2018. The research findings provide a long-term picture of how Canadians approach cyber security for themselves and for the people in their lives. Results show year-over-year progress in specific areas but also highlight where Canadians are vulnerable to cyber threats.

For this iteration of the survey, the objectives were to:

- Assess the performance of the Get Cyber Safe public awareness campaign and help identify shifts in knowledge, behaviours and attitudes.
- Track awareness, attitudes and behaviours relating to cyber security activities among the target audiences.
- Identify and track motivators and barriers to behaviour change.
- Identify and track the best ways of communicating cyber security information; and
- Track public expectations in terms of the involvement of the federal government.

The findings from this year's POR will be used to inform the direction of the Get Cyber Safe campaign, the Cyber Centre, and other communications and public messaging from CSE.

Methodology

A 15-minute online survey was conducted with 2,330 online Canadians aged 18 and older. This included 846 surveys with parents of children under 18 years of age, and 300 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

[1] Get Cyber Safe was created in 2011 under Public Safety Canada, as part of Canada's National Cyber Security Strategy. The initial TBS planning documents for the campaign identified the need for regular POR about cyber security, which Public Safety Canada undertook.

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 ±2.1%, 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 January 9 to January 29, 2026. More information on the methodology can be found in the Appendix: Technical Specifications.

Key findings

Cyber security practices of online Canadians

More than eight in 10 (84%) online Canadians take precautions to protect their online and social media accounts, devices and networks, and nearly two-thirds (63%) do not assume their devices are automatically secure.

Starting with software updates, just over eight in 10 (82%) know how to install the latest software and app updates across their devices and do so. Among this group, 87% install updates regularly, including 46% who always do so when notified. Those who regularly install updates typically act quickly: 52% have automatic updates enabled and 17% install updates immediately after receiving a notification.

Beyond installing updates, online Canadians are generally aware of account security measures and tend to use them. A large majority (94%) have heard of multi-factor authentication (MFA), and among those aware, most (86%) know how to use it and do so regularly. Among those who no longer use MFA, the most common reason (34%) is the perception that it takes too long.

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 (55%). Approximately half (49%) conduct research to validate that a website is legitimate, while 40% read comments about a website’s privacy and reputation, and 38% check for a padlock security symbol in the address bar.

The majority of online Canadians recognize common signs of phishing messages. These include claims about accounts they do not have or unexpected deliveries (88%), requests for sensitive information (87%), and messages containing incorrect email addresses, unfamiliar links, or spelling or grammar mistakes (86%). Nearly as many identify offers that seem too good to be true (84%) and unexpected or unnecessary attachments (79%) as indicators of phishing. Three-quarters (76%) recognize urgent or threatening language, while two-thirds (65%) identify unprofessional graphic design as a sign of phishing.

Most online Canadians (77%) report creating complex passwords using a combination of letters, numbers, and symbols. Smaller proportions report using a password manager (35%), a unique password for each account (32%), or a passphrase (14%). For important accounts, half use unique passwords all (31%) or most (28%) of the time.

While many Canadians report using practices that support account security, some behaviours may increase risk. For example, 38% allow browsers or apps to autofill passwords, 27% write passwords down, and 26% reuse the same password across multiple accounts. Among those who rarely, if ever, use unique passwords, 62% say this is because they find it difficult to remember different passwords.

Cybercrime and threats

Eight in 10 (81%) online Canadians report never having experienced an online scam involving the loss of money or data. Still, more than half (59%) have experienced other types of cyber incidents, most commonly email scams (31%), followed by text scams (26%), malware (26%), and phishing (26%). Despite relatively low reported incidence, concern remains high: nearly three-quarters (73%) are worried about artificial intelligence (AI)-related cybercrime, and more than half (56%) are worried about cybercrime overall. In addition, a strong minority think it is likely they will be affected by at least one of several cyber threats in the next year: a cyber threat causing their personal information to be compromised (26%), loss of files or photos (10%), or financial loss (9%).

When asked which cyber threats concern them most, identity theft tops the list, mentioned by 76% of online Canadians. This is followed by financial loss (64%) and viruses, spyware, or malware (59%). Smaller proportions cite privacy violations (48%), personal data loss (45%), ransom attacks (45%), and phishing scams (42%). Loss of information ranks lowest, identified by 37% as a top concern. Despite almost three-quarters (73%) reporting they feel confident they can identify phishing threats, 42% are concerned about phishing scams.

The majority of online Canadians report being somewhat (43%) or well (28%) prepared to face cyber threats. One-quarter (25%) said they feel unprepared. Among those feeling unprepared for a cyber threat, two main reasons were offered: lack of knowledge (not knowing where to obtain this information, not knowing the different threats, and not having straightforward information available) and futility (protecting themselves online is not possible).

Focusing on specific types of attacks, 4% have been a victim of a ransomware attack, 9% 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 26% think they are vulnerable to a ransomware attack. In addition, one-quarter (26%) have been a victim of a phishing scam and 8% have been a victim of a phishing scam where they have lost money or data.

Views on artificial intelligence

Sixty-two percent of online Canadians report using AI tools, such as ChatGPT, CoPilot, DALL-E: 32% use AI tools both at work and at home, 24% use them at home only, and 6% use them at work only. Four in 10 (42%) say they are confident in their ability to identify AI-generated messages, images, videos, or deepfakes, and an additional 30% say they are somewhat confident.

Communications and the Get Cyber Safe campaign

Three-quarters (75%) of online Canadians feel confident they could protect themselves online as long as they have trustworthy information on the steps to take. Two-thirds (67%) feel confident that they know how to find practical information to protect themselves online and over half (56%) feel they have enough information on how to take steps to protect against cyber threats.

In terms of communication preferences, 59% of online Canadians would prefer to get information to protect themselves from cyber threats via websites. This is followed by instructional videos (41%) and checklists outlining what to do (37%). Approximately one-third are interested in fact sheets or infographics (35%) or social media (33%).

Very few (4%) can name the Government of Canada cyber security awareness campaign unprompted. When prompted, one in 10 (10%) report awareness of Get Cyber Safe. Among those aware of the Get Cyber Safe campaign (n=223), just over one-third (37%) encountered it on social media. Roughly two in 10 saw an online video (24%), a news segment or newspaper coverage (22%), or heard about it through a radio show or podcast (22%). Smaller proportions visited the GetCyberSafe.ca website (17%) or heard about the campaign from someone else (12%).

Businesses and cyber security

Most business owners and managers (77%) say their company has taken some steps to protect itself against cyber threats. Half or more of those surveyed report that their business requires password protection on all devices (59%), keeps security software up to date on all machines (55%), and uses a password or user authentication for wireless and remote access (52%).

When it comes to protecting their company against cyber threats, approximately a third say their organization would benefit from guidelines for reacting to a cyberattack (36%), a list of the types of threats that exist and clues to look out for (36%), best practices for safe cloud computing (35%), or tips or resources for software or hardware to make networks secure (35%).

When thinking about the daily operations of their company, two in 10 business respondents are concerned about work disruptions (19%) and almost as many are concerned about financial loss (18%) or damage to the organization's reputation (17%). Sixteen percent are concerned about their company's data being held for ransom.

Two-thirds of companies are at least somewhat 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 MFA (55%), keeping operating systems, software, and apps updated (52%), backing up files (45%), using anti-virus software (42%), educating employees (35%), storing back-ups offline (34%), and limiting access to software (33%). Despite being somewhat prepared, half of business owners and managers anticipate that it would take some effort (38%) or would be difficult (13%) to recover from a ransomware attack.

Concluding observations

Overall, there has been very little change in online Canadian's knowledge and behaviours related to online security since the 2024 survey. The following observations are offered:

- *Use of protective behaviours remain stable.* A majority of online Canadians continue to take steps to protect their online accounts, social media accounts, devices, and networks. Most know how to install the latest software and app updates and report doing so regularly. Awareness of multi-factor authentication has increased, although the proportion using it is unchanged since 2024. Majorities say they check messages for signs of phishing very often or always, and more than half analyse the appearance of a website or check for "https:" to verify its legitimacy. These behaviours are unchanged over time. Finally, many online Canadians report using complex passwords and unique passwords for their important accounts most of the time.
- *Awareness and use of AI tools have increased.* There has been a significant increase compared to 2024 in the proportion of online Canadians who report using AI tools, with usage nearly doubling. The largest increase is among those who use AI tools both at work and at home. This likely reflects the rapid growth of the AI industry and broader acceptance of AI in workplace environments. Confidence

in identifying AI-generated content has also increased significantly, likely due to greater exposure and general awareness. Despite rising awareness and use, concern about AI-related cybercrime continues to trend upward.

- *Phishing remains a concern.* Although most online Canadians report checking messages for signs of phishing and consider themselves knowledgeable about how to identify phishing attempts, some continue to fall victim to scams involving the loss of money or personal information, and the proportion reporting an attack has increased over time. The persistent volume of spam messages, combined with advances in AI that enable increasingly sophisticated scams, may be contributing to this trend. Many online Canadians also remain concerned about phishing, and nearly one-third rely on others to help identify potential scams or phishing messages, underscoring the continued need for public education initiatives such as the Get Cyber Safe campaign.

Notes to reader

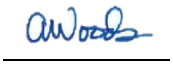
- Detailed findings are presented in the sections that follow. Results are presented in the main portion of the narrative and are typically supported by a graphic or tabular presentation of results.
- All results are expressed as percentages, unless otherwise noted. Throughout the report, percentages 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 with findings from similar surveys conducted in 2018, 2020, 2022, and 2024. Unless explicitly noted in the narrative, observed differences over time are not statistically significant.
- The survey questionnaire is appended to the report.

Contract value

The contract value was $79,075.00 (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.



Alethea Woods
President
Phoenix Strategic Perspectives Inc.

Survey Findings

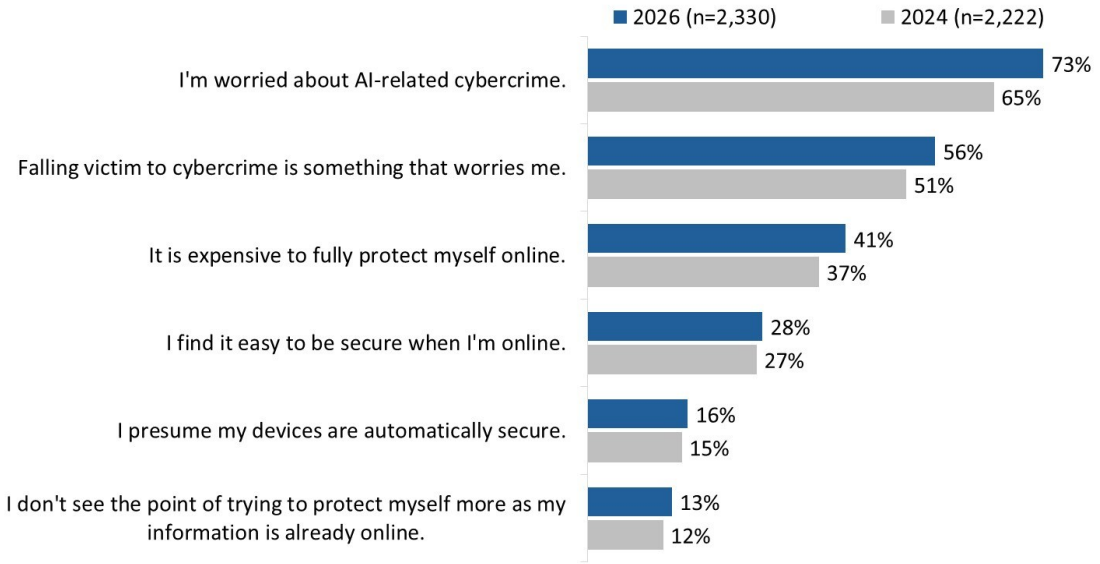
1. Views and attitudes towards cyber security

Majority of Canadians are worried about cybercrimes, and concern has increased since 2024

Respondents were asked to rate their level of agreement or disagreement with six cybersecurity statements using a 10-point scale, where '1' means strongly disagree and '10' means strongly agree. Nearly three-quarters (73%) of online Canadians report being worried about artificial intelligence (AI)-related cybercrime (scores of 7 to 10), up 8 percentage points from 2024 (65%). Just over half (56%) are worried about falling victim to cybercrime in general, also up from 51% in 2024.

Views on personal cybersecurity behaviours are generally consistent with 2024. Four in 10 (41%, up slightly from 37% in 2024) think it is expensive to fully protect themselves online, and roughly three in 10 (28%) say it is easy to be secure online. Relatively few assume their devices are automatically secure (16%) or feel there is no point in protecting their information because it is already online (13%).

Figure 1: Attitudes toward online security: % agreeing with each statement



QSC1. How much do you agree with the following statements about online security? Base: all respondents.

Notable subgroup differences include the following:

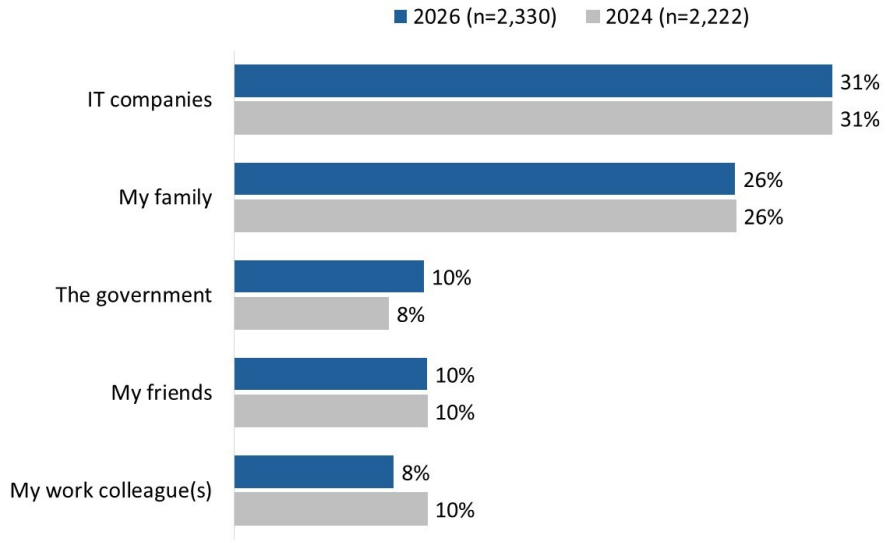
- As age increases, so does concern about falling victim to a cybercrime. Those 18 to 34 are more likely than older Canadians to feel it is unlikely that they will be a target of cybercrime and to find it easy to be secure online.
- Millennials and Gen X respondents are more likely to say that family members rely on them to keep secure online.
- Women are more likely than men to be concerned about AI being used for cybercrime. In contrast, men are more likely than women to feel it is easy to be secure online, and that family members rely on them to keep them secure online.

- Those with a basic or novice level of knowledge are 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, and to worry about becoming a victim of a cybercrime.

Main sources of cyber security advice are largely unchanged from 2024

Online Canadians continue to rely most on IT companies (31%) and family members (26%) for cybersecurity help or advice. Two in 10 rely on the government (10%) or friends (10%), while fewer than one in 10 (8%) turn to work colleagues.

Figure 2: Source of cyber security support



QSC2. Who do you rely on most for cyber security help or advice? Base: all respondents.

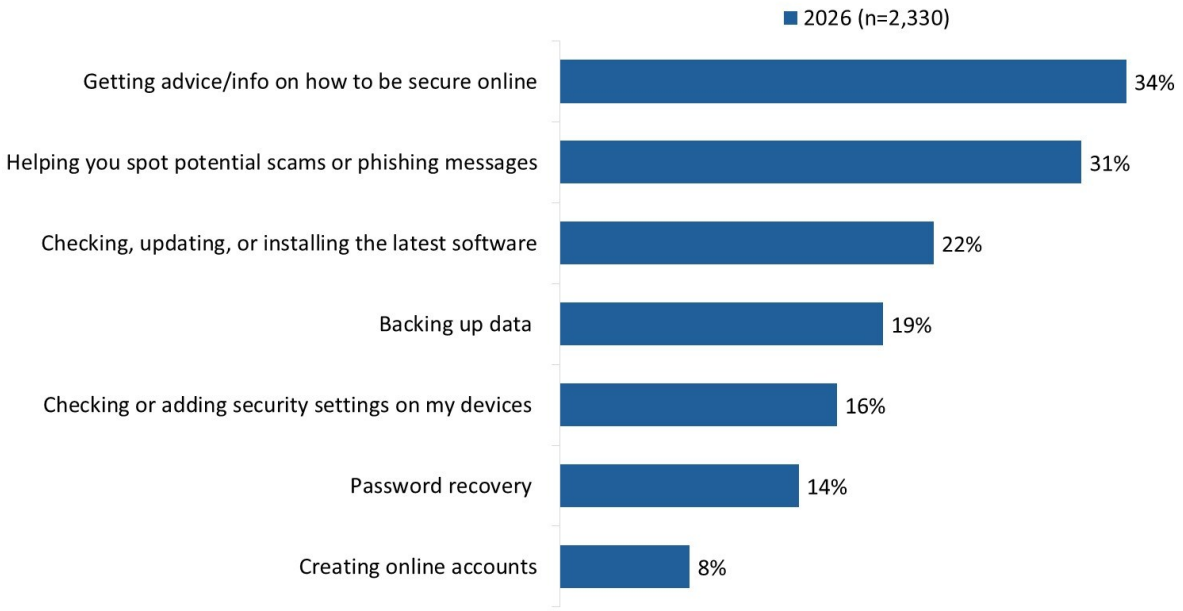
Those aged 65 and older are the most likely to report that they rely on their family for cyber security help or advice, while those aged 18 to 34 are the most likely to rely on friends for such advice. Residents of Quebec are most likely to rely on the Government for cyber security help or advice, while those with a basic or beginner level of knowledge about online security are more likely to rely on their family. Men are more likely to rely on friends and IT companies, while women are more likely to rely on their family.

