Survey of Internet Users Regarding Cyber Security

Summary

Prepared for Public Safety Canada

Supplier: EKOS RESEARCH ASSOCIATES INC.
Contract Number: OD160192340/001/CY
Contract Value: $122,983.55 including taxes
Award Date: August 13, 2018
Delivery Date: September 30, 2018

Registration Number: 032-18
For more information on this report, please contact Public Safety Canada at info@GetCyberSafe.gc.ca

Ce rapport est aussi disponible en français

Survey of Internet Users Regarding Cyber Security

Final Report

Prepared for Public Safety Canada
Supplier name: EKOS RESEARCH ASSOCIATES INC.
Date: September 30, 2018

This public opinion research report presents the results of an online survey conducted by EKOS Research Associates Inc. on behalf of Public Safety Canada. The research study was conducted with 2,072 Canadians between August 21 and September 5, 2018.

Cette publication est aussi disponible en français sous le titre Sondage auprès des utilisateurs d'Internet au sujet de la cybersécurité.

This publication may be reproduced for non-commercial purposes only. Prior written permission must be obtained from Public Safety Canada. For more information on this report, please contact Public Safety Canada at: ps.communications-communications.sp@canada.ca
or at:

Communications Branch
Public Safety Canada
269 Laurier Ave. W.
Ottawa ON K1A 0S5

Catalogue Number:
PS4-245/2018E-PDF
International Standard Book Number (ISBN):
978-0-660-27887-2

Related publications (registration number: POR 130-16):

Catalogue Number PS4-245/2018E-PDF (Final Report, English)
ISBN 978-0-660-27887-2

EKOS RESEARCH ASSOCIATES

Contact: Susan Galley

Ottawa Office
359 Kent Street, Suite 300
Ottawa, Ontario
K2P 0R6
Tel: (613) 235 7215
Fax: (613) 235 8498
E-mail: pobox@ekos.com

www.ekos.com

SUMMARY

The use of Internet-enabled computer technology is ubiquitous across Canada. A priority of Public Safety Canada is to make the public aware of issues of security and safety and help Canadians stay safe from cyber threats. This survey gathers quantitative data on the knowledge, attitudes, and behaviours of Canadians who use the Internet to inform future communications and policy development initiatives. Interviews were completed with 2,072 Canadian adults from across the country who use the Internet. The cases were drawn from a random selection of Prob*it* panel members, a randomly recruited panel of Canadian households assembled through random digit dialling (RDD) methodology used in standard telephone survey sampling techniques.

A series of eight focus group discussions were also held across the country to discuss awareness of online security risks, types of actions taken and need for information.

Usage of the Internet

Survey results confirm that Canadians are using a variety of Internet-enabled devices to access the web on a daily basis, including not only desktop and laptop computers (93 per cent), but smartphones (76 per cent), tablets/readers (58 per cent), smart TVs (27 per cent), streaming services (25 per cent), gaming systems (21 per cent), and other devices. Virtually everyone has access from home, and almost nine in ten are using secure Wi-Fi in their home. Canadians spend an average of five hours online per day.

Canadians use the Internet for a wide variety of activities, with almost everyone using the Internet for email and browsing websites. Canadians also commonly use the Internet to perform financial transactions, follow the news, view videos and movies, make purchases, use social networking sites such as Facebook or Twitter, and/or access government information services. Email is the most ubiquitous source of risk with 98 per cent of Canadians engaging in this online activity.

Level of Concern and Awareness

Canadians who are actively using the Internet are very concerned about having their personal information obtained and used without permission as a result of their online activities. In fact, half say they are very concerned and, by and large, the remainder are moderately concerned. The importance of taking steps to protect personal information online and home computers is also not lost on Canadians with more than eight in ten seeing this as important. A similar proportion recognizes the importance of protecting mobile devices from online threats.

Canadians perceive online threats to be fairly commonplace today; 43 per cent believe it is very common for Canadians to be affected, and more than four in ten feel it is moderately common. In terms of one's own personal online security, one in three think it very likely they will be affected by an online threat in the near future, and another one in three believe it to be moderately likely.

