Government of Canada Gouvernement du Canada

Get Cyber Safe Awareness Tracking Survey:
Executive Summary

Prepared for the Communications Security Establishment

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

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

Ce rapport est aussi disponible en français

Get Cyber Safe Awareness Tracking Study
Executive Summary

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

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

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

media@cse-cst.gc.ca

Catalogue number:
D96-17/2024E-PDF

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

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

Executive Summary

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

Background and objectives

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

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

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

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

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

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

Methodology

A 15-minute online survey was conducted with 2,222 online Canadians aged 18 and older. This included 619 surveys with parents of children under 18 years of age, and 301 surveys with Canadians who own or act in a managerial position in a small- to medium-sized business employing between one and 100 individuals.

The sample was drawn from Advanis' proprietary General Population Random Sample (GPRS) which has been developed using probability-based recruitment; specifically, random digit dialling (RDD) via Interactive Voice Response (IVR) and via live Computer Assisted Telephone Interviewing (CATI). This panel of more than 600,000 individuals can be considered representative of the general public in Canada.

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

Key findings

Cyber security practices of online Canadians

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

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

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

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

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

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

Cybercrime and threats

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

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

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

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

Communications and the Get Cyber Safe campaign

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

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

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

Businesses and cyber security

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

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

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

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

Parents and cyber security

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

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

Concluding observations

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

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

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

Notes to reader

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

Contract value

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

Statement of political neutrality

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

aWoods

Alethea Woods
President
Phoenix Strategic Perspectives Inc.