Gouvernement du Canada | Government of Canada

Sondage de suivi sur la connaissance de la campagne Pensez cybersécurité

Sommaire

Préparé pour le Centre de la sécurité des télécommunications Canada

Nom de la firme de recherche : LES ASSOCIÉS DE RECHERCHE EKOS INC.
Numéro de contrat : 2L165-220295/001/CY
Valeur du contrat : 63 991,29 $
Date d'attribution des services : 13 décembre 2021
Date de livraison des services : 15 mars 2022

Numéro d'enregistrement : ROP 070-21

Pour obtenir de plus amples renseignements sur ce rapport, veuillez communiquer avec CST à media@cse-cst.gc.ca

This report is also available in English

Canada

Sondage de suivi sur la connaissance de la campagne Pensez cybersécurité

Sommaire

Préparé pour le Centre de la sécurité des télécommunications Canada
Nom du fournisseur : **LES ASSOCIÉS DE RECHERCHE EKOS INC.**
Date : Mars 2022

Cette recherche sur l'opinion publique présente les résultats d'un sondage en ligne mené par Les Associés de recherche EKOS inc. pour le compte du Centre de la sécurité des télécommunications Canada. Cette étude a été menée auprès de 2 050 Canadiens entre le 21 janvier et le 14 février 2022.

This publication is also available in English under the title: Get Cyber Safe Awareness Tracking Survey.

Direction générale des Communications
Services publics et Approvisionnement Canada
Portage III Tour A
16A1-11 rue Laurier
Gatineau QC K1A 0S5

Numéro de catalogue : D96-17/2022F-PDF
Numéro international normalisé du livre (ISBN) : 978-0-660-42689-1

Publications connexes (numéro d'enregistrement : ROP 070-21)
D96-17/2022E-PDF (English)
978-0-660-42688-4

SOMMAIRE

A. CONTEXTE ET OBJECTIFS

Puisque les Canadiens sont les plus grands utilisateurs d'Internet au monde, il importe qu'ils comprennent bien les enjeux de cybersécurité et qu'ils s'y conforment pleinement. Pour ce faire, il est essentiel qu'ils soient en mesure de reconnaître une cybermenace, qu'ils connaissent les mesures à prendre pour combattre ces menaces, qu'ils connaissent les sources d'information fiables sur la façon de naviguer sur le Web en toute sécurité et qu'ils s'engagent à protéger leur identité, celle d'autrui ainsi que les appareils dotés d'une connexion Internet. Voilà pourquoi la Stratégie de cybersécurité du Canada comprend une évaluation des connaissances de la population et de son engagement à l'égard de la cybersécurité, et la mise en œuvre de la campagne de sensibilisation Pensez cybersécurité, dont l'objectif est d'améliorer les connaissances et la compréhension du public dans ce domaine.

Voici les objectifs de ce projet de recherche :

- Évaluer le rendement de la campagne de sensibilisation publique.
- Définir le niveau de connaissance, les attitudes et les comportements des publics cibles de la campagne de sensibilisation en matière de cybersécurité.
- Déterminer les facteurs de motivation et les obstacles au changement de comportement, et en faire le suivi.
- Cerner et faire le suivi des meilleures façons de communiquer ces renseignements.
- Assurer le suivi des attentes du public en ce qui a trait à la participation des gouvernements provinciaux et fédéral, d'administrations municipales, et d'organismes non gouvernementaux.

B. MÉTHODOLOGIE

L'échantillon se compose de 2 050 entretiens réalisés avec des Canadiens âgés de 16 ans ou plus qui utilisent régulièrement Internet, y compris 553 entrevues avec des parents d'enfants de moins de 18 ans, et 301 entretiens avec des Canadiens qui occupent un poste de direction dans une PME comptant entre un et cent employés. L'échantillon se fonde sur une sélection aléatoire de membres du panel Prob*it* de partout au pays. Les panélistes de Prob*it* ont été sélectionnés pour former une base de sondage hybride recruté sur des téléphones cellulaires et des lignes terrestres à l'aide d'un système à composition aléatoire. Ce panel, qui regroupe plus

de 120 000 membres, peut être tenu comme représentatif de la population canadienne (c'est-à-dire qu'une population cible donnée comprise dans notre panel correspond de très près à l'ensemble de la population), et il est donc possible de lui attribuer une marge d'erreur.

