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: 2L165-200745/001/CY

Contract Value: $82,958.08

Award Date: March 2, 2020

Delivery Date: March 31, 2020

Registration Number: POR 086-19

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

Summary

Prepared for Communications Security Establishment
Supplier name: EKOS RESEARCH ASSOCIATES INC.
Date: March 31, 2020

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 2,700 Canadians between March 16, and 29, 2020.

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:
D96-17/2020E-PDF

International Standard Book Number (ISBN):
978-0-660-34869-8

Related publications (registration number: POR 086-19):

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.
- Profile 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.
- Identify and track the best ways of communicating such information.

B. METHODOLOGY

The sample consists of 2,710 completed interviews with Canadians 16 years of age or older who use the Internet on a regular basis, including 350 interviews with youth between the ages of 16 and 24, and 350 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 15,312 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 18 per cent. The final survey sample of 2,710 yields a level of precision of +/-1.9 per cent for the

sample overall and +/-3 to 6 per cent for most sub-groups that could be isolated in the analysis (including all regions, age, education, and income segments).

Prior to conducting the survey, the instrument was tested with 14 cases in English and 10 cases in French. The bilingual survey was administered online between March 16 and 29, 2020. 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. Less than one in five 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 or the loss of files or photos. Combining the likelihood across the three areas, however, one in five 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. Just over one in three believe they are unlikely to experience a threat in any of the three areas. Slightly more, over one-quarter, believe it is likely that a friend of family member will be affected by a cyber threat in the next year. When thinking about cyber threats, three in four Canadians are concerned about identity theft. Other threats on the mind of Canadians are financial loss, followed by general viruses, spyware or malware.

Awareness

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

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, two in five say they have been the victim of a virus, spyware, or malware on their computer and over one-quarter have been victimized

by an email scam. Other cyber attacks experienced have included text scams, social media account hacks, or identity theft.

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

Precautions

Similar to 2018, nearly nine in ten Canadians take precautions to protect their online and social media accounts, devices and networks. However, nearly two in three admit that they change some passwords more than others. One in four change passwords at least a few times a year, but one in ten never change their password. Passwords for online bank accounts are changed most often (by three in five). The majority say it is best to make passwords complex with a combination of letters, numbers and symbols.

Over half of 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 four in five), followed by passwords, a code received by email, or PINs for 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 fewer, although higher than in 2018, 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

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

Three in ten Canadians help others with their cyber security. For six in ten, this includes parents or friends. Less than half help other relatives. About three in ten help co-workers or their children.

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

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

Experience of Business

Among the concerns business owners or managers have in daily operations, only about one in four are concerned about work disruptions, financial loss, or damage to the organization's reputation due to a cyber threat. Similar to 2018, two in five are not concerned because they feel the threat for their type of company is very low. One in five have researched and taken steps to protect their business online. Just over half of business owners or managers report that their business has implemented password protection on all devices, use password or user authentication for wireless and remote access, or kept security software up to date on all machines.

Two in five business owners or managers say that their organization would benefit from a list of the types of threats that exist and clues to look out for, guidelines for reacting to a cyber attack, or steps to protect mobile devices in a public setting. Over three in ten would see value in information on best practices for safe cloud computing, resources on how to encrypt computers, laptops, and storage devices, best practices for use of storage devices, or guidelines on use of personal devices for work. About one in four indicate their organization would benefit from tips on the type of software/hardware to make networks secure, best practise for employees on how to handle passwords, guidelines to establish rules for safe email usage

policies, guidelines on how to establish strong social media policy, tips on communicating the importance of following cyber security to employees, best practices on a clear internet usage policy, or having information on steps for handling work-related information possessed by departing employees.

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.

E. CONTRACT VALUE

The contract value for the POR project is $82,958.08 (including HST).

Supplier Name: EKOS Research Associates
PWGSC Contract Number: 086-19
Contract Award Date: March 2, 2020
To obtain more information on this study, CSE at: media@cse-cst.gc.ca

[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.

F. 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 Communications Policy of the Government of Canada and Procedures for Planning and Contracting Public Opinion Research.

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)