Government of Canada | Gouvernement du Canada

Get Cyber Safe Awareness Tracking Survey

Summary

Prepared for Communications Security Establishment

Supplier: EKOS RESEARCH ASSOCIATES INC.
Contract Number: 2L165-220295/001/CY
Contract Value: $63,991.29
Award Date: December 13, 2021
Delivery Date: March 15, 2022

Registration Number: POR 070-21
For more information on this report, please contact CSE at: media@cse-cst.gc.ca

Ce rapport est aussi disponible en français

Canada

Get Cyber Safe Awareness Tracking Survey

Final Report

Prepared for Communications Security Establishment
Supplier name: EKOS RESEARCH ASSOCIATES INC.
Date: March 2022

This public opinion research report presents the results of an online survey conducted by EKOS Research Associates Inc. on behalf of the Communications Security Establishment. The research study was conducted with 2,050 Canadians between January 21 and February 14, 2022.

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

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

Catalogue Number:
D96-17/2022E-PDF

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

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

EXECUTIVE SUMMARY

A. BACKGROUND AND OBJECTIVES

As the most frequent internet users in the world, it is important for Canadians to have a strong understanding of – and dedication to – cyber security and safety. This includes knowing how to identify an online threat, knowing the actions that should be taken to combat these threats, knowing where to find reliable information about how to stay safe online, and a commitment to protecting identities and safeguarding internet-enabled devices. It is for this reason that Canada's Cyber Security Strategy includes assessing public awareness and engagement with cyber security, as well as implementing the Get Cyber Safe public awareness campaign, which aims to boost general knowledge and understanding.

The objectives of the proposed research are as follows:

- Assess performance of the public awareness campaign and help identify shifts in knowledge, behaviours, and attitudes.
- Track awareness, attitudes and behaviour relating to cyber security among the campaign target audience(s) for the public awareness campaign.
- Identify and track motivators and barriers to behaviour change (for those who have taken action, what prompted them to do so, for those who have not, why not?).
- Identify and track the best ways of communicating such information.
- Track public expectations in terms of the involvement of the federal, provincial, and municipal governments, as well as non-governmental agencies.

B. METHODOLOGY

The sample consists of 2,050 completed interviews with Canadians 16 years of age or older who use the internet on a regular basis, including 553 interviews with parents of children under 18 years of age, and 301 with Canadians who own or act in a managerial position in a small- to medium-sized business employing between one and 100 individuals. The sample is based on a random selection of Prob*it* panel members from across the country. Prob*it* panellists were selected using a random-digit dial (RDD) landline-cell phone hybrid sample frame. This panel of more than 120,000 individuals can be considered representative of the general public in Canada (meaning that the incidence of a given target population within our panel very closely resembles the public at large) and margins of error can be applied.

In this survey, a sample of 12,295 was drawn from the online only portion of the Prob*it* panel and survey cases were completed online only, since this is the specific portion of the Canadian public that would be targeted by the communications campaign. The participation rate was 17 per cent. The final survey sample of 2,050 yields a level of precision of +/-2.2 per cent for the sample overall and +/-3 to 6 per cent for most sub-groups that could be isolated in the analysis (including all regions, age, education, and income segments).

Prior to conducting the survey, the instrument was tested with 41 cases in English and 20 cases in French. The bilingual survey was administered between January 21 and February 14, 2022 and took an average of 15 minutes to complete online. The database was subsequently reviewed for data quality, outliers, coding requirements, weighting and construction of independent variables, and was used to explore sub-group patterns (e.g., by age, gender and so on) in the analysis. Weighting of the sample was based on population parameters according to the latest Census on age, gender and region of the country.

C. KEY FINDINGS

Level of Concern

Most Canadians do not feel it is likely they will be affected by a cyber threat. Over one in ten are concerned that they will be affected by a cyber threat causing their personal information to be compromised and less than one in ten are concerned they would experience a threat that results in financial loss, the loss of files or photos, or their data held for ransom. Combining the likelihood across the three areas, however, less than one in ten Canadians believe it is likely that they will experience a cyber threat in the next year, largely driven by the higher likelihood of compromised personal information. When thinking about cyber threats, three in four Canadians are concerned about identity theft. Other top threats on the mind of Canadians are general viruses, spyware or malware, and financial loss. For most Canadians who say they are not concerned about cyber threats, it is because they say they take steps to protect themselves online or that they do not do anything risky online.

Awareness

A portion of Canadians are aware of some steps to take to verify that a website is secure. The majority look for a website from a trustworthy source, such as a well-known software provider or a government website, or only use websites that they know well. Less than half look for the "https" address as their method of verifying that a website is secure, verify a site through the security lock symbol.

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

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

Precautions

Similar to previous measurement periods, nearly nine in ten Canadians take precautions to protect their online and social media accounts, devices and networks. The majority say it is best to make passwords complex with a combination of letters, numbers and symbols. Over two in three Canadians use a multi-factor authentication in some form of their online activity. For these Canadians, authentication most often involves a code received by text (for nearly nine in ten), followed by a code received by email, passwords, or PINs for about two in three. Most Canadian households, nine in ten, secure their Wi-Fi with a unique password; however, only one in six use a separate password for visitors.

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

Information

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

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

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

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

Experience of Business

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

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

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

D. NOTE TO READERS

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

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

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

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

E. POLITICAL NEUTRALITY CERTIFICATION

I hereby certify as Senior Officer of EKOS Research Associates Inc. that the deliverables fully comply with the Government of Canada political neutrality requirements outlined in the Policy on Communications and Federal Identity and the Directive on the Management of Communications.

Specifically, the deliverables do not include information on electoral voting intentions, political party preferences, standings with the electorate, or ratings of the performance of a political party or its leaders.

Signed by: 

Susan Galley (Vice President)