Canadians rely on other people for help with a variety of online activities

Approximately a third of online Canadians rely on others for advice and information on how to be secure online (34%) and for helping spot potential scams or phishing messages (31%). In addition, 22% rely on others for checking, updating or installing software updates, 19% for backing up their data, 16% for checking or adding security settings to their devices, and 14% for password recovery. Fewer than one in 10 (8%) require support when creating online accounts.

Reliance on others for cyber security tasks varies across demographic groups. Older respondents are more likely to rely on others for support, with Baby Boomers and the Silent Generation showing greater reliance than Gen Z, Millennials, and Gen X. Women are also more likely than men to report relying on others for help. In contrast, those with more advanced knowledge of online security are less likely to depend on others to perform these tasks.

Figure 3: Activities for which support is needed

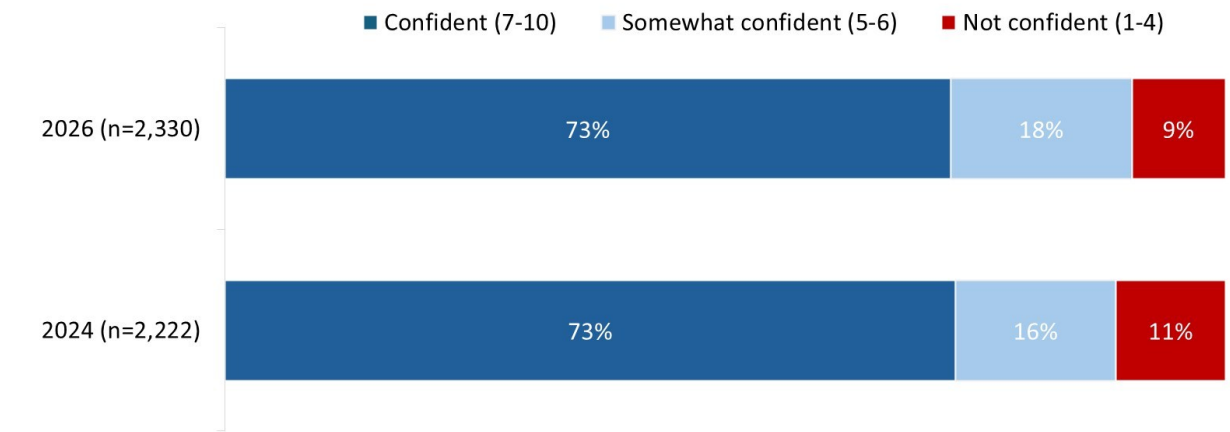


QCS3. For which of the following do you rely on other people for help (e.g., family, friends, or colleagues)? [Multiple responses accepted] Base: all respondents.

Canadians' confidence in spotting scam messages remains high

Nearly three-quarters (73%) of online Canadians are confident in their ability to identify a phishing message or malicious link, while 18% are somewhat confident. This represents no change from 2024. Only 9% report lacking confidence in their ability 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: all respondents.

Confidence in identifying phishing messages or malicious links varies across demographic groups. Younger respondents, particularly Gen Z and Millennials, report higher confidence than Baby Boomers and the Silent Generation. Men are more likely than women to report confidence, and confidence increases with

household income. Those who are always connected and those with more advanced cyber security knowledge are also more likely to feel confident identifying phishing attempts.

2. Cyber security measures

Precautions to protect online accounts remain common despite a slight decline

Most online Canadians report taking precautions to protect their online accounts and devices (84%). This reflects a gradual decline over time, down from 89% in 2018 to 84% in 2026.

Figure 5: % taking security precautions

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

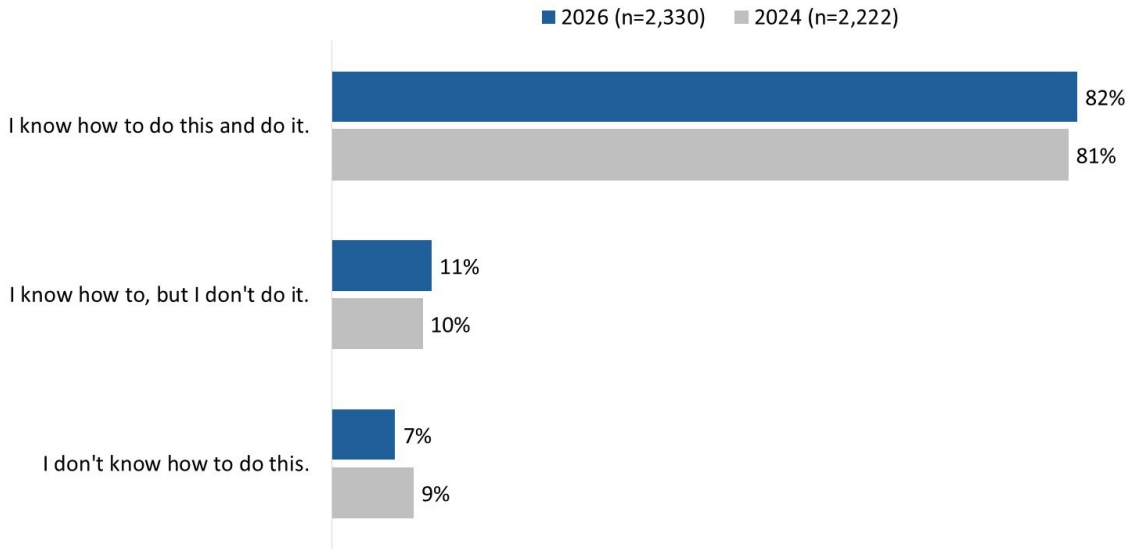
The likelihood of taking precautions to protect online accounts, social media accounts, devices, or networks is higher among residents of Atlantic Canada, Ontario, Alberta, and British Columbia (including the Territories) compared with residents of Quebec. It is also higher among Millennials compared with Gen Z, men, those with a college or university education compared with those with a high school education or less, and individuals earning $100,000 or more annually.

Majority of online Canadians install software and app updates

Beyond taking precautions to protect their online accounts, eight in 10 Canadians (82%) know how to install the latest software and app updates across their devices and do so. Another 11% know how to install these updates but do not do so, while just 7% report not knowing how. Results are consistent with 2024.

Older Canadians, particularly those aged 65 and older, women, those with a high school education or less or a college education, and individuals with basic or beginner-level online security knowledge are more likely to report not knowing how to do this.

Figure 6: Knowledge of installing latest software or app updates

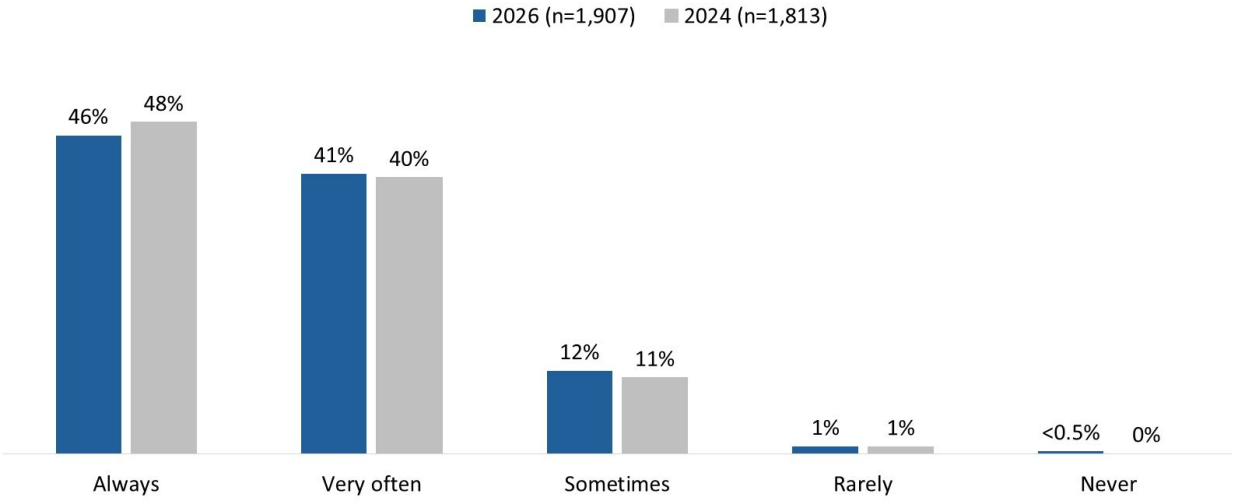


QBEH2. Do you know how to install the latest software and app updates across your devices (e.g., computer and mobile phone)?
Base: all respondents.

Regular installation of software and application updates remains widespread

Among respondents who know how to install the latest software and app updates (n=1,907), a large majority (87%) do so regularly, including 46% who say they always install updates when notified. Smaller proportions report installing updates only sometimes (12%) or rarely (1%). These results are virtually unchanged from 2024.

Figure 7: Frequency of installing latest software or app updates



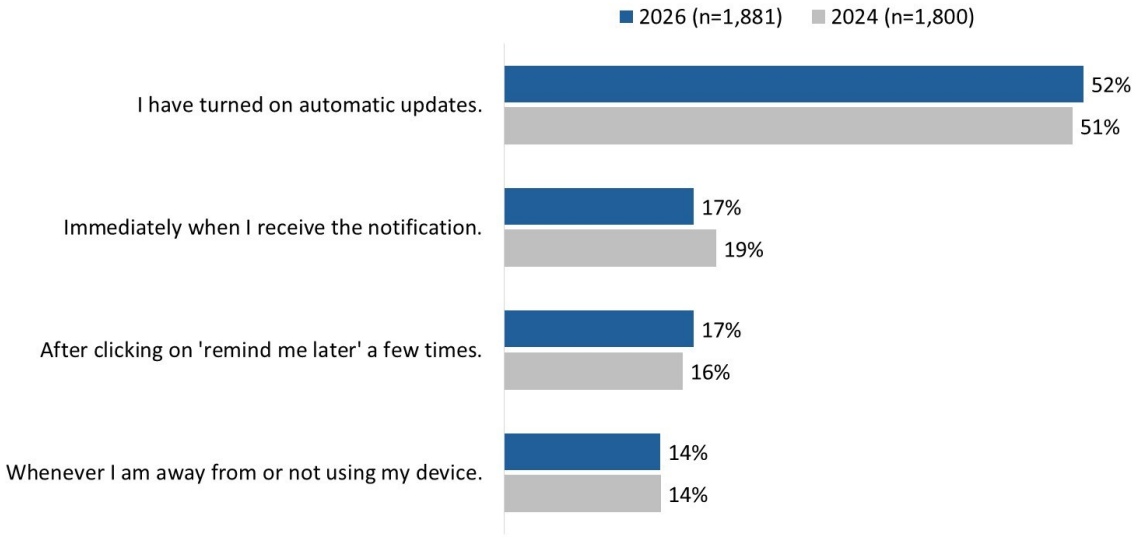
QBEH3. How often do you install the latest software or application updates to your devices when notified that they are available?
Base: those who know how to install and do it.

The likelihood of 'always' installing the latest software or application updates when notified increases with age and is highest among those with advanced online security knowledge. Gen Z is the least likely to always install updates.

Immediate installation of updates is common among online Canadians

Among those who often install software updates (n=1,881), 69% do so immediately, including 52% with automatic updates enabled and 17% who install updates upon notification. Among the rest, 17% delay updates after selecting "remind me later," and 14% update only when not using their device. Results are virtually unchanged from 2024.

Figure 8: Typical timing for installing software updates



QBEH4. When do you typically install software updates on your devices? Base: those who install updates often.

Use of automatic updates increases with age. Canadians aged 55 and older are more likely than younger Canadians to install updates immediately upon notification. Gen Z is most likely to delay updates by selecting "remind me later," while Gen Z and Millennials are more likely than older generations to install updates when away from their device.

Most online Canadians know about MFA and use it regularly

Awareness of multi-factor authentication (MFA) has increased 4 percentage points, from 90% in 2024 to 94% in 2026.

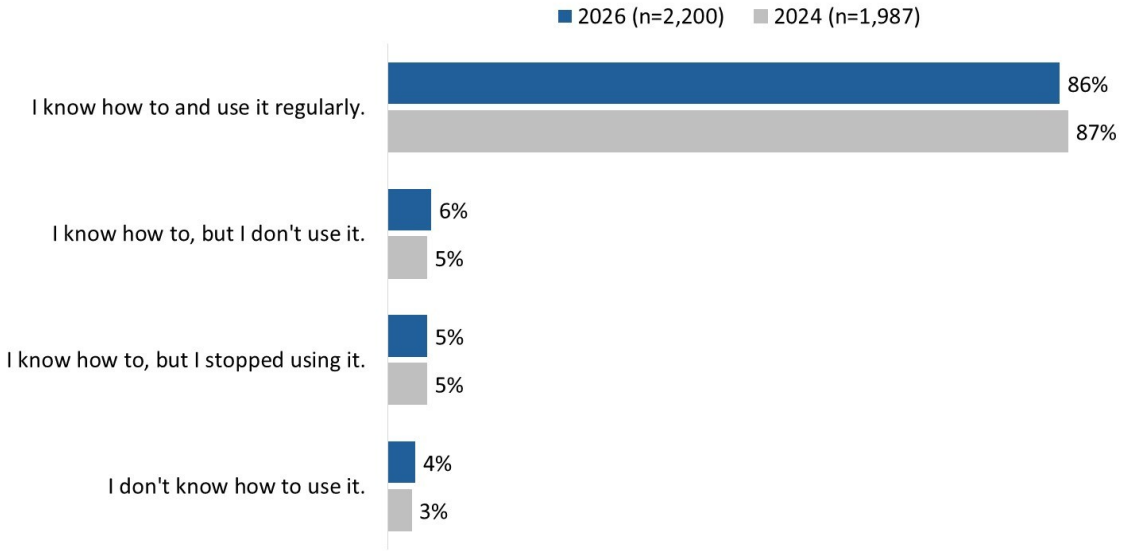
Figure 9: Awareness of MFA: % that have heard of MFA

QBEH6. Have you ever heard of multi-factor authentication (MFA)? Base: all respondents.

Awareness of MFA is higher among Gen Z, Millennials and Gen X, and lower among residents of Quebec and those with a basic or beginner level of online security knowledge.

Eighty-six percent of online Canadians aware of MFA (n=2,200) know how to use it and do so regularly. A further 11% know how to use MFA but do not use it (6%) or have stopped using it (5%). Very few (4%) indicated they do not know how to use MFA. These results are virtually unchanged from 2024.

Figure 10: Ability use to MFA



QBEH7. Do you know how to use multi-factor authentication (MFA)? Base: those who have heard of MFA.

Millennials are the most likely to know how to use MFA and to use it regularly, while Baby Boomers and the Silent Generation are less likely to do so. Use of MFA also increases with education, and those with advanced online security knowledge are the most likely to report familiarity with and regular use.

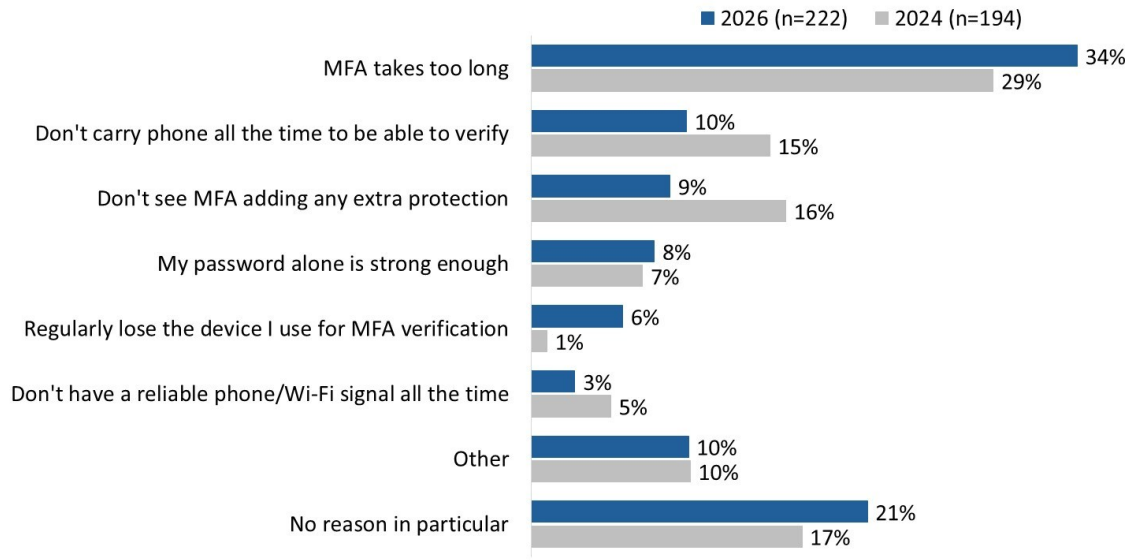
Variety of reasons for not or no longer using MFA

Those who do not, or no longer, use multi-factor authentication (n=222) attribute their lack of use to a variety of reasons. The reason mentioned by the single largest proportion (34%, up from 29% in 2024) is that multi-factor authentication takes too long. Following this, 10% do not carry their phone with them all the time to be able to verify (down from 15% in 2024), 9% do not think MFA adds any extra protection (down from 16%), and 8% think their password alone is strong enough.