Dans le cadre du présent sondage, un échantillon de 12 295 personnes a été créé à partir du volet en ligne seulement du panel Prob*it.* Les sondages ont été réalisés en ligne seulement, car il s'agit de la portion précise de la population canadienne que ciblerait la campagne de communications. Le taux de participation s'est établi à 17 %. L'échantillon du sondage final, en vertu duquel 2 050 sondages ont été achevés, présente un niveau de précision de +/-2,2 % pour l'échantillon dans son ensemble et de +/- 3 à 6 % pour la plupart des sous-groupes qui ont pu être isolés dans l'analyse (y compris pour tous les segments relatifs aux régions, aux groupes d'âge, au niveau de scolarité et au revenu).

Avant de lancer le sondage, le questionnaire a été mis à l'essai 41 fois en anglais et 20 fois en français. Le sondage bilingue a été mené en ligne entre le 21 janvier et le 14 février 2022 et a pris 15 minutes en moyenne à compléter en ligne. La base de données a ensuite fait l'objet d'un examen afin d'analyser la qualité, les valeurs aberrantes, les exigences en matière de codage, la pondération et la construction de variables indépendantes, ce qui a servi à établir les tendances des sous-groupes (p. ex. par âge, par sexe, etc.) dans l'analyse. La pondération de l'échantillon se fondait sur les paramètres de la population du plus récent recensement en ce qui concerne l'âge, le sexe, et la région du pays.

C. PRINCIPALES CONSTATATIONS

Niveau de préoccupation

La plupart des Canadiens ne croient pas probable qu'ils soient touchés par une cybermenace. Plus d'une personne sur dix se dit préoccupée par la possibilité d'être touchée par une cybermenace qui compromettrait ses renseignements personnels, et moins d'une personne sur dix est préoccupée par une menace pouvant entraîner des pertes financières, la perte de fichiers ou de photos, ou la possibilité que leurs données soient conservées en vue d'obtenir une rançon. En combinant la probabilité dans les trois domaines, cependant, moins d'un Canadien sur dix croit qu'il est probable qu'il soit la victime d'une cybermenace au cours de la prochaine année, en grande partie en raison de la probabilité plus élevée que certains renseignements personnels soient compromis. Lorsqu'il est question de cybermenaces, trois Canadiens sur quatre craignent un vol d'identité. Les autres menaces les plus importantes qui viennent à l'esprit des Canadiens sont les virus, les logiciels espions, les logiciels malveillants et les pertes financières. La plupart des Canadiens qui disent ne pas être préoccupés par les

cybermenaces affirment que c'est parce qu'ils prennent des mesures pour se protéger en ligne ou parce qu'ils ne font rien de risqué sur le Web.

Connaissance

Certains Canadiens connaissent des mesures à prendre pour s'assurer qu'un site Web est sécurisé. La plupart d'entre eux recherchent des sites Web d'une source fiable, comme un fournisseur de logiciels bien connu ou un site Web d'un gouvernement, ou n'utilisent que les sites Web qu'ils connaissent bien. Moins de la moitié recherche des adresses « https » pour s'assurer qu'un site Web est sécurisé ou s'assure que le site présente le symbole de verrouillage de sécurité.

Un Canadien sur quatre ne croit pas être prêt à faire face aux cybermenaces, principalement parce qu'il est d'avis qu'on ne peut jamais vraiment se protéger en ligne. En fait, un répondant sur quatre dit avoir été victime d'un virus, d'un logiciel espion ou d'un logiciel malveillant sur son ordinateur, ou d'une fraude par courriel. Parmi les autres cyberattaques mentionnées figurent les tentatives d'hameçonnage, les arnaques par texto et le piratage de comptes de médias sociaux. Quelques personnes mentionnent le vol d'identité et les rançongiciels.

En cas de cyberattaque, quatre Canadiens sur cinq changeraient leurs mots de passe. Sept répondants sur dix communiqueraient avec leur banque. Plus de la moitié supprimerait du matériel suspect ou mettrait à jour son logiciel de sécurité.

Mesures de précaution

Comme dans les éditions antérieures de l'enquête, près de neuf Canadiens sur dix prennent des mesures de précaution pour protéger leurs comptes de médias sociaux et d'autres comptes en ligne, leurs appareils et leurs réseaux. La plupart des gens disent qu'il est préférable d'utiliser des mots de passe complexes avec une combinaison de lettres, de chiffres et de symboles. Plus de deux Canadiens sur trois utilisent une authentification à facteurs multiples dans leurs activités en ligne. Pour ces Canadiens, l'authentification comprend le plus souvent un code reçu par texto (pour près de neuf personnes sur dix), suivie par un code reçu par courriel, un mot de passe ou un NIP (pour environ deux personnes sur trois). La plupart des Canadiens, soit neuf personnes sur dix, protègent leur réseau sans fil avec un mot de passe unique. Néanmoins, seul un Canadien sur six utilise un mot de passe distinct pour les visiteurs.

