Government of Canada | Gouvernement du Canada

Sondage de suivi sur la connaissance de la campagne Pensez cybersécurité

Sommaire

Préparé pour le Centre de la sécurité des télécommunications Canada

Fournisseur : LES ASSOCIÉS DE RECHERCHE EKOS INC.
No du contrat : 2L165-200745/001/CY
Valeur de l'entente : 82 958,08 $
Date du contrat : 2 mars 2020
Date de livraison : 31 mars 2020

No d'inscription : POR 086-19

Pour de plus amples renseignements au sujet de ce rapport, veuillez communiquer avec CST at: 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 : 31 mars 2020

Ce rapport de 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. L'étude de recherche a été menée auprès de 2 700 Canadiens du 16 au 29 mars 2020.

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

Secteur des communications
Services publics et Approvisionnement Canada
11 rue Laurier, Phase III, Place du Portage
Gatineau QC K1A 0S5

Numéro de catalogue : D96-17/2020F-PDF

Numéro international normalisé du livre (ISBN) : 978-0-660-34870-4

Publications connexes (numéro d'enregistrement : POR 086-19) :

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.

B. MÉTHODOLOGIE

L'échantillon se compose de 2 710 entretiens réalisés avec des Canadiens âgés de 16 ans ou plus qui utilisent régulièrement Internet, y compris 350 entrevues avec des jeunes âgés de 16 à 24 ans, et 350 entrevues avec des Canadiens qui occupent un poste de direction dans une PME comptant entre un et cent employés, ou qui en sont propriétaire. 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 15 312 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 18 %. L'échantillon du sondage final, en vertu duquel 2 710 sondages ont été achevés, présente un niveau de précision de +/-1,9 % 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 14 fois en anglais et 10 fois en français. Le sondage bilingue a été mené en ligne du 16 au 29 mars 2020. 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 estiment peu probable qu'ils soient touchés par une cybermenace. Moins d'une personne sur cinq se dit préoccupée par la possibilité d'être touchée par une cybermenace qui compromettrait ses renseignements personnels et moins d'une personne sur dix se dit préoccupée par une menace pouvant entraîner une perte financière ou la perte de fichiers ou de photos. Toutefois, lors de la combinaison des probabilités associées à l'ensemble des domaines, un Canadien sur cinq considère comme probable qu'il soit touché par une cybermenace au cours de la prochaine année, ce qui est en grande partie le résultat de la tendance plus marquée qu'ont les répondants à estimer que leurs renseignements personnels pourraient être compromis. Un peu plus du tiers des répondants est d'avis qu'il est peu probable qu'il soit touché par l'une ou l'autre des cybermenaces. Une proportion un peu plus élevée, soit une personne sur quatre, croit qu'il est probable qu'un membre de sa famille ou un(e) ami(e) soit touché(e) par une cybermenace au cours de la prochaine année. Lorsqu'il est question de cybermenaces, trois Canadiens sur quatre craignent le vol de leur identité. Les autres menaces évoquées sont celles entraînant une perte financière, suivies par les virus en général, les logiciels espions ou les logiciels malveillants.

Connaissance

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. Une portion des Canadiens connaît les mesures à prendre pour s'assurer qu'un site Web est sécurisé. La plupart d'entre eux recherchent des sites Web provenant d'une source digne de confiance, comme un fournisseur de logiciels bien connu ou le gouvernement. Moins de la moitié utilise uniquement des sites Web qu'il connaît bien, s'assure que le site a une adresse « https » ou s'assure que le site est authentifié par un symbole ou la marque VeriSign.

Un Canadien sur quatre croit ne pas être préparé pour faire face à une cybermenace, principalement parce qu'on ne peut jamais vraiment se protéger en ligne. En fait, deux personnes sur cinq disent avoir été victimes d'un virus, d'un logiciel espion ou d'un logiciel malveillant sur leur ordinateur et plus du quart a été victime d'un courriel frauduleux. Parmi les autres cyberattaques figurent la fraude par texto, le piratage de comptes de médias sociaux et le vol d'identité.

S'ils étaient victimes d'une cyberattaque, quatre Canadiens sur cinq changeraient leurs mots de passe et plus de deux personnes sur trois communiqueraient avec leur banque. Un peu moins de répondants affirment qu'ils supprimeraient du matériel suspect ou qu'ils mettraient à jour leur logiciel de sécurité.

Précautions

Tout comme en 2018, près de neuf Canadiens sur dix prennent des précautions pour protéger leurs comptes en ligne, leurs comptes de médias sociaux, leurs appareils et leurs réseaux. Cependant, près de deux personnes sur trois déclarent changer plus souvent leurs mots de passe que d'autres. Un répondant sur quatre change ses mots de passe au moins quelques fois par année, mais une personne sur dix ne les change jamais. Les mots de passe des comptes de services bancaires en ligne sont ceux qui sont les plus souvent modifiés (par trois personnes sur cinq). 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 la moitié des Canadiens utilisent une authentification multifactorielle dans certaines activités en ligne. Pour ces gens, l'authentification comprend le plus souvent un code reçu par message texte (quatre personnes sur cinq), suivie par des mots de passe, un code reçu par courriel ou un NIP (deux personnes sur trois). La plupart des ménages canadiens, soit neuf personnes sur dix, protègent leur réseau Wi-Fi avec un mot de passe unique. Néanmoins, un seul Canadien sur six utilise un mot de passe distinct pour les visiteurs.