Reasons offered by smaller proportions included regularly losing the device set up for multi-factor authentication (6%) and not having a reliable phone or Wi-Fi signal all the time (3%).

Two in 10 (21%) have no reason in particular for not or no longer using multi-factor authentication.

Figure 11: Main reason for not using MFA

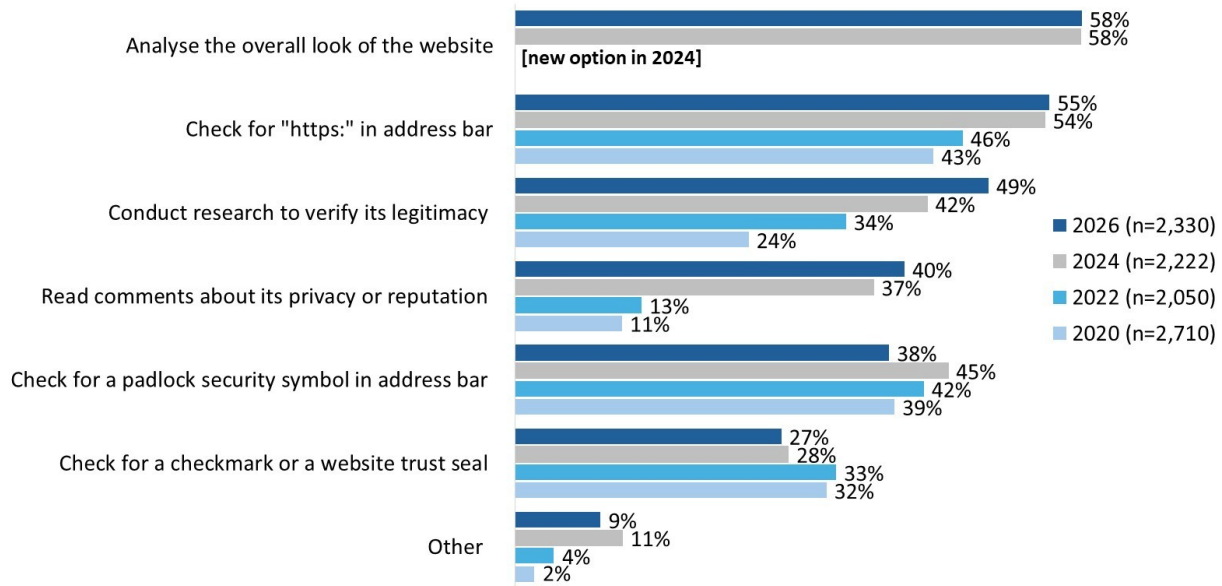


QBEH8. What is the main reason you don't use (or stopped using) multi-factor authentication (MFA)? Base: those who know how to use MFA but choose not to.

Online Canadians use a variety of strategies to verify a website

To verify a website is legitimate, almost six in 10 (58%) online Canadians analyse the overall look of the website; this is unchanged from 2024. Additionally, 55% check for "https:" in the address bar and approximately half (49%, up from 42% in 2024) conduct research to verify its legitimacy. Four in 10 (40%, up from 37% in 2024) read comments about the website's privacy or reputation and almost as many (38%, down from 45% in 2024) check for a padlock security symbol in the address. Just over one-quarter (27%) check for a checkmark or a website trust seal.

Figure 12: Steps to verify website is secure



QBEH12. What steps do you take to verify that a website is legitimate? Base: all respondents.

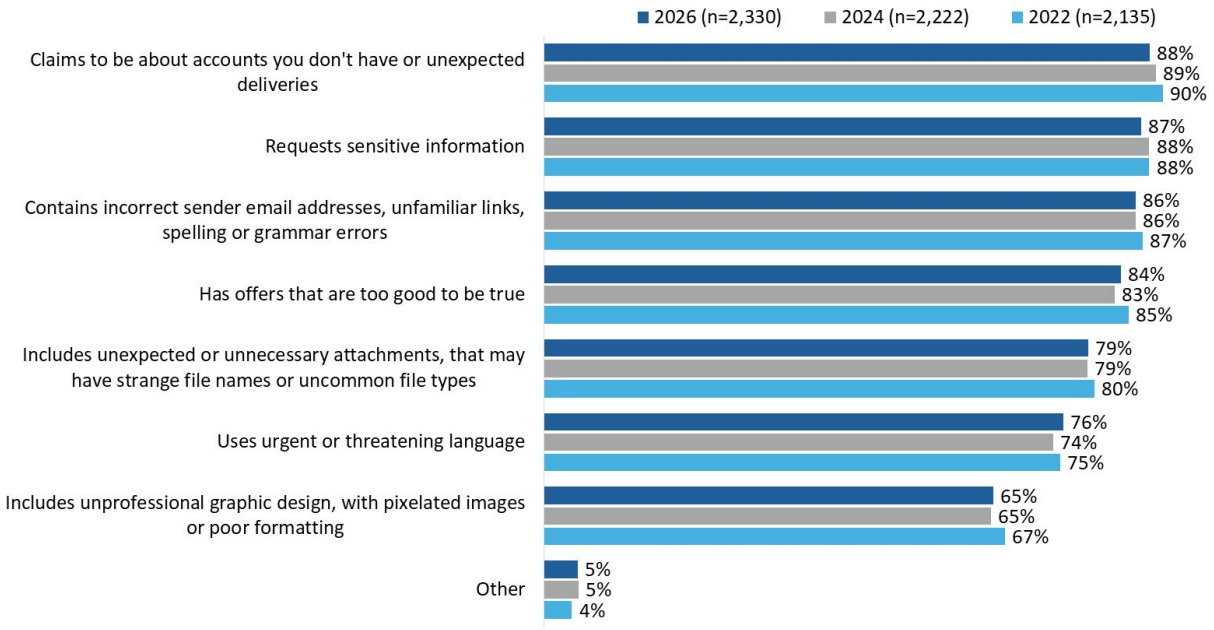
Canadians age 65 and older are generally less likely than younger Canadians to take steps to verify that a website is legitimate. Conversely, those with advanced knowledge of online security are more likely to take all of these steps to verify the legitimacy of a website.

Most online Canadians generally recognize the signs of phishing messages

The vast majority of online Canadians recognize common signs of phishing. Most identify claims about accounts they do not have or unexpected deliveries (88%), requests for sensitive information (87%), and messages containing incorrect email addresses, unfamiliar links, or spelling or grammar errors (86%). Nearly as many recognize offers that seem too good to be true (84%) and unexpected or unnecessary attachments (79%) as phishing indicators. Three-quarters (76%) identify urgent or threatening language as a sign of phishing, while 65% point to unprofessional graphic design.

Knowledge has been consistent since 2022.

Figure 13: Knowledge of phishing signs



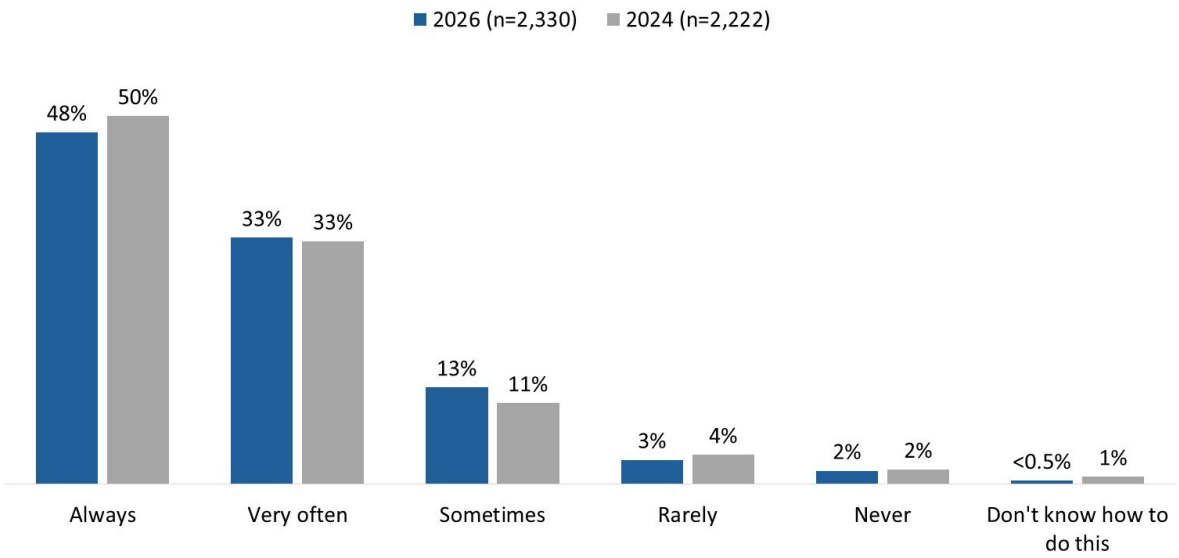
QBEH13. As far as you know, what are signs of phishing? Base: all respondents.

Millennials are among the most likely to recognize common signs of phishing, while the Silent Generation is less likely to do so. Recognition of phishing signs increases with education and household income and is highest among those with intermediate or advanced online security knowledge.

Phishing vigilance remains high among online Canadians

Most online Canadians check messages for signs of phishing before clicking links or responding. Nearly half always do so (48%), and another third do so very often (33%). A further 13% check some of the time, while very few (5%) say they rarely or never do so. These results are virtually unchanged from 2024.

Figure 14: Frequency of checking messages for signs of phishing



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.

The following groups are more likely to report that they 'always' check messages for signs of phishing: residents of Ontario and Alberta compared to Quebec, those under the age of 65, and Millennials compared to Gen Z, Baby Boomers and the Silent Generation. Additionally, those with advanced knowledge of online security and those always connected to the internet are more likely to always check messages for signs of phishing.

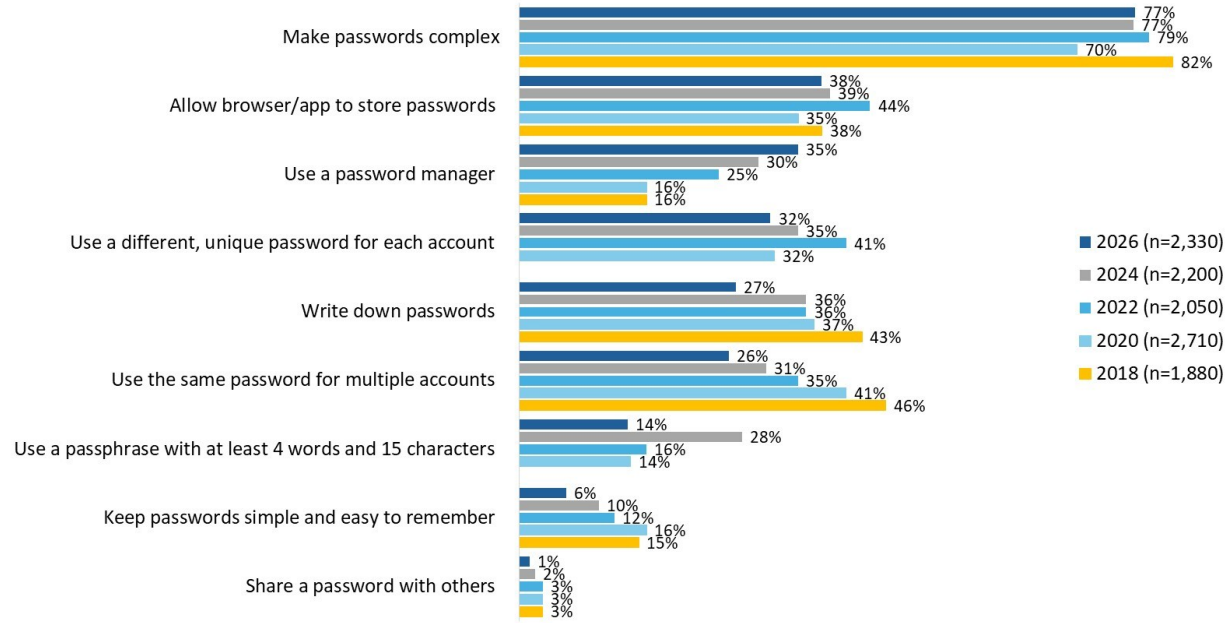
Three-quarters make their passwords complex; some have habits that put them at risk

Over three-quarters (77%) of online Canadians report creating complex passwords using a combination of letters, numbers, and symbols. Smaller proportions use a password manager (35%, up from 30% in 2024), a different, unique password for each account (32%, down from 35%), and a passphrase with at least four words and 15 characters (14%, down from 28%).

Some respondents report behaviours that may increase account vulnerability. For example, 38% allow browsers or apps to store passwords, 27% (down from 36% in 2024) write down their passwords, 26% (down from 31%) reuse passwords across multiple accounts, 6% (down from 10%) keep passwords simple and easy to remember, and 1% report sharing their passwords.

When comparing year-over-year, complex passwords remain the most common practice, while several higher-risk behaviours, such as writing down or reusing passwords, have declined compared with 2024.

Figure 15: Actions taken with passwords



QBEH15. When it comes to your passwords, which of the following actions do you take? Base: all respondents.

Password behaviours vary systematically by age. Canadians aged 18 to 44 are more likely to rely on convenience behaviours, such as storing passwords in browsers or apps, using password managers, and reusing passwords. Those aged 35 to 64 are most likely to use complex passwords, while Canadians aged 65 and older are most likely to write passwords down.

Turning to gender, men are more likely to use a password manager and unique passwords, while women are more likely to write their password down and choose to use a passkey, when available, in place of a password.

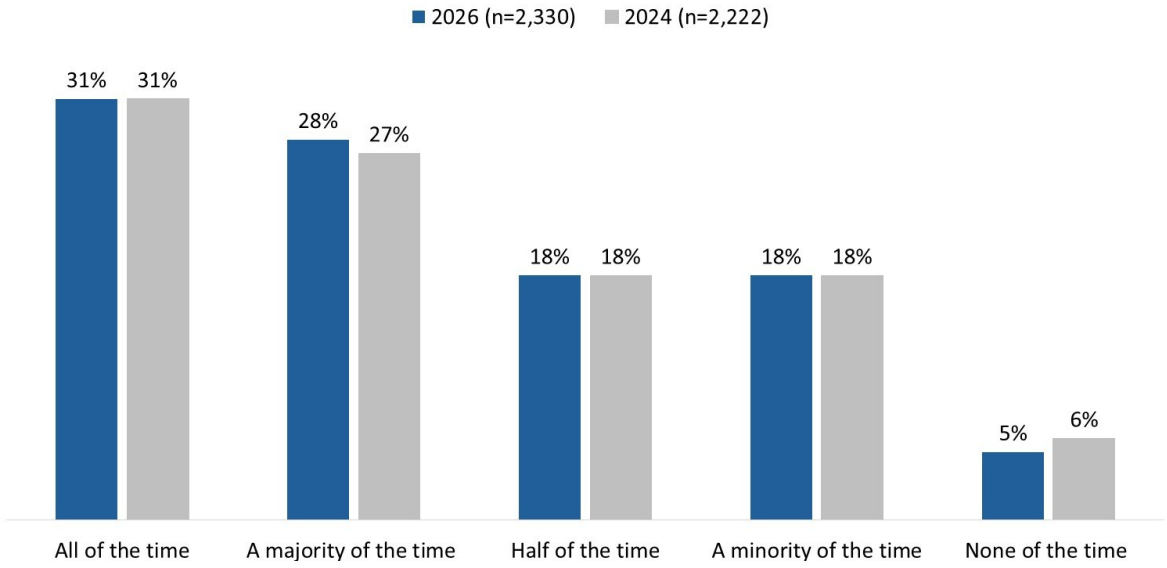
Other noteworthy subgroup differences include the following:

- The likelihood of using a password manager as well as choosing to use a passkey increases with household income.
- University graduates are more likely to use complex passwords.
- Parents are more likely to use a password with four to 15 characters, but they are less likely to use a different password for each account.

Most Canadians use unique passwords at least some of the time

Half of online Canadians report using unique passwords for their important online accounts ‘all of the time’ (31%) or a ‘majority of the time’ (28%). A further one-third do so ‘half of the time’ (18%) or a ‘minority of the time’ (18%). Very few (5%) say they do not use unique passwords. Results are virtually unchanged from 2024.