Près de trois Canadiens sur quatre effectuent des copies de sécurité de leurs fichiers sur le disque dur de leur ordinateur. Plus de la moitié stockent leurs données sur un disque dur externe. De plus en plus de Canadiens ont recours à un serveur virtuel ou à un service infonuagique. Pour une personne sur cinq, les données et les fichiers personnels stockés sur

leur ordinateur, leur téléphone intelligent ou un autre appareil mobile sont automatiquement sauvegardés sur un nuage informatique. Une proportion semblable sauvegarde manuellement ses fichiers une ou deux fois par année. Une personne sur six ne fait jamais de copies de sécurité.

Information

Deux Canadiens sur cinq recherchent des renseignements sur les types de cybermenaces ou sur la façon de savoir si un courriel est une escroquerie. Plus d'un répondant sur trois a recherché des renseignements sur la sécurité de son réseau sans fil à la maison ou sur la façon de protéger ses appareils mobiles. Près de la moitié des Canadiens a recours à un moteur de recherche pour trouver ces renseignements. Environ trois personnes sur dix recherchent de l'information sur un site Web du gouvernement, sur le site Web d'un fournisseur de logiciels ou de matériel informatique, dans les médias (y compris sur le site Web d'un organisme de presse), ou par le biais d'amis et de membres de leur famille. Le service des TI d'un employeur est une source d'information pour un répondant sur trois qui recherche de l'information. Il s'agit plus souvent d'une source chez les personnes âgées de 25 à 54 ans et chez celles dont le niveau de scolarité est plus élevé. La plupart des répondants trouvent les renseignements utiles parce qu'ils se fient à la source de l'information.

Plus de la moitié des Canadiens préfèrent obtenir des renseignements sur la cybersécurité par l'entremise de sites Web. Trois personnes sur dix préfèrent recourir à des listes de choses à faire, à des fiches d'information et à de l'infographie. Environ une personne sur cinq dit préférer des vidéos didactiques, des histoires sur la façon dont les gens sont touchés, des publications dans des médias sociaux ou des bulletins, comme des abonnements par courriel.

Comme nous l'avons constaté en 2018 et en 2020, si des renseignements fiables sont fournis, deux Canadiens sur trois croient pouvoir se protéger en ligne ou trouver de l'information pratique en ligne pour se protéger contre les cybermenaces. Près de trois personnes sur cinq conviennent qu'il est de la responsabilité des particuliers de protéger leurs renseignements personnels.

Très peu de répondants ont entendu parler de la campagne Pensez cybersécurité. Parmi le répondant sur dix qui affirme connaître la campagne en entendant son nom, un sur trois dit avoir vu quelque chose aux nouvelles ou avoir lu une publication dans des médias sociaux. Plus d'une personne sur quatre a vu une vidéo en ligne sur la campagne Pensez cybersécurité. Près d'une personne sur cinq en a entendu parler dans une émission de radio ou dans un balado, sur le site Web pensezcybersecurite.gc.ca ou par le bouche-à-oreille.

Expérience d'entreprises

Parmi les préoccupations des propriétaires ou gestionnaires d'entreprise dans les opérations quotidiennes, seules trois personnes sur dix sont préoccupées par de possibles interruptions de travail ou pertes financières. Une moins grande proportion se préoccupe de l'atteinte à la réputation de l'organisation que peut causer une cybermenace ou de la possibilité que des données de leur entreprise soient conservées en vue d'obtenir une rançon. À l'instar de 2018 et de 2020, moins de la moitié des répondants n'a aucune crainte, car les répondants estiment que peu de menaces pèsent sur les entreprises comme la leur. Ce taux est plus élevé chez les personnes ayant fait des études universitaires. Une personne sur quatre effectue des recherches et prend des mesures pour protéger son entreprise en ligne. Plus de deux propriétaires ou gestionnaire d'entreprise sur trois déclarent que leur entreprise prend des mesures pour protéger tous ses appareils avec un mot de passe. Une moindre proportion, mais tout de même plus de la moitié, garde les logiciels de sécurité à jour sur tous les dispositifs, utilise un mot de passe ou un système d'authentification d'utilisateur pour l'accès sans fil et à distance, ou effectue des copies de sécurité de tous les dispositifs.