Près de trois Canadiens sur quatre sauvegardent leurs fichiers sur le disque dur de leur ordinateur. Plus de la moitié stockent leurs données sur un disque dur externe et moins de répondants, bien que cette proportion soit plus élevée qu'en 2018, ont recours à un hébergeur virtuel ou à un nuage. 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. Une proportion semblable sauvegarde manuellement ses fichiers une ou deux fois par année, tandis qu'une personne sur six ne les sauvegarde jamais.

Information

Un peu moins de la moitié des Canadiens recherche de l'information sur la façon de savoir si un courriel est frauduleux ou sur les divers types de cybermenaces. Plus du tiers des répondants recherche des renseignements sur la sécurité du réseau Wi-Fi à domicile ou sur la protection des appareils mobiles. Trois Canadiens sur cinq ont recours à un moteur de recherche pour trouver ces renseignements. Environ trois personnes sur dix trouvent des renseignements par le biais de médias, notamment du site Web d'un organe de presse, d'un gouvernement, d'un fournisseur de services Internet ou de logiciels, ou par l'intermédiaire d'amis et de membres de leur famille. Le service des TI de l'employeur constitue une source d'information pour le quart des personnes qui recherchent de l'information. Un peu plus d'une personne sur quatre considère l'information comme utile si elle a confiance dans la source d'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 ou à de l'infographie. Une personne sur cinq dit préférer des vidéos didactiques, des médias sociaux, des histoires sur la façon dont les gens ont été touchés ou des bulletins d'information, comme des abonnements à un courriel.

Trois Canadiens sur dix aident d'autres personnes avec la cybersécurité. Six personnes sur dix aident leurs parents ou des amis. Moins de la moitié des répondants aident d'autres membres de leur famille. Environ trois personnes sur dix aident des collègues ou leurs enfants.

Comme en 2018, deux Canadiens sur trois sont convaincus de pouvoir se protéger en ligne s'ils ont accès à des renseignements dignes de confiance. Plus de trois personnes sur cinq sont d'accord pour dire qu'il leur appartient de protéger leurs renseignements personnels ou sont convaincues de savoir comment trouver des renseignements pratiques en ligne pour se protéger en ligne.

Très peu de répondants ont entendu parler de la campagne Pensez cybersécurité. Environ 30 % des répondants qui affirment connaître la campagne en entendant son nom disent l'avoir vu dans des médias sociaux. Le quart des répondants a vu un segment aux nouvelles ou dans des médias sociaux. Près d'une personne sur cinq en a entendu parler d'une personne, dans une émission de radio, dans un fichier balado, dans une vidéo en ligne ou sur le site Web pensezcybersecurite.gc.ca.

Expérience d'entreprises

Parmi les préoccupations liées aux activités quotidiennes des propriétaires ou des gestionnaires d'entreprise, seule une personne sur quatre se préoccupe des interruptions de travail, des pertes financières ou de l'atteinte à la réputation de l'organisation que peuvent causer les cybermenaces. Comme en 2018, deux personnes sur cinq ne sont pas préoccupées, car elles estiment que peu de menaces pèsent sur les entreprises comme la leur. Une personne sur cinq effectue des recherches et prend des mesures pour protéger son entreprise en ligne. Un peu plus de la moitié des propriétaires ou des gestionnaires d'entreprise signalent que leur entreprise exige une protection par mot de passe sur tous les dispositifs, qu'elle utilise un mot de passe ou un système d'authentification d'utilisateur pour l'accès sans fil et à distance, ou qu'elle utilise un logiciel de sécurité à jour sur tous ses ordinateurs.

Deux propriétaires ou gestionnaires d'entreprise sur cinq déclarent que leur organisation tirerait profit d'une liste de menaces existantes, de signaux à surveiller, de directives à suivre pour réagir à une cyberattaque ou de mesures à prendre pour protéger les appareils mobiles dans un lieu public. Plus de trois personnes sur dix considèrent comme important d'avoir accès à des renseignements traitant de pratiques exemplaires sur la sécurité des services infonuagiques, de ressources sur la façon de crypter des ordinateurs, des portables et des dispositifs de stockage, de pratiques exemplaires sur l'utilisation de dispositifs de stockage ou de directives sur l'utilisation de dispositifs personnels au travail. Environ une personne sur quatre indique que son organisation tirerait profit de conseils sur le type de logiciel ou matériel permettant de sécuriser des réseaux, de pratiques exemplaires sur la façon pour les employés de gérer les mots de passe, de directives pour mettre en place des règles relatives à la politique d'utilisation sécuritaire des courriels, de directives sur la façon d'établir une politique solide en matière de médias sociaux, de conseils pour communiquer aux employés l'importance de suivre de politiques de cybersécurité, de pratiques exemplaires pour une politique d'utilisation d'Internet claire et de mesures pour gérer les renseignements liés au travail que possèdent les employés qui quittent l'organisation.

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.

E. VALEUR DE L'ENTENTE

La valeur du contrat du projet de sondage sur l'opinion publique est de 82 958,08 $ (TVH incluse).

Nom du fournisseur : Les Associés de recherche EKOS
No de contrat – TPSGC : 086-19
Date d'attribution du contrat : 2 mars 2020
Pour obtenir de plus amples renseignements sur cette étude, veuillez envoyer un courriel à CST at: media@cse-cst.gc.ca.

[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.

F. 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)