Figure 16: Frequency of using unique passwords



QBEH17. How often do you use unique passwords for your important online accounts (e.g., emails, social media, payment-related sites)? Base: all respondents.

Gen Z is less likely to use unique passwords 'all of the time' or a 'majority of the time', while men and those with advanced knowledge of online security are more likely to use unique passwords all of the time'.

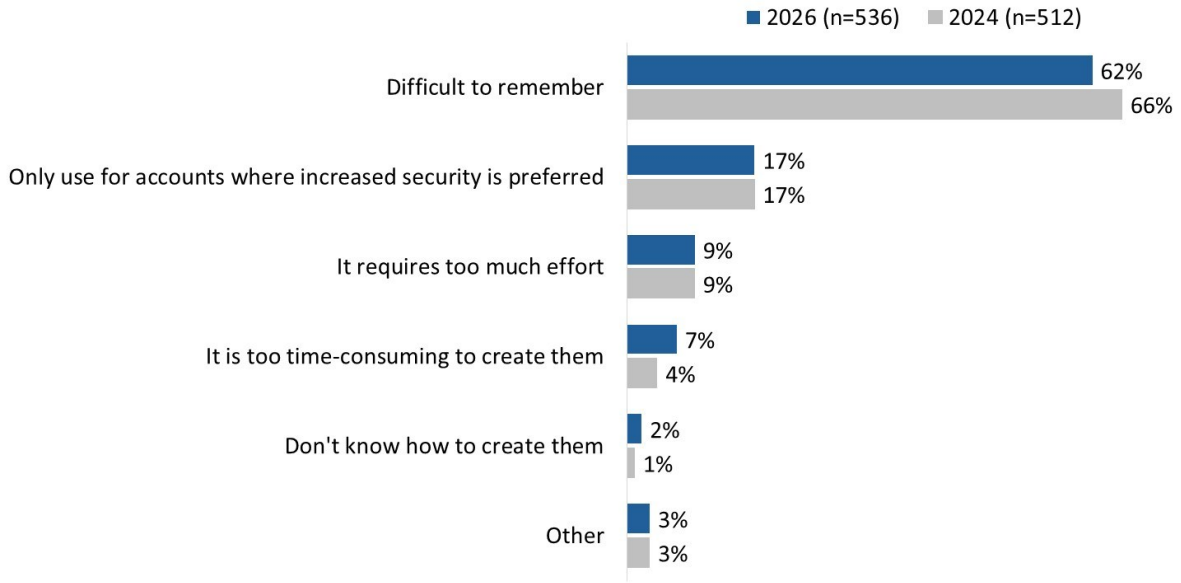
Avoiding having to remember passwords is the main reason Canadians reuse them

Among those who rarely, if ever, use unique passwords (n=536), roughly six in 10 (62%) say this is because they find it difficult to remember different passwords. Others cite effort (9%), the time required to create them (7%), or not knowing how (2%). Seventeen percent report using unique passwords only for accounts where stronger security is needed.

Results are largely consistent with 2024, with a slight decrease in those citing difficulty remembering passwords (66% to 62%) and a slight increase in those saying unique passwords are too time-consuming to create (4% to 7%).

Online Canadians from Quebec are more likely than those from Ontario, Alberta and British Columbia, including the Territories, to only use unique passwords for accounts where they want increased security. Women are more likely than men to rarely use unique passwords because they are difficult to remember.

Figure 17: Main reason for not using unique passwords

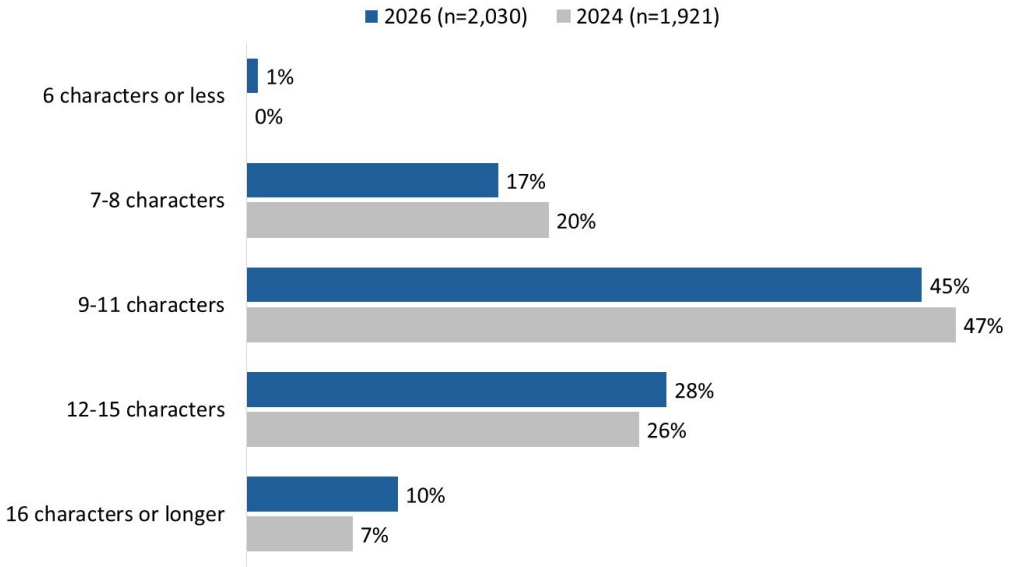


QBEH18. What is the main reason you rarely, if at all, use unique passwords for your online accounts? Base: those who do not create unique passwords.

Most online Canadians use mid-length passwords, with some using longer ones

Password length varies, with roughly six in 10 reporting passwords between seven and eight characters (17%) or nine and 11 characters (45%). Among the rest, nearly four in 10 use longer passwords, including 28% with 12 to 15 characters and 10% with 16 or more characters. Use of passwords with at least 12 characters has increased slightly since 2024.

Figure 18: Length of passwords

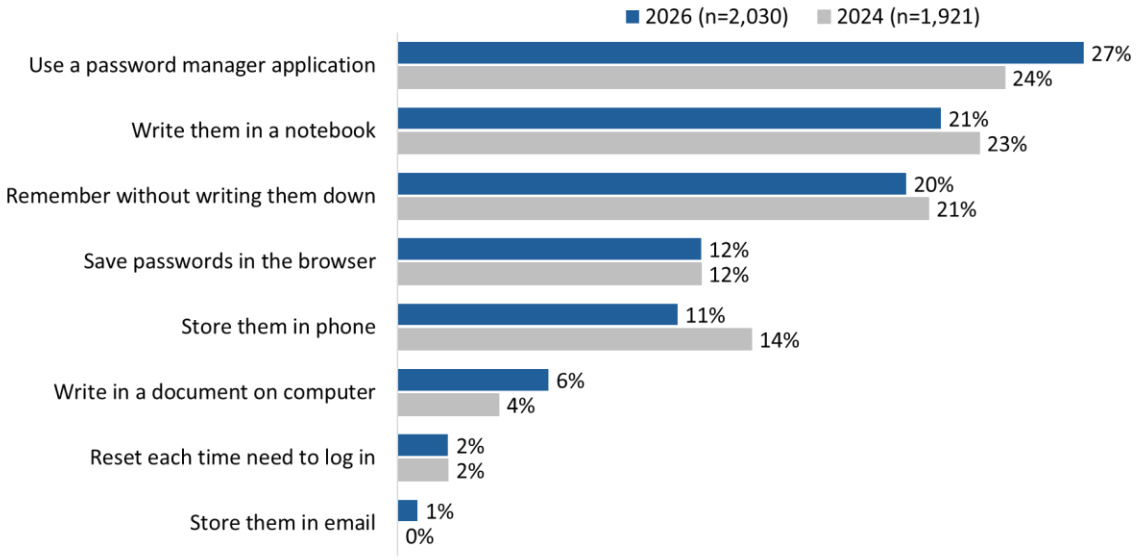


QBEH21. How long are the password(s) you usually create? Base: those who are not business respondents.

Preferred method of remembering passwords varies

Approximately a quarter (27%, up from 24% in 2024) use a password manager application to manage multiple passwords. Smaller proportions report writing them down in a notebook (21%) or remembering them without writing them down (20%).

Figure 19: Preferred method of remembering passwords



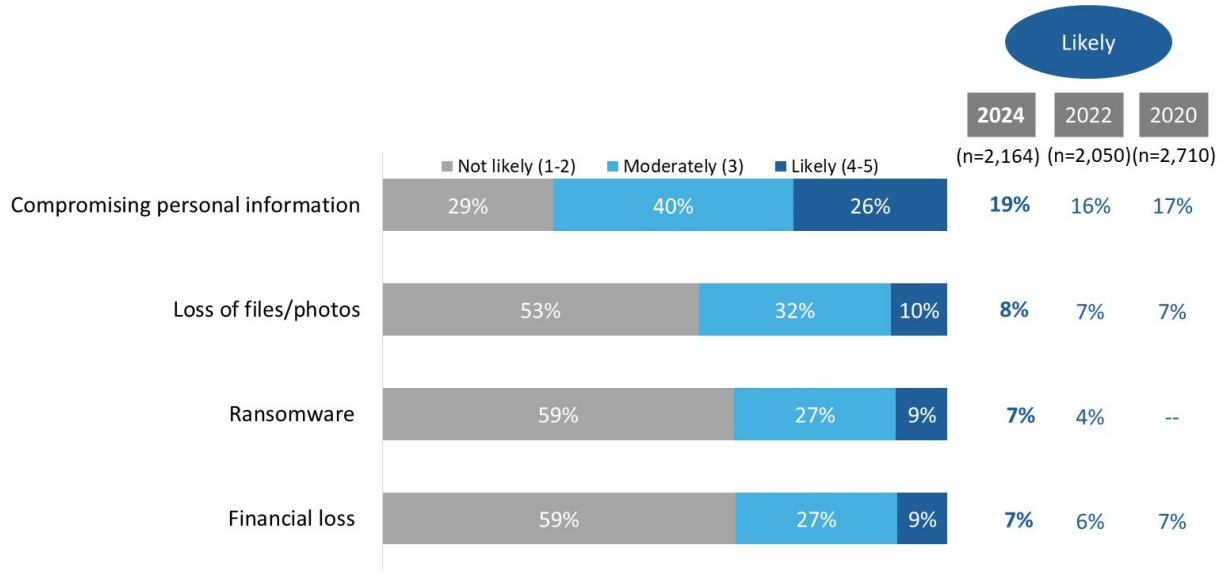
QBEH22. What is your preferred method of remembering multiple passwords? Base: those who are not business respondents.

3. Cyber threats

A third of online Canadians think they're likely to be affected by a cyber threat

One-third (33%) of online Canadians think it is likely they will be affected by at least one of four cyber threats over the next year (compared to 8% in 2022 and 24% in 2024). One-quarter of online Canadians (26%; up from 19% in 2024) think it is likely that they will be affected by a cyber threat causing their personal information to be compromised. Similar to previous years, few believe they will experience a threat that results in the loss of files or photos (10%), having their data held for ransom (9%), or financial loss (9%).

Figure 20: Likelihood of being affected by various threats



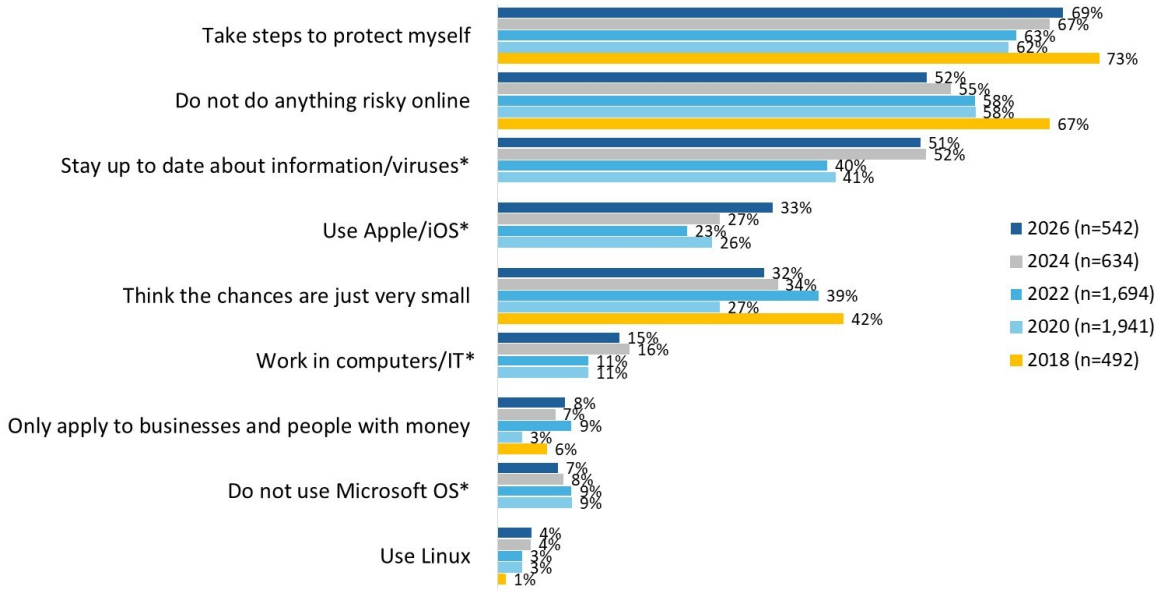
QCT1. In the next year, how likely do you think it is that you will be affected by a cyber threat ...? Base: all respondents.

The likelihood of believing they would not be affected by cyber threats increases as age decreases. A similar pattern is observed among those with advanced online security knowledge, who are also more likely to hold this view.

Those who feel at low risk of cyber threats cite their actions and online behaviour

Among those who feel unlikely to be affected by a cyber threat (n=542), most attribute this to protective behaviours, such as the steps they take to protect themselves online (69%), avoiding risky online behaviour (52%, down from 55% in 2024), and staying up to date on information about threats and viruses (51%). About one-third also cite using Apple/iOS (33%, up from 27% in 2024) or believing the chances are simply very small (32%). The full range of reasons is shown in Figure 21.

Figure 21: Reasons cyber threat is viewed as unlikely



*Not a response option in 2018.

QCT2. Why don't you think it is likely that you will be affected by a cyber threat? Base: those who think they are unlikely to be affected by a Cyber threat [Multiple responses accepted].

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

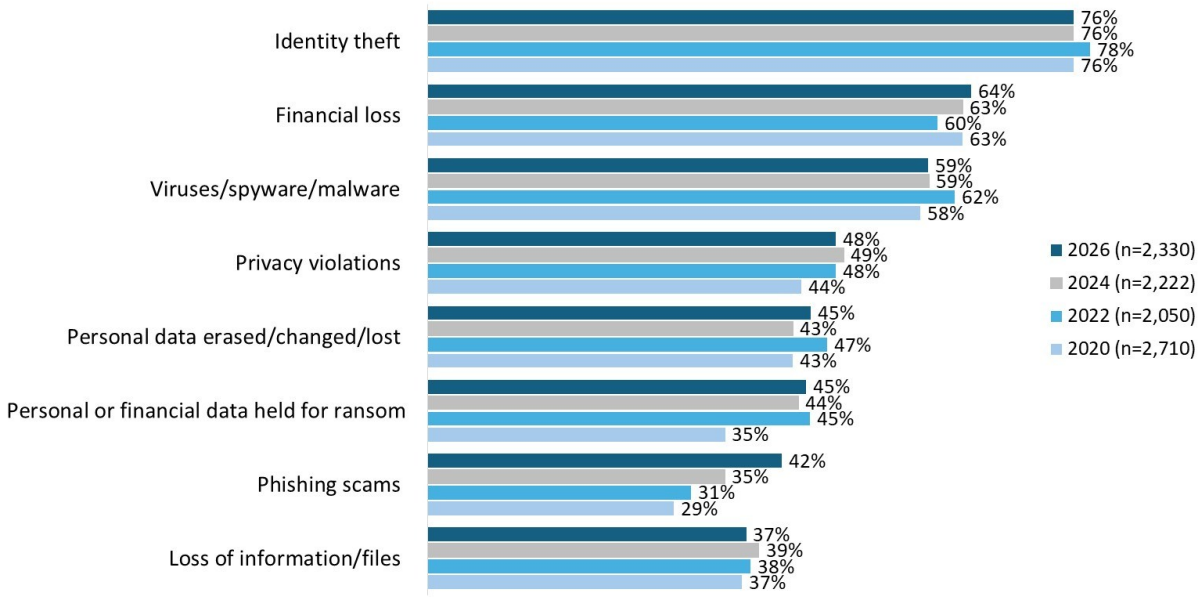
Three-quarters (76%) of online Canadians express concern about identity theft. This is followed by financial loss (64%) and viruses, spyware, or malware (59%). Roughly half (48%) are concerned about privacy violations, 45% about personal data or ransom attacks, and 42% about phishing scams. A little over one-third (37%) are most concerned about information or file loss.

Overall, results have remained relatively stable, with most measures changing by no more than three percentage points between 2024 and 2026. One exception is concern about phishing scams, which has continued to increase over time, from 29% in 2020 to 42% in 2026.