The majority of Canadians online are aware of the threats individuals can face when using the Internet. Similar to the awareness levels in 2016, nine out of ten Canadians are aware of spyware/ malware on computer devices, being a victim of an online scam or fraud, and identity theft. Eight in ten are also familiar with privacy violations, and loss. More Canadians (three in four) are now aware of personal data held for ransom (a 12-point increase from 2016), as well as the loss of files or information, or personal data erased, changed, or lost. Almost all Canadians also report being aware of precautions they can take to protect themselves online, such as not sharing passwords, not opening email attachments from people they do not know, and limiting the personal information they share online, and using anti-virus/anti-spyware software. Virtually everyone is also aware that their laptop or computer can be affected by an online threat, and eight in ten are aware of the same potential for a smartphone or tablet/reader. This drops considerably, however, when it comes to awareness of possible risks to voice activated devices, smart TVs, or wearable devices.

Results suggest that Canadians' familiarity with crypto currency is quite limited and that its use is rare. Just under half of Canadians would consider themselves at least moderately familiar with the alternative currency and of those who are familiar, just one in ten have used it.

Level of Protective Measures Taken

The vast majority of Canadians say they are just as cautious – or even more cautious – when protecting themselves against online threats as they are in response to real-world threats. They report a strong repertoire of precautions they take to protect their devices and personal information online, including two in three or more who say they download files only from trusted sources, keep anti-virus software up-to-date, lock devices with password protection, password-protect their Wi-Fi, and generally use caution with unknown sources.

About nine in ten Canadians say that they refrain from sharing passwords, while eight in ten use complex passwords or exercise caution when giving out information like their real name, address, or phone number and when responding to solicitations from strangers. Roughly nine in ten say that they have anti-virus software installed on their computers. Other precautions that are used less often include changing default passwords, checking privacy policies, using multiple email accounts under a pseudonym, not using an administrator account when accessing the web, and using encryption software. There is a fairly significant increase from one in four Canadians in 2016 to now one in three Canadians who report using two-step authentication or biometric protection.

Nevertheless, many risky forms of behaviour are prevalent. Nearly half of Canadians report using the same passwords for multiple accounts, and four in ten allow their browsers to store their passwords. Also, between three in ten and four in ten Canadians never change their passwords, or do so only every few years, for social media, shopping, and email accounts. Younger Canadians (25 or younger) are more likely than older Canadians to be prompted to change their social media account passwords when they hear about a breach.

Although one in ten Canadians say they are less likely to take precautions against online threats when compared to in-person threats, three in ten are more likely to exercise caution in the digital world than the real world (and six in ten say they exercise the same degree of precaution).

Incidence of Victimization

The incidence of victimization from online attacks appears to be on the rise. More than half of Canadians (56 per cent) report having been a victim of a virus, spyware, or malware attack on the device(s) they use to access the Internet for personal use. Results also indicate that there is at least a moderate impact from these attacks for more than half, with one in five reporting a significant impact. Between five and 12 per cent have experienced identity theft and financial loss as a result of online activity.

Need for Information

Canadians have looked for a range of information about online threats, including protecting devices with anti-virus software (48 per cent), how to secure home networks (38 per cent), and how to tell if an email is a scam (38 per cent). Three in ten looked for information about how to protect devices and computer files (30 per cent), while one-quarter researched steps towards safe social networking. Use of public Wi-Fi, general terms related to cyber security, and cyberbullying were also sought out by about one in six. Most looked for this information using a general search engine (two in three) or from a vendor website (four in ten). Government websites or friends and family were consulted about a third of the time. Results suggest that most are looking for information proactively rather than trying to fix a problem that has already occurred, highlighting a willingness to take steps provided they have access to the information they need. This was echoed in the focus group discussions where many expressed an interest in a website with centralized information about general, and new security risks, and considerations for protective behaviours.

Two-thirds of Canadians are confident that they can protect themselves online as long as they have the basic information on steps to take, suggesting a need for concrete information, particularly for those less knowledgeable and confident. Six in ten feel that they have enough information on how to take steps to protect themselves against online threats, although one in four Canadians do not feel this way. Canadians are similarly mixed about whether they feel they have enough information to know how new technologies might affect their personal privacy, with half agreeing that this is the case and one in three disagreeing.

