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 du fournisseur : Phoenix Strategic Perspectives Inc.
Numéro de contrat : CW2346933
Valeur du contrat : 81 085,41 $ (incluant les taxes applicables)
Date d'attribution du contrat : 2024-01-23
Date de présentation du rapport : 2024-03-31
Numéro d'enregistrement : POR nº 119-23

Pour plus d'information sur le présent rapport, veuillez communiquer avec le CST à l'adresse : 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 par le Centre de la sécurité des télécommunications
Nom du fournisseur : Phoenix Strategic Perspectives Inc.
Avril 2024

Le présent rapport de recherche sur l'opinion publique présente les résultats d'un sondage en ligne mené par Phoenix SPI auprès de 2 222 Canadiens et Canadiennes de 18 ans et plus pour le compte du Centre de la sécurité des télécommunications (CST) entre le 29 février et le 19 mars 2024.

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

Numéro de catalogue :
D96-17/2024F-PDF

Numéro international normalisé du livre (ISBN) :
978-0-660-72843-8

Publications connexes (numéro d'enregistrement : POR n° 119-23) :
Numéro de catalogue : D96-17/2024E-PDF
ISBN : 978-0-660-72842-1

Sommaire

Le Centre de la sécurité des télécommunications (CST) a chargé Phoenix Strategic Perspectives Inc. (Phoenix SPI) de réaliser le sondage de suivi biennal en ligne sur la connaissance de la campagne Pensez cybersécurité.

Contexte et objectifs

Le CST est l'organisme national de cryptologie chargé de préserver, pour le gouvernement du Canada, la sécurité des technologies de l'information et de recueillir du renseignement électromagnétique étranger. Dans le cadre de ses activités axées sur la cybersécurité, le CST exploite le Centre pour la cybersécurité, qui est la source unifiée d'avis, de conseils, de services et de soutien spécialisés en matière de cybersécurité pour la population canadienne. Depuis 2018, le CST dirige la campagne nationale de sensibilisation du public Pensez cybersécurité, qui a été créée pour renseigner les Canadiens et les Canadiennes au sujet de la cybersécurité et des mesures simples qu'ils peuvent prendre pour se protéger en ligne.

À l'appui de la campagne Pensez cybersécurité, le CST a mené une recherche sur l'opinion publique (ROP) axée sur les attitudes et les comportements des Canadiens et des Canadiennes en ligne. La ROP a d'abord pris la forme d'un sondage téléphonique national en 2020, suivi d'un sondage national en ligne en 2022 (pour suivre les changements au fil du temps). Auparavant, Sécurité publique Canada avait mené une ROP pour la campagne Pensez cybersécurité en 2011, 2017 et 2018. Les deux enquêtes ont été conçues dans le but de recueillir des données sur les connaissances et les attitudes de la population canadienne en ligne à l'égard de la cybersécurité dans le contexte de la campagne de sensibilisation du public Pensez cybersécurité.

Au printemps 2022, le CST a également effectué un sondage distinct à titre de contribution au rapport intitulé *Oh Behave! Rapport annuel sur les attitudes et comportements en matière de cybersécurité*, qui n'était auparavant mené qu'aux États-Unis et au Royaume-Uni. Le rapport *Oh Behave!* est un rapport de recherche annuel qui vise à mieux comprendre les attitudes et les comportements des gens en matière de sécurité. Un volet canadien a été ajouté pour l'enquête de 2022, qui mettait l'accent sur le facteur humain du cyberrisque, en particulier les comportements de cybersécurité de base, comme la création et la gestion de mots de passe, l'application de l'authentification multifactorielle (AMF), l'installation des plus récentes mises à jour, la vérification de la légitimité des messages, la reconnaissance et le signalement des tentatives d'hameçonnage et la sauvegarde des données.