Noteworthy subgroup differences include the following:

- Respondents aged 45+ are more likely than younger online Canadians to be concerned about phishing scams as well as viruses, spyware or malware. Online Canadians 18- to 34-year-olds are less likely to be concerned about identity theft and more apt to be concerned about privacy violations.
- Concern about privacy violations, financial loss, and loss of information, files or personal data is higher among women.
- The likelihood of being concerned about privacy violations is higher among those from households reporting an annual income of under $40,000.
- Concern about identity theft and financial loss increase with education levels.
- Those who reside in Quebec are the most likely to be concerned about identity theft, while concern about viruses, spyware and malware is generally higher among residents of Ontario and British Columbia, including the Territories.

Figure 22: Top cyber threat concerns

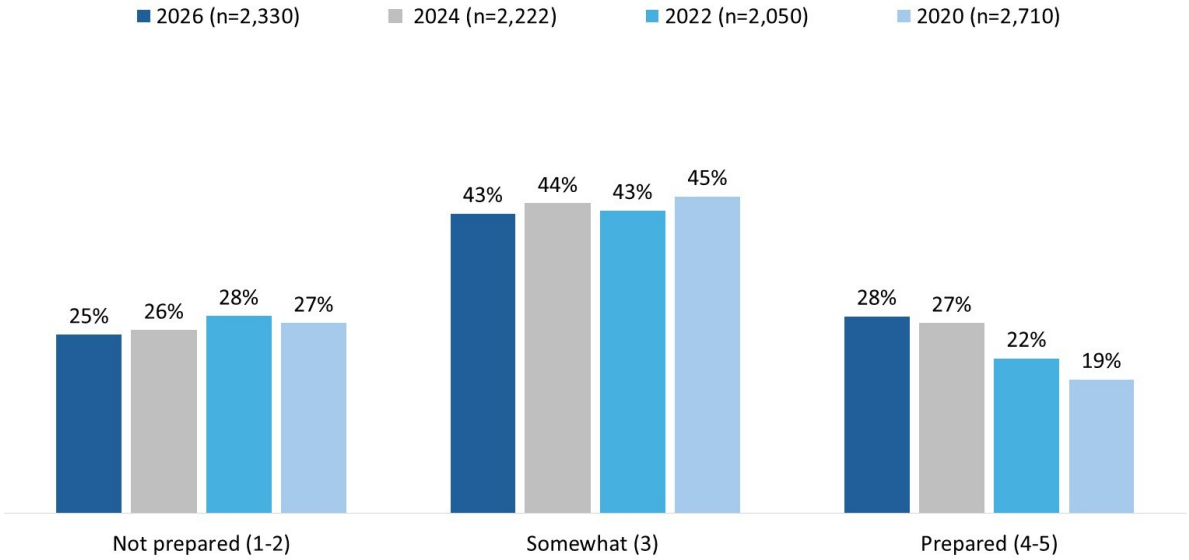


QCT3. What kinds of cyber threats are you most concerned about? Base: all respondents [Multiple responses accepted].

Most feel at least somewhat prepared to face cyber threats

A majority of online Canadians report feeling somewhat prepared (43%) or well prepared (28%). One-quarter say they feel unprepared. The proportion that feels well prepared has increased gradually, from 19% in 2020 to 28% in 2026.

Figure 23: Cyber threat preparedness



QCT4. How well prepared are you to face cyber threats? Base: all respondents.

Residents of Quebec are more likely than those in most other parts of Canada to feel unprepared to face cyber threats (except in Saskatchewan and Manitoba). This perception is also more common among

individuals earning under $100,000 annually, women, and those with basic or novice online security knowledge.

Lack of information is the top reason for feeling unprepared for cyber threats

Among those who feel unprepared to handle a cyber threat (n=574), the top reasons are not knowing where to find information (42%, up from 39% in 2024) and the belief that you can never fully protect yourself online (38%). Other reasons include lack of time (30%), limited knowledge of threat types (27%), and information that is not straightforward (21%). See Figure 24 for the full list of reasons.

Compared with the 2020 baseline, lack of knowledge about where to find information has increased steadily, from 23% to 42% by 2026. Over the same period, the perception that you can never fully protect yourself online has gradually declined, from 44% to 38%.

Figure 24: Reasons for feeling unprepared for cyber threats

QCT5. Why do you feel not prepared to face cyber threats? Base: those not prepared for cyber threats [Multiple responses accepted].

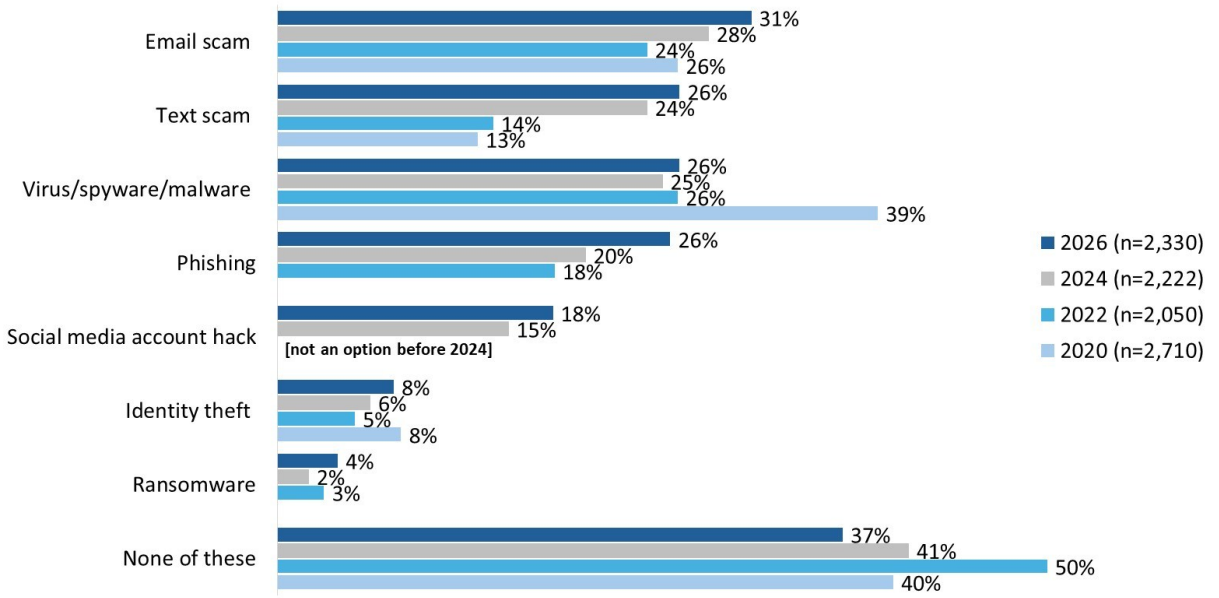
Reasons for feeling unprepared vary by demographic group. Gen Z is most likely to attribute their lack of preparedness to the belief that cyber threats are unlikely to affect them. In contrast, respondents aged 65 and older are more likely than younger Canadians to cite resource or knowledge gaps, including difficulty finding clear information, not knowing where to obtain guidance, and limited knowledge of different types of threats. Women are also more likely to say they feel unprepared because they do not know where to find information on steps to take.

Email scams remain the most common cyber incident among online Canadians

The most common types of cyber incidents reported by online Canadians are email scams (31%), followed by text scams (26%), malware attacks (26%), and phishing scams (26%). Eighteen percent report experiencing a social media account hack, while relatively few have experienced identity theft (8%) or a ransomware attack (4%).

Over time, more online Canadians report having experienced cyber attacks, with fewer saying they have experienced none of these types of incidents (37% in 2026, compared with 41% in 2024 and 50% in 2022). The most notable change is the increase in phishing attacks, rising from 18% in 2022 to 26% in 2026. By contrast, the proportion of online Canadians reporting a virus, spyware, or malware attack remains below the baseline observed in the initial survey, when 39% reported this type of incident.

Figure 25: Experience with cyber attacks



QCT6. Have you ever been a victim of any of the following cyber attacks? Base: all respondents [Multiple responses accepted].

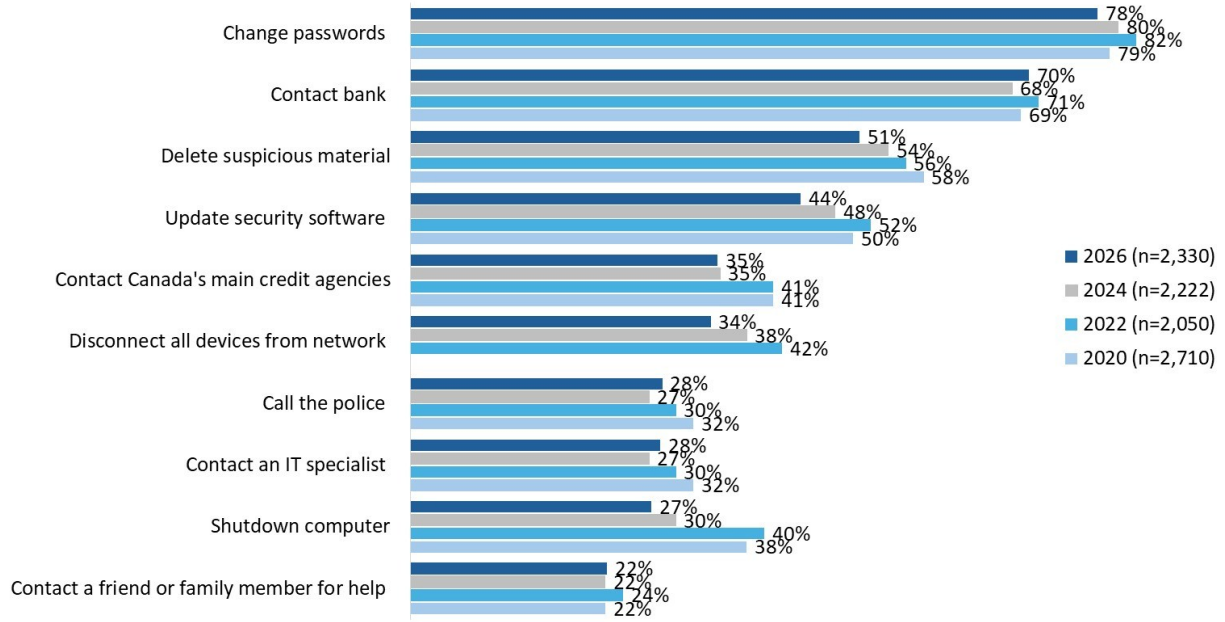
Regional and demographic differences are observed in reported experiences with cyber attacks. Residents of Quebec are more likely than those elsewhere in Canada to report having been a victim of an email scam. Older Canadians, particularly those aged 55 and older, are more likely to report email scams and phishing. Men are more likely to report experiencing virus, spyware, malware, or ransomware attacks. In contrast, Canadians with advanced online security knowledge are more likely to report never having experienced any of these types of cyberattacks.

Top responses to a cyber attack continue to be changing passwords and contacting the bank

If respondents knew or suspected they had been a victim of a cyber attack, most say they would take protective action. The most common responses include changing passwords (78%), contacting their bank (70%), and deleting suspicious material (51%). Smaller proportions say they would update security software (44%), contact Canada's main credit agencies (35%), or disconnect devices from their network (34%). About a quarter would call the police (28%), contact an IT specialist (28%), or shut down their computer (27%). Two in 10 (22%) say they would seek help from a friend or family member.

Over time, the steps that would be taken by online Canadians to protect themselves have remained relatively stable.

Figure 26: Responses to a cyber attack



QCT7. If you knew or suspected that you'd been a victim of a cyber attack, what steps would you take to protect yourself? Base: all respondents [Multiple responses accepted].

Notable subgroup differences include the following:

- Residents of Quebec are more likely than those living elsewhere in the country to contact Canada's main credit agencies.
- Online Canadians aged 65+ are more likely than younger Canadians to shutdown their computer and delete the suspicious material.
- Women are more likely than men to turn to a third party for help—specifically, contacting their bank, an IT specialist, or a friend or family member.

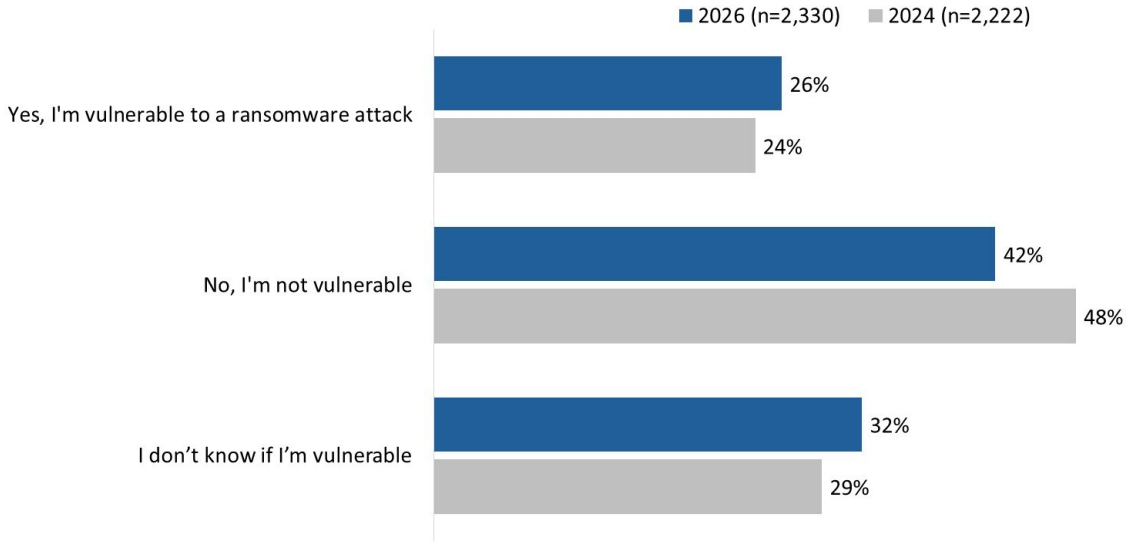
One-quarter believe they are vulnerable to a ransomware attack

One-quarter (26%) of online Canadians think they are vulnerable to a ransomware attack, while 42% feel they are not vulnerable (down from 48% in 2024). The rest (32%) do not know if they are vulnerable to a ransomware attack.

Perceived vulnerability to ransomware attacks differs across groups. Higher vulnerability is reported among residents of Saskatchewan and Manitoba (versus Atlantic Canada, Quebec, and British Columbia including the Territories), Gen X, men, and business owners. Those with advanced online security knowledge are more likely to believe they are not vulnerable.

Canadians aged 35 to 64 are more likely than younger Canadians to feel vulnerable, while those aged 65 and older are most likely to say they are unsure whether they are vulnerable.

Figure 27: Vulnerability to a ransomware attack

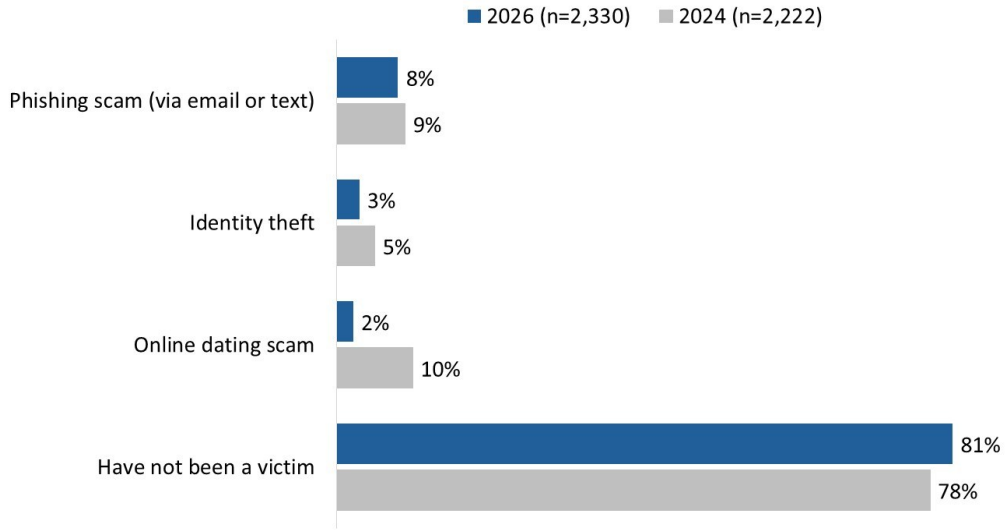


QCT8. Do you think you are vulnerable to a ransomware attack? Base: all respondents.

Few online Canadians report having been a victim of online scams

Most online Canadians (81%) report not having been a victim of an online scam involving the loss of money or data. Phishing scams are the most commonly reported type (8%), followed by identity theft (3%) or online dating scams (2%, down from 10%).

Figure 28: Personal experience with online scams where money or data lost



QCCE1. Have you ever personally been a victim of online scams where you have lost money or data? / QCCE1B. Was this…? Base: all respondents.