La moitié des propriétaires ou gestionnaires d'entreprise affirme que son entreprise tirerait profit de directives pour réagir à une cyberattaque ainsi que d'une liste de types de menaces qui existe et de signaux à rechercher. Deux de ces répondants sur cinq croient qu'il leur serait utile de connaître des mesures à prendre pour protéger les appareils mobiles dans un lieu public, des pratiques exemplaires traitant de la façon pour les employés de gérer les mots de passe, des pratiques exemplaires sécuritaires avec les services infonuagiques, des ressources traitant de la façon de crypter des ordinateurs, des conseils et ressources relatifs au type de logiciel ou de matériel permettant de sécuriser des réseaux, des directives concernant la mise en place des règles en lien avec une politique d'utilisation sécuritaire des courriels, des pratiques exemplaires traitant de l'utilisation de dispositifs de stockage ou des pratiques exemplaires traitant de l'établissement d'une politique claire en matière d'utilisation d'Internet.

Près de la moitié des propriétaires ou gestionnaires d'entreprise croit qu'il faudrait un certain effort pour se remettre de l'attaque d'un rançongiciel ou qu'il serait difficile de s'en remettre. Deux propriétaires ou gestionnaires d'entreprise sur trois ont des employés qui travaillent à la maison au moins à temps partiel. Des instructions supplémentaires sont fournies à ces employés sur les différentes façons de protéger l'entreprise contre les cybermenaces lors de travail à domicile. Les principales instructions portent sur l'utilisation d'un logiciel antivirus, sur l'authentification à facteurs multiples, sur l'utilisation d'un pare-feu ou sur les copies de sécurité de renseignements. Les propriétaires ou gestionnaires d'entreprise citent de nombreux types d'informations nécessaires pour protéger leur entreprise contre les cybermenaces. La

moitié d'entre eux mentionnent la nécessité de directives pour réagir à une cyberattaque et une liste de types de menaces qui existe et de signaux à rechercher.

D. NOTE AUX LECTEURS

Les résultats détaillés de l'étude sont présentés dans les sections ci-dessous. Les résultats globaux sont présentés dans la section principale du rapport et sont normalement appuyés par un graphique ou une présentation tabulaire. Des textes à puces sont également utilisés pour mettre en évidence des différences statistiques importantes entre des sous-groupes de répondants. Si aucune différence n'est soulignée dans le rapport, cela signifie que la différence n'est statistiquement pas considérable[1] par rapport aux résultats globaux ou que cette différence est considérée comme beaucoup trop faible pour être digne de mention. Le questionnaire du sondage se trouve à l'annexe A. L'annexe B contient des détails sur la méthodologie et les caractéristiques de l'échantillon.

Il est à noter que le sondage comprenait un certain nombre de questions sur les comportements qui pourraient avoir tendance à exercer de la pression de désirabilité sociale chez les répondants, les incitant à mettre un bémol sur leurs pratiques risquées en ligne[2]. Les résultats pour la proportion de répondants de l'échantillon qui ont répondu « je ne sais pas » ou qui n'ont pas fourni une réponse peuvent ne pas être indiqués dans la représentation graphique des résultats, particulièrement lorsqu'ils ne sont pas appréciables (p. ex., 10 % ou moins). Aussi, il est possible que les résultats ne donnent pas 100 % en raison des arrondissements.

[1] Dans la mesure du possible, un test du chi carré et un test T standard ont été utilisés. Les différences notées étaient importantes dans une proportion de 95 %.

[2] Ivar Krumpal, « Determinants of Social Desirability Bias in Sensitive Surveys: A Literature Review », Quality and Quantity, juin 2013, Volume 47, numéro 4, p. 2025-2047.

E. CERTIFICATION DE NEUTRALITÉ POLITIQUE

À titre de cadre supérieur des Associés de recherche EKOS Inc., j'atteste par la présente que les documents remis sont entièrement conformes aux exigences de neutralité politique du gouvernement du Canada exposées dans la Politique de communication du gouvernement du Canada et dans la Procédure de planification et d'attribution de marchés de services de recherche sur l'opinion publique.

En particulier, les documents remis ne contiennent pas de renseignements sur les intentions de vote électoral, les préférences quant aux partis politiques, les positions des partis ou l'évaluation de la performance d'un parti politique ou de ses dirigeants.

Signé par : 

Susan Galley (Vice-présidente)