Canadians are mixed in their trust of a variety of sources in terms of the technical reliability, currency, and neutrality of information about online threats. Around half of Canadians trust law enforcement organizations, governments, and security software companies. Slightly fewer trust Internet service providers for current and reliable information about online threats. When Canadians are asked to indicate their most trusted source for unbiased information about online threats, law enforcement agencies and governments again top the list, with half of Canadians expressing confidence in these groups. Not-for-profit organizations rank third, while financial institutions, friends and family, private vendors, and security software companies are each trusted by one in four Canadians.

Most Canadians think that the responsibility for ensuring that web-enabled personal devices are safe and secure rests with the individual owners of the devices, suggesting again that they are willing to take action, provided they have the information they need to do it.

Canadians have varying interpretations of what constitutes “fake news”. About four in ten interpret the term to mean information that is falsely used to shape opinion or facts, although three in ten feel that it refers to information that comes from a biased source. There is no consensus on who should take charge in helping Canadians recognizing fake news, although the plurality of Canadians believe that governments should play a key role.

Concern Among Parents

Results suggest that while many parents feel that they have the information they need to protect their children online, a significant minority do not feel this to be the case. For example, while more than half feel that they are confident they have the information to help their child navigate online, one in four say they do not. Four in ten also agree that they cannot keep up with the apps, games, and other technology that young people are using. More than half say that they are concerned for their children’s privacy and also about cyberbullying and online harassment. Fewer (one in five to four in ten) are concerned with the legal implications of image and file sharing. Those parents who are not concerned about their children’s exposure to these threats say they have already spoken with their children about these issues, their children are not online to an extensive degree (more often among parents with younger children), their child receives sufficient information at school, or they trust their child to act appropriately.

Concerns Among Businesses

Although a survey of the general public, the research took the opportunity to ask those who are self-employed or in a managerial position in a small- to medium-sized company (i.e., with fewer than 250 employees) about their IT practices and level of concern when it comes to online protection. A total of 533 businesses were represented. Although one in four say that they are very concerned, half rated themselves as moderately concerned, and one in five say that are not concerned with work disruptions and/or financial loss from online threats. Among those unconcerned, this is most often because they feel that the threat is very low or they feel that they have researched and taken appropriate steps to protect the business.

Results show that there is as much need for improvement in security protection from online threats to businesses as there is among members of the public in their personal space. Between half and seven in ten employers require employees to password protect devices, keep security software up to date, use password authentication, back up information, and set spam filters. About half of the time, employees are asked to download only from trusted sources, use complex passwords, and click with caution when opening attachments and responding to email invitations. Slightly fewer instruct employees to not give out passwords, use caution when responding to solicitations from strangers, and change default passwords. Results also show that there is a strong appetite for information on a range of topics to help businesses identify and manage their risks from online threats. These include having a list of threats to look for, procedures for dealing with a cyber attack, steps to protect mobile devices in a public setting, best practices for storage of data, guidelines for employees' use of personal devices for work, and guidelines to establish rules for safe email usage policies, each of interest to at least four in ten businesses.

Segments of the Population

There are a number of repeating patterns found in the survey results. Younger Canadians are more active online, and tend to be more knowledgeable about online threats and security. Older Canadians are less active, but more concerned about security, and typically more apt to be looking for information and advice on how to protect themselves online. The generational divide is typically found with the younger boomers (with results looking quite different for those under 45 to 55, and those 45 to 55 and older). Socioeconomic status also provides a key demarcation, with those reporting higher education often reporting more online activity and awareness of the issue. Residents of Quebec report lower awareness of online threats and security, less concern about potential threats, and fewer protective measures taken.

The contract value for the POR project is $122,983.55 (including HST).

Supplier Name: EKOS Research Associates
PWGSC Contract Number: OD160192340/001/CY
Contract Award Date: August 13, 2018
To obtain more information on this study, please email info@GetCyberSafe.gc.ca