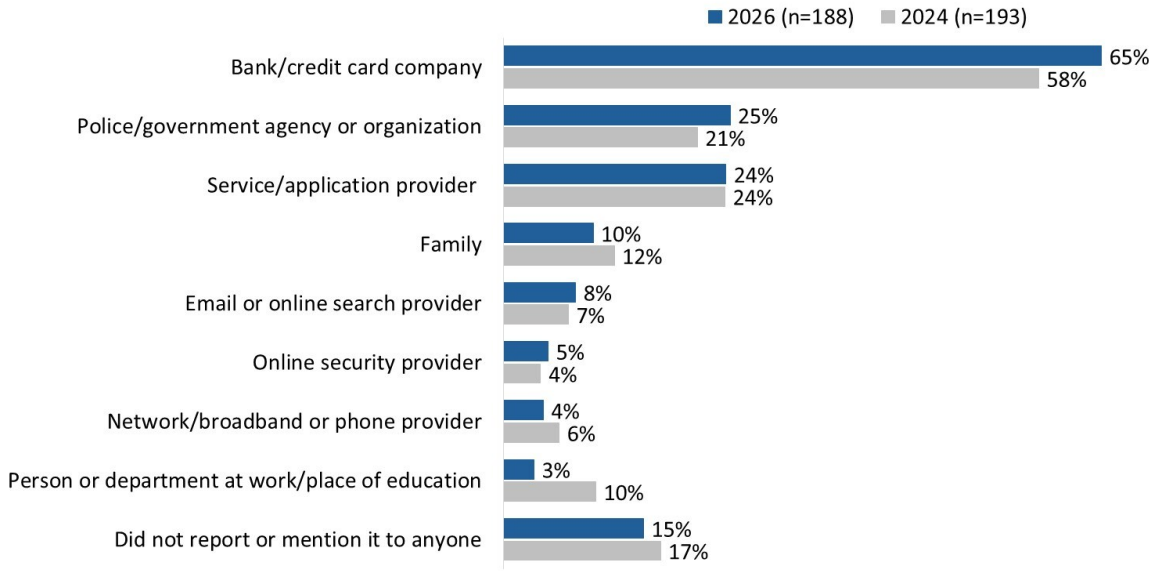
The incidence of online scams involving financial or data loss is highest among lower-income households (under $40,000 annually) and individuals with basic or novice online security knowledge.

Reported experiences vary by region and age. Residents of Atlantic Canada are more likely than those in Quebec, Ontario, Alberta, and British Columbia, including the Territories to report being a victim of a phishing scam. Ontario residents are more likely than those in Atlantic Canada, Saskatchewan and Manitoba, and Alberta to report identity theft. By age, Baby Boomers are more likely than Gen Z and Millennials to report having experienced a phishing scam.

Victims of phishing scams most likely to report this to their financial institution

Among those who were a victim of a phishing scam (n=188), most say they reported the incident to their bank or credit card provider (65%). In addition, about one-quarter contacted the police or a government organization (25%) or the relevant service or application provider (24%). Other responses were cited less frequently; the full range is shown in Figure 29.

Figure 29: Reporting of phishing scams by victims

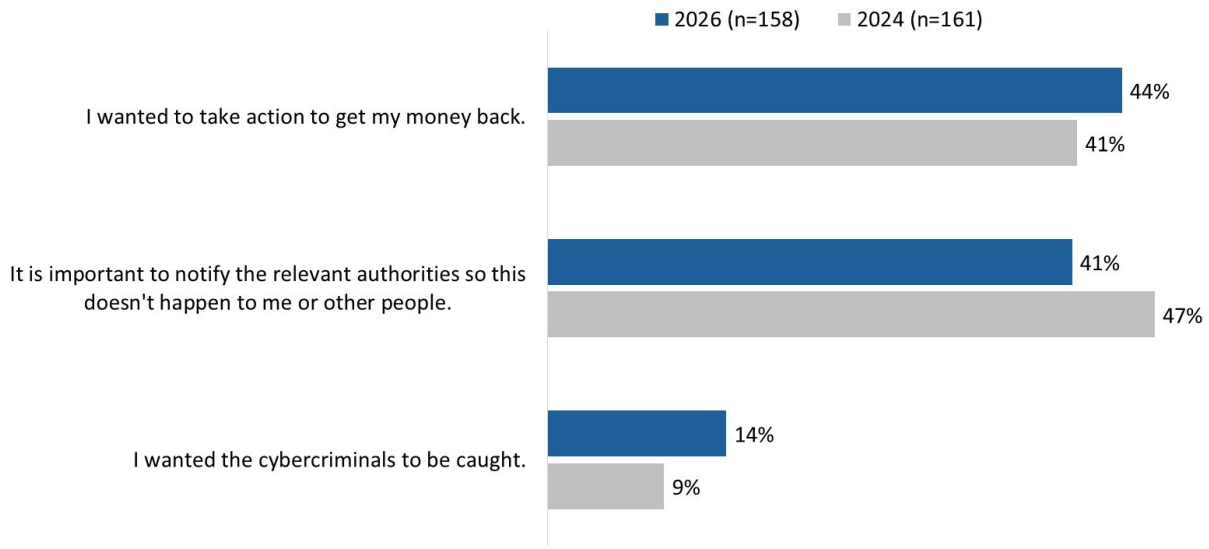


QCCE2. You mentioned that you have lost money or data through a phishing scam. Did you report this to anyone? Base: those who were a victim of phishing scam [Multiple responses accepted].

Reason for reporting phishing scams varied, as did the reasons for not reporting

Among those who were a victim of a phishing scam and reported it (n=158), 44% did so because they wanted to take action to get their money back and 41% because it is important to notify the relevant authorities, so it doesn't happen again or to others. Only fourteen percent say they reported because they wanted the cybercriminals to be caught.

Figure 30: Reasons for reporting phishing scams



QCCE3. What is the main reason you reported a phishing scam? Base: those who were a victim of phishing scam and reported it.

Among those who experienced a phishing scam and did not report it (n=30), the most commonly cited reasons were that the amount of money lost was small or the data compromised was of limited importance, and the perception that no action would be taken.

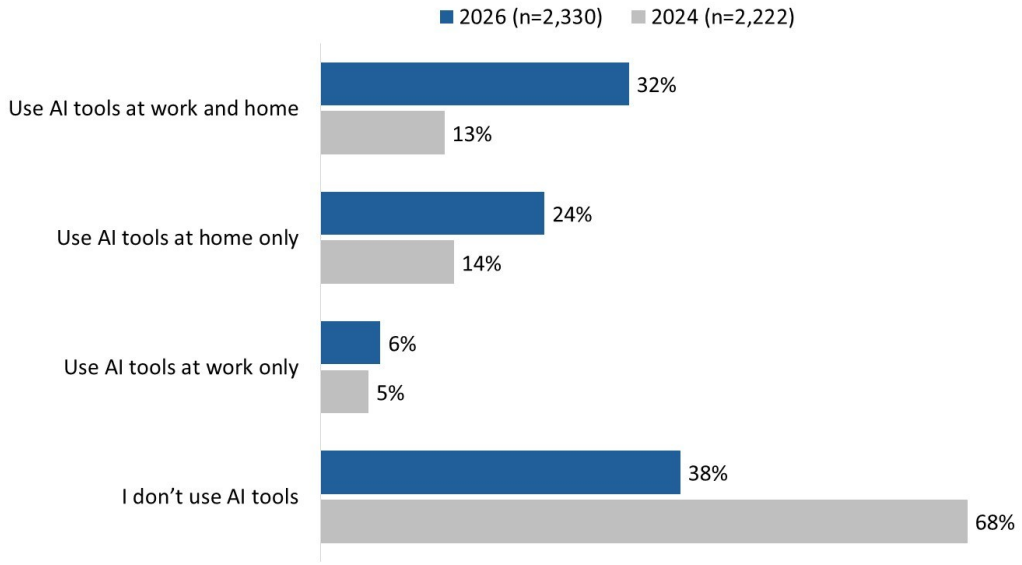
4. View on artificial intelligence

Use of AI tools has increased substantially since 2024

Use of AI tools, such as ChatGPT, CoPilot, DALL-E, has increased significantly since 2024, when a third (32%) reported using these tools. By 2026, this has nearly doubled to 62%. In terms of where online Canadians use AI tools, 32% report using AI tools both at work and at home (up from 13% in 2024), 24% use them at home only (up from 14%), and 6% use them at work only.

AI tool use varies by age and income. At-home only use is highest among Canadians aged 65 and older, while use both at work and at home is more common among those under 45 and those with household incomes over $150,000. Baby Boomers and the Silent Generation are more likely to report not using AI tools.

Figure 31: Use of AI tools

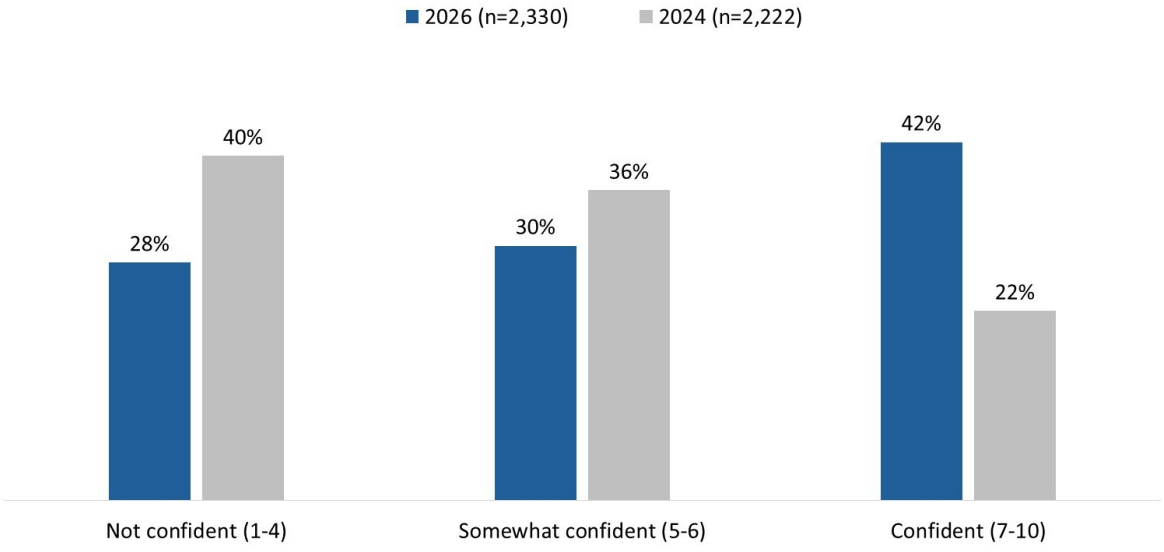


QAI1: Do you use any Artificial Intelligence (AI) tools at home or at work? Base: all respondents.

Confidence in recognizing AI-generated content is increasing

Alongside increasing use of AI tools, more online Canadians report feeling confident in their ability to recognize AI-generated content. Four in 10 (42%) say they are confident (scores of 7 to 10) in their ability to identify AI-generated messages, images, videos, or deepfakes. This represents a 20-point increase since 2024, when 22% reported this level of confidence. An additional 30% say they are somewhat confident, while 28% report not being confident in their ability to identify AI-generated content.

Figure 32: Confidence in ability to recognize AI content



QAI3. How confident are you in your ability to recognize AI-generated content (e.g., messages, pictures, videos, deepfakes)? Base: all respondents.

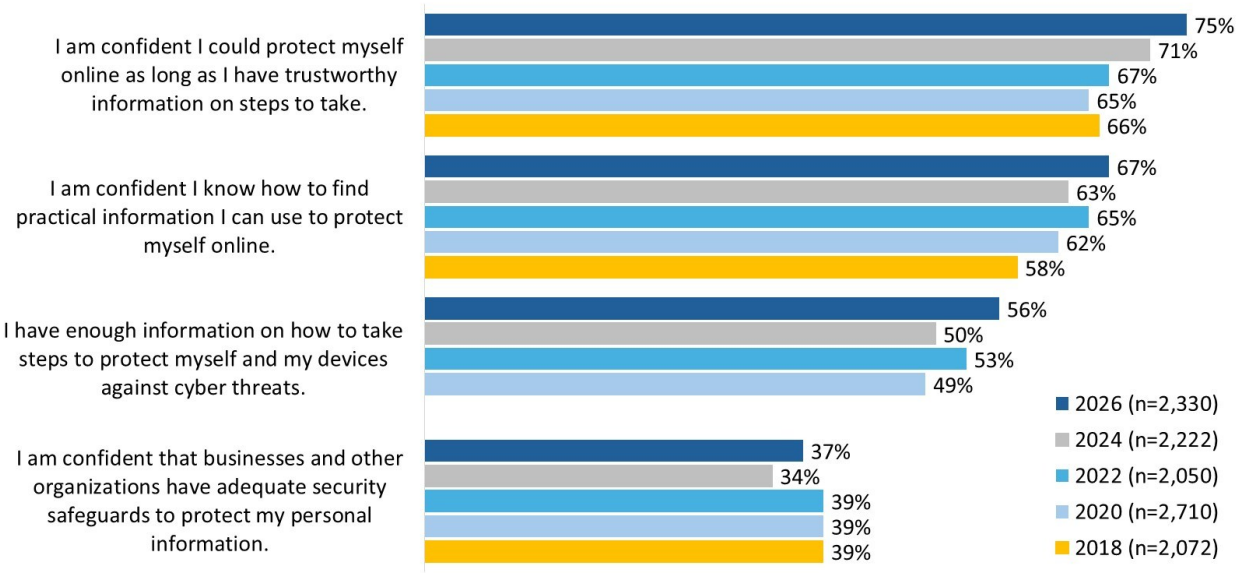
Younger online Canadians, men, those with secondary school education, and those with advanced online security knowledge are more likely to be confident about their ability to recognize AI-generated content.

5. Communications and the Get Cyber Safe campaign

Confidence in accessing and using cyber security information has increased

Three-quarters (75%) of online Canadians feel confident they could protect themselves online as long as they have trustworthy information on steps to take. Two-thirds (67%) are confident they know how to find practical information they can use to protect themselves online. Additionally, a little over half (56%, up from 50%) of online Canadians feel they have enough information on how to take steps to protect themselves and their devices against cyber threats. Far fewer (37%) are confident that businesses and other organizations have adequate security safeguards to protect their personal information.

Figure 33: Cyber threat prevention information: % agreeing with each statement



QINFO1. Please rate the degree to which you agree with the following statements. Base: all respondent [Multiple responses accepted].

Notable subgroup differences include the following:

- Younger online Canadians are more likely to think they have enough information to take steps to protect themselves, and to be confident they could protect themselves and find practical information.
- Men are more likely than women to agree that they have enough information on how to take steps to protect against cyber threats as well as to be confident they can find practical information to protect themselves online.
- Those with a higher annual household income ($100,000 and over) are more apt to agree that they have enough information to protect themselves and their devices.

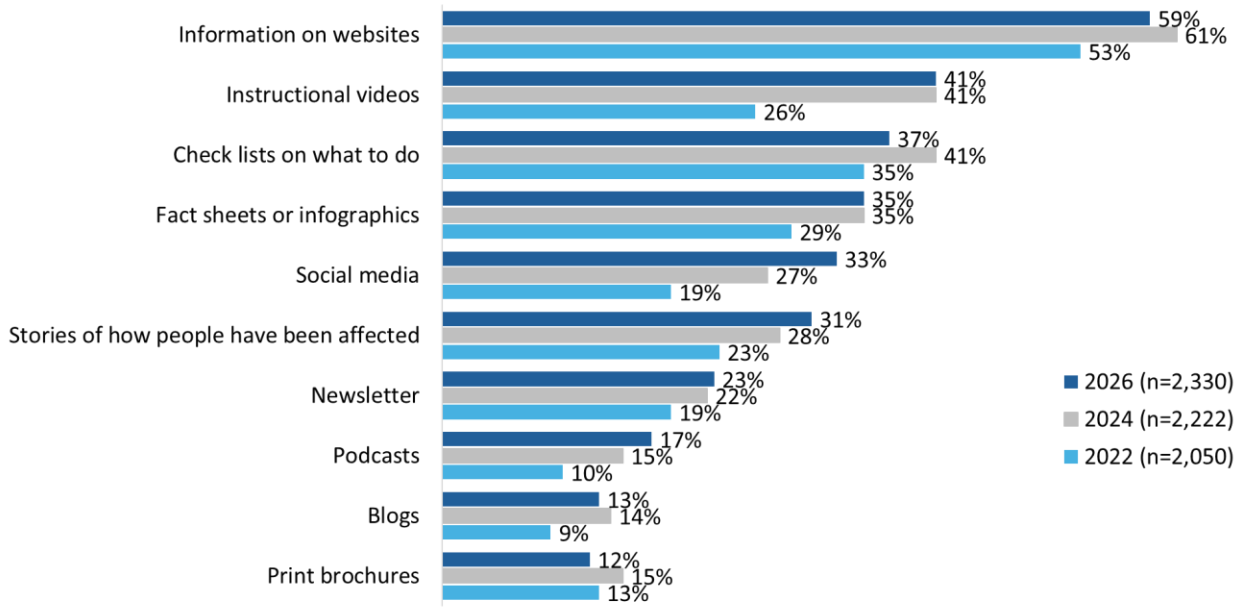
- The Silent Generation, followed by Baby Boomers, are most in need of information: they are more likely to lack confidence in their ability to find practical information and to protect themselves online with trustworthy information, and they are more apt to feel they do not have information to take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

Websites continue to be the most preferred source of cyber safety information

Fifty-nine percent of online Canadians say they would prefer to receive information on protecting themselves from cyber threats via websites. This is followed by instructional videos (41%) and checklists outlining what to do (37%). Approximately one-third are interested in fact sheets or infographics (35%) or social media (33%). The full range of preferred formats is shown in Figure 34.

Over time, the same three formats—websites, instructional videos, and checklists—continue to rank highest. Results are generally consistent with 2024, with most year-over-year differences within five percentage points. One exception is social media, which is cited more frequently this year than in previous waves.

Figure 34: Preferred source of cyber threat information



QINFO2. How do you prefer to get information to protect yourself from cyber threats? Base: all respondents [Multiple responses accepted].

Notable subgroup differences include the following:

- Online Canadians aged 65+ are most likely to prefer check lists and print brochures. In contrast, younger Canadians (those under 35) are more apt to prefer social media and information on websites, while those under 45 are more likely to prefer stories of how people have been affected.
- More men prefer to get information to protect themselves from cyber threats via podcasts, blogs, and informational websites. Women, conversely, are more apt to prefer fact sheets or infographics, check lists, and print brochures.

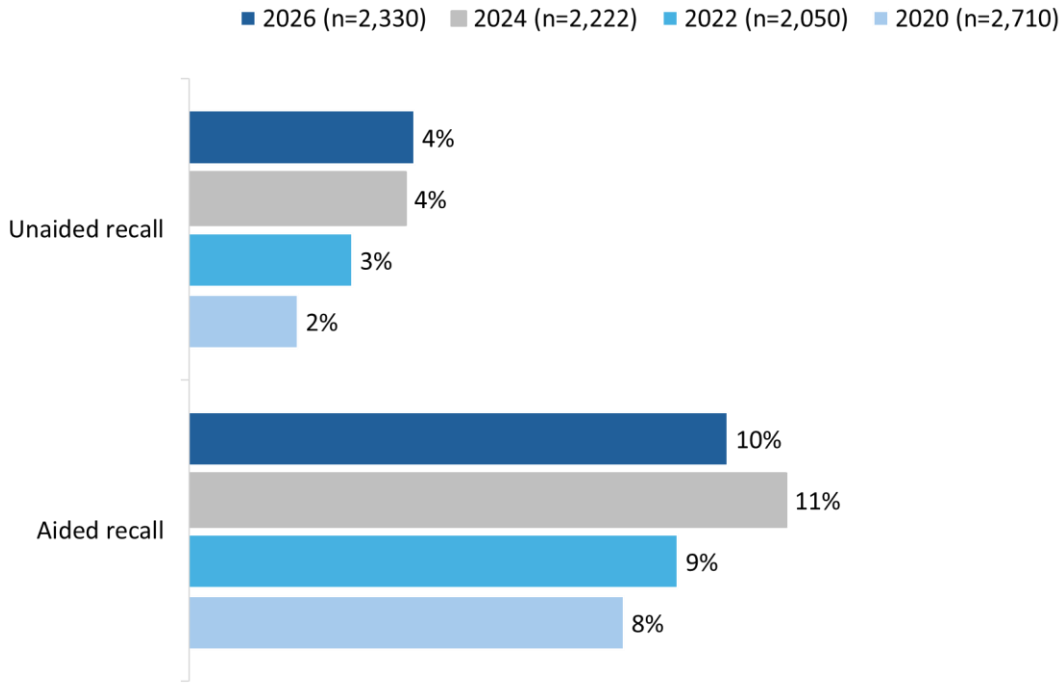
- University graduates are more likely to prefer fact sheets or infographics and instructional videos.

Recall of Get Cyber Safe campaign remains low

Awareness remains unchanged from 2024: 4% of online Canadians can name the Government of Canada cyber security awareness campaign unprompted. When prompted, one in 10 (10%) report awareness of Get Cyber Safe.

With prompting, Gen Z is most likely to recall the campaign.

Figure 35: Recall of the Get Cyber Safe awareness campaign



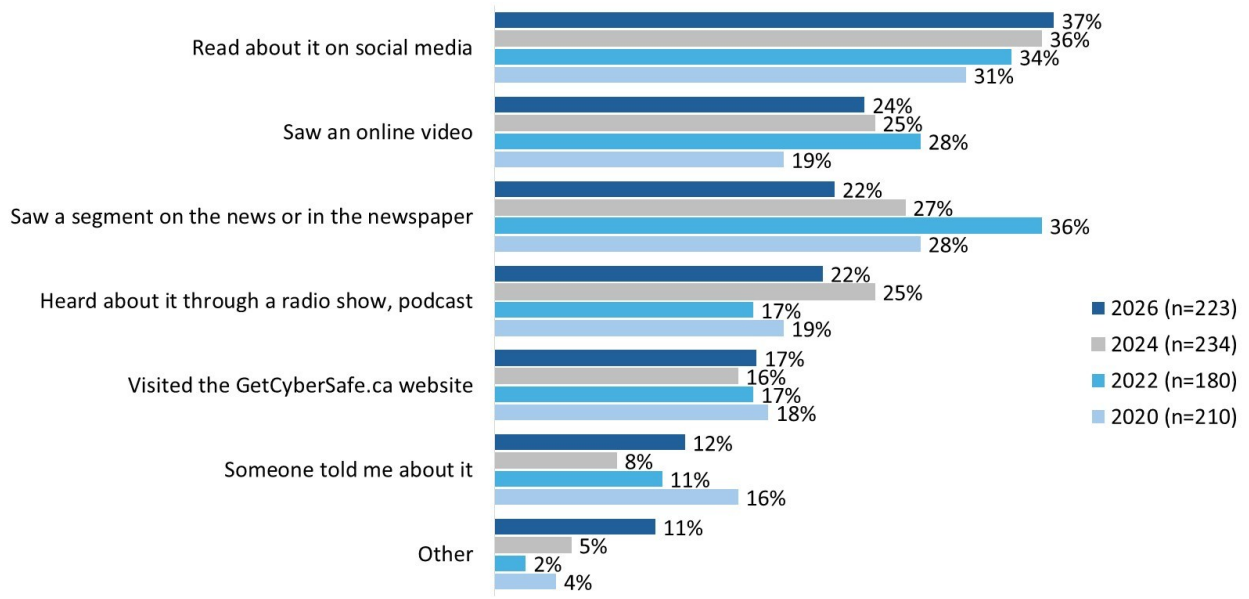
QGCS1. There is a Government of Canada awareness campaign created to inform Canadians about cyber security and the simple steps they can take to protect themselves online. Can you name this campaign? / QGCS3. Have you seen, heard, or read anything from the Government of Canada with the title Get Cyber Safe that talked about online threats and how to protect yourself? Base: all respondents.

Roughly four in 10 attributed their awareness of campaign to social media

Among those aware of the Get Cyber Safe campaign (n=223), just over one-third (37%) say they encountered it on social media. Roughly two in 10 report seeing an online video (24%), a news segment or newspaper coverage (22%), or hearing about it through a radio show or podcast (22%). Smaller proportions report visiting the GetCyberSafe.ca website (17%) or hearing about the campaign from someone else (12%).

The proportion of online Canadians who report seeing a segment on the news or in a newspaper has continued to decline, falling from 36% in 2022 to 27% in 2024 and 22% in 2026.

Figure 36: Sources of awareness of the Get Cyber Safe campaign



QGCS4. Where did you see, hear, or read this? Base: those who heard of Get Cyber Safe [Multiple responses accepted].

6. Business 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=300).

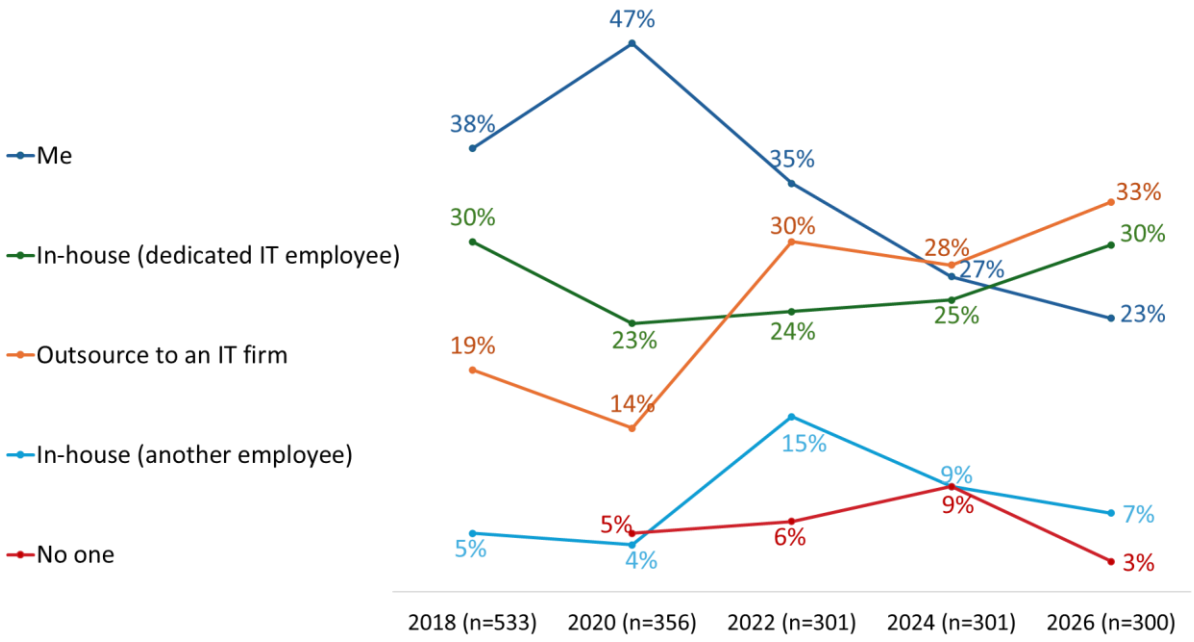
For the purpose of this survey, small businesses are considered establishments that employ up to 100 employees. Just over one-quarter (26%) of companies in the survey sample employ fewer than five employees. Among the rest, 16% employ five to nine employees, 38% 10 to 49, and 20% 50 to 100 employees.

IT responsibility is outsourced

One-third (33%) of business respondents report outsourcing IT support. Three in 10 (30%) say they have a dedicated in-house IT employee, while 23% say they are personally responsible for their company's IT. Relatively few business respondents report that another non-dedicated employee handles IT (7%) or that no one is responsible (3%).

Over time, fewer business owners and managers report personally handling their company's IT, declining from 47% in 2020 to 35% in 2022, 27% in 2024, and 23% in 2026. Use of external IT providers has generally increased over time, from 14% in 2020 to 33% in 2026, though levels have fluctuated slightly between waves. Use of in-house dedicated IT support has increased this year after being consistent between 2020 to 2024) and is back in line with the 2018 baseline results.

Figure 37: Responsibility for company IT



QBUS1. Who is responsible for your company's IT? Base: business respondents.

Most businesses have taken steps to protect themselves against cyber threats

Most business respondents (77%) say their company has taken steps to protect against cyber threats. Among the remainder, 4% say no measures have been implemented, while 18% are unsure whether their company has taken action.

Half or more of business owners and managers report that their organization requires password protection on all devices (59%), keeps security software up to date across machines (55%), and uses password protection or user authentication for wireless or remote access (52%). The full list of measures is shown in Figure 38.

Cyber security measures have remained stable over time, with a few exceptions. More businesses are adopting a cyber security policy for employees (25% to 33%) and providing cyber security best-practices training (24% to 32%), while fewer are backing up information on all devices (42% in 2024 to 37% in 2026).

Figure 38: Measures implemented by companies to safeguard against cyber threats

	2026 (n=300)	2024 (n=301)	2022 (n=301)	2020 (n=360)	2018 (n=533)
Require password protection on all devices	59%	57%	69%	57%	71%
Keep security software up to date on all machines	55%	55%	63%	51%	69%
Use a password or user authentication for wireless, remote access	52%	51%	60%	52%	67%

Set spam filters	39%	40%	49%	39%	54%
Back up information on all devices	37%	42%	58%	49%	60%
Adopt a cyber security policy for employees	33%	25%	32%	18%	--
Provide cyber security best practices training for employees	32%	24%	24%	15%	--
Use encryption software	31%	31%	34%	23%	36%
Use information removal protocols when employees leave	27%	27%	28%	18%	37%
Do not use administrator account when accessing the web	14%	14%	24%	15%	25%
None of these	4%	*6%*	*5%*	*9%*	*5%*
Don't know	18%	*16%*	*8%*	*10%*	*5%*

QBUS2. Which of the following steps has your company taken to protect itself against cyber threats? Base: business respondents [Multiple responses accepted].

Most Businesses would benefit from cyber threat information

When it comes to protecting their company against cyber threats, roughly one-third of business owners and managers said that their organization would benefit from guidelines for reacting to a cyber attack (36%, down from 44% in 2024), a list of the types of threats that exist and clues to look for (36%, down from 42% in 2024), tips or resources for the type of software or hardware to make networks secure (35%), and best practices for safe cloud computing (35%). The full range of information deemed beneficial by respondents can be found in the table below.

Figure 39: Cyber threat information viewed as beneficial for businesses

	2026 (n=300)	2024 (n=301)	2022 (n=301)	2020 (n=360)	2018 (n=533)
Guidelines for reacting to a cyber attack	36%	44%	50%	40%	46%
A list of the types of threats that exist and cues to look for	36%	42%	49%	41%	47%
Best practices for safe cloud computing	35%	34%	43%	36%	35%
Tips/resources for software/hardware to make networks secure	35%	33%	41%	29%	36%
Steps to protect mobile devices in a public setting	32%	38%	44%	39%	40%
Guidelines to establish rules for safe email usage policies	32%	35%	40%	28%	39%
Resources on encrypting computers, laptops, storage devices	31%	33%	41%	34%	37%
Best practices for employees on how to handle passwords	30%	32%	44%	29%	37%
Tips on communicating the importance of cyber security policies to employees	30%	28%	35%	25%	32%
Guidelines on use of personal devices for work	30%	27%	42%	31%	40%
Best practices for a clear internet usage policy	30%	26%	38%	27%	37%
Steps for handling work information of departing employees	29%	27%	33%	22%	33%
Best practices for use of storage devices	28%	31%	39%	34%	40%
Guidelines on how to establish a social media policy	22%	22%	28%	26%	37%
Other	3%	3%	4%	3%	4%
None of these	*7%*	*5%*	*5%*	*9%*	*8%*
Don't know	*21%*	*12%*	*11%*	*13%*	*12%*

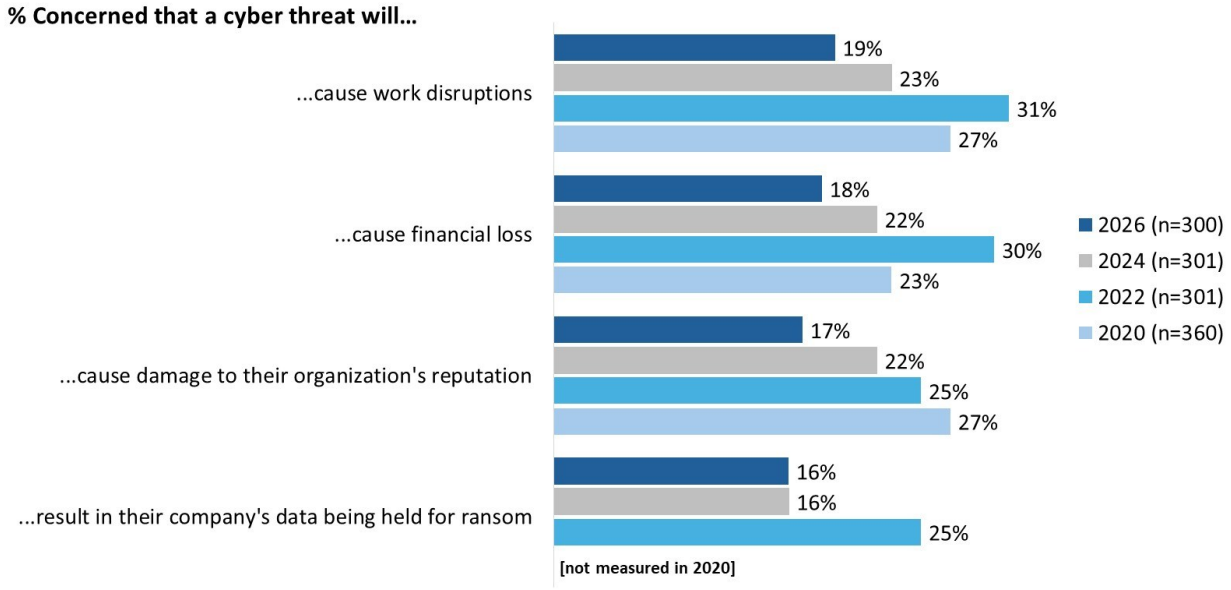
QBUS3. Which of the following types of information do you think your company would benefit from having in order to protect itself against cyber threats? Base: business respondents [Multiple responses accepted].

Concern about cyber threats has declined year-over-year

When thinking about their company's daily operations, roughly two in 10 business owners and managers express concern about work disruptions (19%), financial loss (18%), and reputational damage (17%). Sixteen percent report concern about their company's data being held for ransom.

Since 2022, concern has declined across nearly all areas. The only exception is concern about company data being held for ransom, which has remained stable at 16% since 2024.

Figure 40: Level of concern about cyber threat impacts



QBUS4. Thinking about the daily operations of your company, how concerned are you that a cyber threat will ...? Base: business respondents.

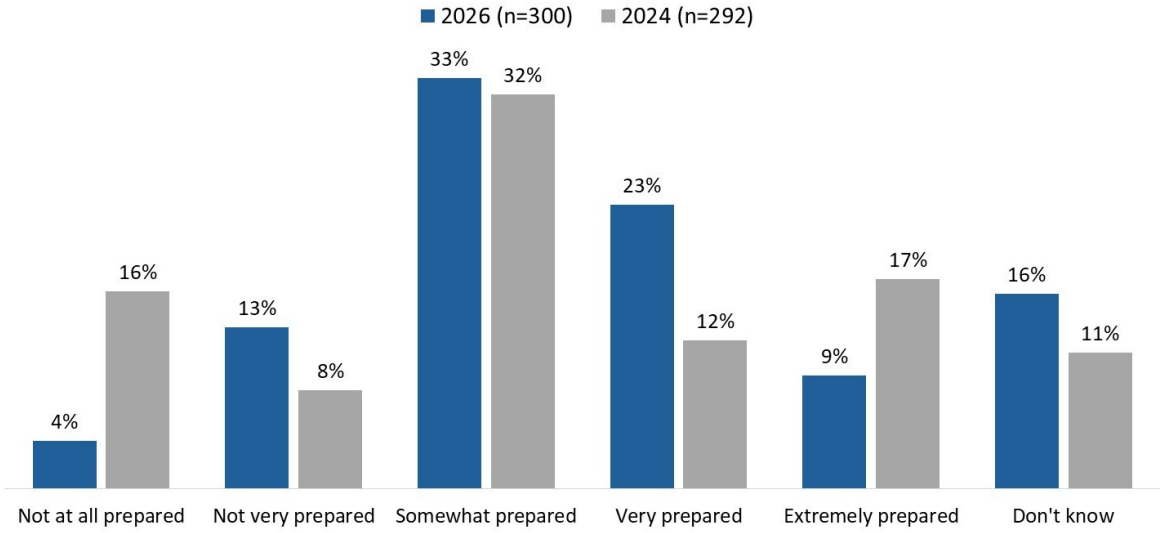
Two-thirds of companies are a least somewhat prepared to defend against ransomware attacks

A majority of business owners and managers say their company is at least somewhat prepared to defend against ransomware attacks, including 33% who feel somewhat prepared, 23% very prepared, and 9% extremely prepared. Roughly two in 10 (17%) say their company is not prepared, while 16% are unsure how to rate their organization's readiness.

Over time, perceptions of preparedness are stable.[2]

[2] Scale was adjusted in 2026 from a 7-point scale to a 5-point scale. 2024 data was compressed to match 2026. Differences observed over time are not statistically significant.

Figure 41: Readiness to defend against ransomware attacks



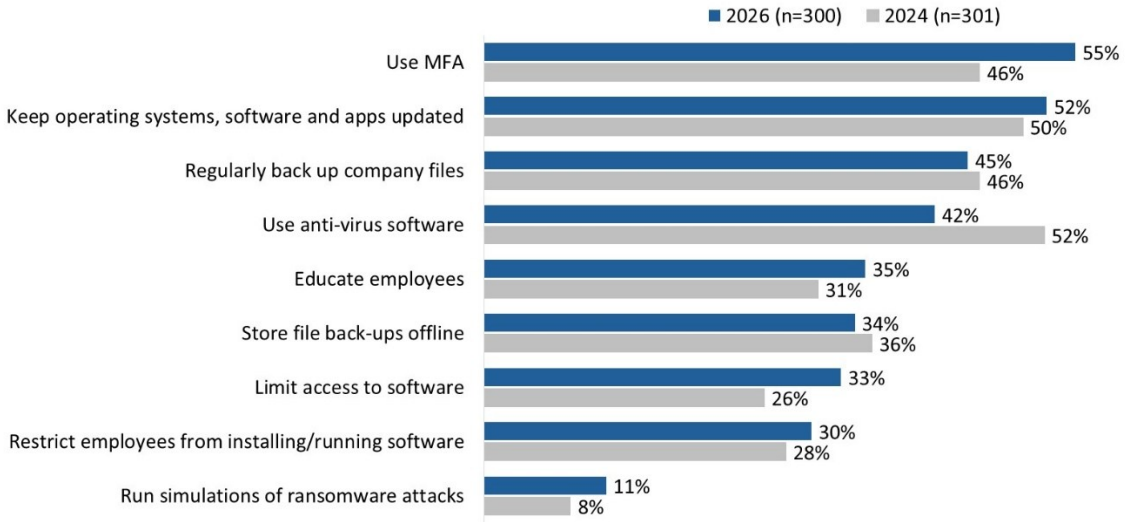
QBUS5. How would you rate your company's current level of readiness to defend against ransomware attacks? Base: business respondents.

About half of businesses use MFA and keep systems updated

Roughly half of business owners and managers said their company uses MFA (55%, up from 46% in 2024), and keeps operating systems, software and apps updated (52%). Forty-five percent regularly back up company files, while slightly fewer use anti-virus software (42%, down from 52%).

In addition, around one-third educate employees (35%), store file back-ups offline (34%), and limit access to software (33%). Three in 10 (30%) restrict employees from installing or running software. Very few (11%) run simulations of ransomware attacks. Nearly one-quarter (23%) of business owners and managers did not know whether their company has done anything to protect itself from ransomware attacks.

Figure 42: Actions to protect company from ransomware attacks

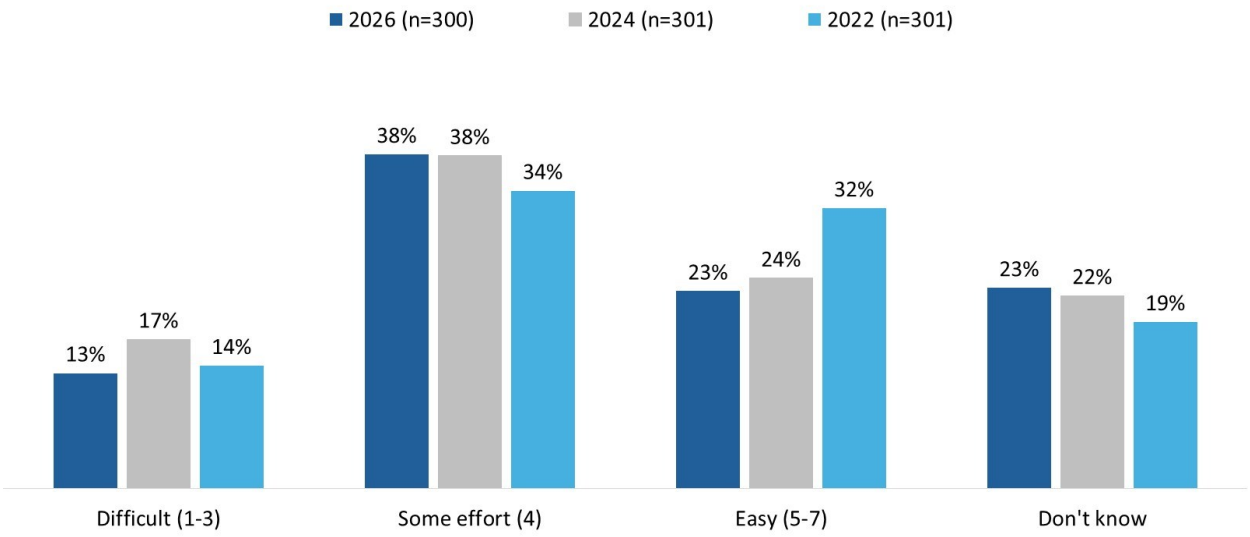


QBUS6. What, if anything, has your company done to protect itself from ransomware attacks? Base: business respondents [Multiple responses accepted].

Recovering from a ransomware attack would take some effort for most companies

Half of business owners and managers say that it would take some effort (38%) or would be difficult (13%) for their company to recover from a ransomware attack. Approximately one-quarter feel it would be easy for their company to recover (23%) or do not know (23%).

Figure 43: Ransomware attack recovery ability



QBUS7. How well would your company be able to recover from a ransomware attack? Base: business respondents.

Profile of Survey Respondents

Present in the tables below is a profile of survey respondents (using weighted data). In total, 81% of the surveys were completed in English and 19% in French.

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

Age	**%**
18-24	10%
25-34	17%
35-44	16%
45-54	16%
55-64	18%
65+	24%

Generation	**%**
Gen Z: 1997-2008	17%
Millennials: 1981-1996	28%
Gen X: 1965-1980	28%
Baby Boomers: 1946-1964	25%
Silent: 1928-1945	3%

Gender	**%**
Man	47%
Woman	49%
Another gender	1%
Prefer not to answer	2%

Education	%
Elementary school or less	2%
Secondary school	14%
College, vocational or trade school	32%
Undergraduate university program	7%
Graduate or professional university program	50%
Prefer not to answer	2%

Employment status	%
Working full-time	47%
Working part-time	7%
Self-employed	13%
Unemployed, but looking for work	4%
A student attending school full-time	7%
Retired	17%
Not in the workforce	3%
Other	2%
Prefer not to answer	1%

Household income	%
Under $20,000	5%
$20,000 to just under $40,000	8%
$40,000 to just under $60,000	10%
$60,000 to just under $80,000	10%
$80,000 to just under $100,000	14%
$100,000 to just under $150,000	20%
$150,000 and above	20%
Prefer not to answer	13%

Parent	%
Yes	35%
No	64%
Prefer not to answer	1%

Age of children	%
Under 5 years	26%
5 to 8 years	28%
9 to 12 years	30%
13 to 15 years	30%
16 to 17 years	29%

Frequency of using the internet	%
A few times per week	<0.5%
A few times a day	23%
I'm always connected	77%

Level of online security knowledge	%
Advanced	20%
Intermediate	46%
Basic	29%
Novice/Beginner	3%
I don't have any knowledge about staying secure online.	1%

Appendix

Technical specifications

The following specifications applied to the survey:

- A 15-minute online survey was administered to 2,330 Canadians, 18 years of age and older, who use the internet at least a few times a month. The overall results can be considered accurate within ±2.1%, 19 times out of 20.
- Quotas were in place for 300 business owners and managers/supervisors of companies with fewer than 100 employees (business sub-sample) and 600 households with children under 18 years of age (parent sub-sample). In total, surveys were completed with 300 business owners and managers/supervisors and 846 parents. The margins of error are greater for results pertaining to subgroups of the total sample.
- 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 January 5, 2026, with 30 individuals. Fourteen surveys were completed in French and the rest in English. The average length of the survey was 16.8 minutes. On January 9, changes to the questionnaire were implemented to reduce the survey length (the target length was 15 minutes). Changes involved the removal of questions and changes to the wording of one question (QSC3). As a result, the pre-test data were not retained in the final survey data.
- The fieldwork began in full on January 9 and was completed January 29, 2026.
- 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, 20,601 panellists were recruited to participant in the survey. A total of 2,330 panellists completed the survey, for a participation rate of 14.2%.

The survey data were 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%	6%
Quebec	23%	20%
Ontario	39%	41%
Saskatchewan and Manitoba	6%	7%
Alberta	11%	11%
British Columbia and Territories	14%	15%

Age	% Weighted	% Unweighted
18-24	10%	9%
25-34	17%	17%
35-44	16%	19%
45-54	16%	18%
55-64	18%	14%
65+	24%	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 [INSERT]. 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]
01. Less than a few times a month [THANK AND TERMINATE]
02. A few times per month [THANK AND TERMINATE]
03. Once a week
04. A few times per week
05. A few times a day
06. I'm always connected [SKIP TO S6]

S5. [IF S4=03-05] 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 [THANK AND TERMINATE]
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, 30 or more hours per week
02. Working part-time, that is, less than 30 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]
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]
[RANDOMIZE ITEMS]
a) I find it easy to be secure when I'm online.
b) I presume my devices are automatically secure.
c) It is expensive to fully protect myself online.
d) I don't see the point of trying to protect myself more as my information is already online.
e) Falling victim to cybercrime is something that worries me.
f) I'm worried about Artificial Intelligence (AI)-related cybercrime.

[DO NOT RANDOMIZE; ALWAYS PRESENT LAST]

g) Family members rely on me to keep them 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]
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) with the following things? [CAB24]
[RANDOMIZE ITEMS]
a) Getting advice and information on how to be secure online.
b) Creating online accounts.
c) Checking or adding security settings on your 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).

* Add description: Phishing is when scammers pretend to be a trusted organization to trick people into giving personal or financial information. They often use emails, texts, or direct messages to get things like passwords or banking details.

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

* Add description: Phishing is when scammers pretend to be a trusted organization to trick people into giving personal or financial information. They often use emails, texts, or direct messages to get things like passwords or banking details.

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? [Cyber24]
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]
01. I don't know how to do this. [SKIP TO QBEH6]
02. I know how to, but I don't do it. [SKIP TO QBEH6]
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]
01. Never [SKIP TO QBEH6]
02. Rarely [SKIP TO QBEH6]
03. Sometimes
04. Very often
05. Always

QBEH4. [IF QBEH3=03-05] When do you typically install software updates on your devices? [CAB24]
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]
Also known as Two-Factor or Two-Step Verification.

01. Yes
02. No [SKIP TO QBEH10]

QBEH7. [IF QBEH6=01] Do you know how to use multi-factor authentication (MFA)? **[CAB24]**

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 QBEH12]

QBEH8. [QBEH7=02, 03] What is the main reason you don't use (or stopped using) multi-factor authentication (MFA)? [CAB24]
[RANDOMIZE]
01. MFA takes too long.
02. I don't carry my phone with me all the time to be able to use MFA.
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 use MFA.
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.

QBEH12. What steps do you take to verify that a website is legitimate? **[CAB24]**
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? [Cyber24]
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]
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? [Cyber24]
Please select all that apply

[RANDOMIZE]
01. [CANNOT BE SELECTED WITH 02] Keep your passwords simple and easy to remember
02. [CANNOT BE SELECTED WITH 01] Make your passwords complex with a combination of letters, numbers and symbols
03. Use a passphrase 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. Choose to use a passkey, when it's available, in place of a password (A passkey is a login method that uses your device's biometrics, like a fingerprint or facial recognition, or a PIN)
11. [ANCHOR] Other (please specify)
12. [ANCHOR] None of these
13. [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]
'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] What is the main reason you rarely, if at all, use unique passwords for your online accounts? [CAB24]
[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 passwords you usually create? [CAB24]
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]
[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.

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 ... [Cyber24]
[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? [Cyber24]
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. Think 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? [Cyber24]
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? [Cyber24]
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? [Cyber24]
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? [Cyber24]
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? [Cyber24]
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? [Cyber24]
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? [Cyber24]
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

QCCE1. Have you ever personally been a victim of online scams where you have lost money or data? [CAB24-MODIFIED]
01. Yes
02. No

QCCE1B. Was this… [CAB24MODIFIED]
Please select all that apply

[RANDOMIZE]
01. A phishing scam (via email or text)
02. An online dating scam [SKIP TO QAI1]
03. Identity theft [SKIP TO QAI1]
04. Other, please specify [SKIP TO QAI1]

Add descriptions:

- "Phishing scam": 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 QCCE1B=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]
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]
[RANDOMIZE]
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]
[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:

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]
***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]
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? [Cyber24]
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? [Cyber24]
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? [Cyber24]
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 ... [Cyber24]
[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]
01. Not at all concerned
02. Not very concerned
03. Somewhat concerned
04. Very concerned
05. 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? [Cyber24]
01. Not at all prepared
02. Not very prepared
03. Somewhat prepared
04. Very prepared
05. Extremely prepared
I don't know
Prefer not to answer

QBUS6. What, if anything, has your company done to protect itself from ransomware attacks? [Cyber24]
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? [Cyber24]
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. [Cyber24]
[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? [Cyber24]
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? [Cyber24]
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? [Cyber24]
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? [Cyber24]
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. Less than a High School diploma or equivalent
02. High School diploma or equivalent
03. Registered Apprenticeship or other trades certificate or diploma
04. College, CEGEP or other non-university certificate or diploma
05. University certificate or diploma below bachelor's level
06. Bachelor's degree
07. Post graduate degree above bachelor's level
08. 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 Canada. In the coming months, a report with the findings from this study will be available from Library and Archives Canada. Thank you very much for taking part. It is appreciated.