Pour cette itération de l'enquête, le sondage de 2022 du CST sur la campagne Pensez cybersécurité et le sondage *Oh Behave!* de 2024 ont été fusionnés en vue de créer un questionnaire complet qui permettrait de faire ce qui suit :

- évaluer l'efficacité de la campagne de sensibilisation du public;
- aider à cerner les changements dans les connaissances, les comportements et les attitudes;
- réaliser un suivi de la sensibilisation, des attitudes et des comportements liés aux activités de cybersécurité;

- déterminer et suivre les facteurs de motivation et les obstacles au changement de comportement;
- déterminer et suivre les meilleures façons de communiquer l'information;
- réaliser un suivi des attentes du public en ce qui a trait à la participation du gouvernement fédéral.

La ROP de cette année éclairera l'orientation de la campagne Pensez cybersécurité, ainsi que d'autres communications et messages publics du CST. Les résultats de la recherche seront utilisés à deux fins. Ils aideront la campagne Pensez cybersécurité à sensibiliser la population canadienne à la sécurité en ligne, en plus de soutenir les futures activités de politique et de communication du Centre pour la cybersécurité et du CST.

Méthodologie

Un sondage en ligne de 15 minutes a été mené auprès de 2 222 Canadiens et Canadiennes en ligne de 18 ans et plus. Entre autres, 619 parents d'enfants de moins de 18 ans y ont répondu, tout comme 301 personnes qui sont propriétaires ou gestionnaires d'une petite et moyenne entreprise comptant un effectif d'au plus 100 personnes.

L'échantillon est tiré de l'échantillon populationnel aléatoire d'Advanis, qui a été développé à l'aide d'un recrutement fondé sur les probabilités, plus précisément de la méthode de composition aléatoire par l'entremise de la réponse vocale interactive et d'entrevues téléphoniques assistées par ordinateur (ETAO) en direct. Ce panel de plus de 600 000 personnes peut être considéré comme représentatif du grand public au Canada.

Les résultats ont été pondérés pour refléter la répartition réelle des Canadiens et des Canadiennes selon la région, l'âge et le genre. La marge d'erreur pour un échantillon de cette taille est de ±2 %, 19 fois sur 20. Les marges d'erreur sont plus grandes pour les résultats relatifs aux sous-groupes de l'échantillon total. Le travail sur le terrain a été effectué du 29 février au 19 mars 2024. De plus amples renseignements sur la méthodologie se trouvent à l'annexe Spécifications techniques.

Principales constatations

Les pratiques de cybersécurité des Canadiens et des Canadiennes en ligne

La grande majorité des Canadiens et des Canadiennes en ligne (86 %) ont déclaré qu'ils prenaient des précautions pour protéger leurs comptes en ligne et dans les médias sociaux, ainsi que leurs appareils et réseaux. Les deux tiers (65 %) ne supposent pas que leurs appareils sont automatiquement sécurisés.

Huit personnes sur 10 (81 %) savent comment installer les plus récentes mises à jour de logiciels et d'applications sur leurs appareils. Parmi ces répondants, près de neuf personnes sur 10 (88 %) le font régulièrement et près de la moitié (48 %) le font toujours lorsqu'ils sont avisés que des mises à jour sont disponibles. Les personnes qui installent régulièrement des mises à jour ont tendance à le faire immédiatement : 51 % ont activé la fonction des mises à jour automatiques et 19 % procèdent à la mise à jour dès qu'ils reçoivent une notification à cet effet.

En plus d'installer des mises à jour, les Canadiens et les Canadiennes en ligne sont au courant des mesures possibles pour sécuriser leurs comptes et ont tendance à les utiliser. Neuf répondants sur 10 (90 %) ont entendu parler de l'authentification multifactorielle (AMF) et la plupart des personnes qui connaissent l'AMF (87 %) savent comment l'activer et l'utilisent régulièrement. Les gens qui n'utilisent pas régulièrement l'AMF doivent être convaincus de l'utilité de cette mesure de sécurité supplémentaire. Quatre non-utilisateurs sur 10 (39 %) ne croient pas que l'AMF mettra un terme aux activités des cybercriminels, 24 % ne voient aucun avantage à utiliser l'authentification multifactorielle, 21 % considèrent que cela n'est pas nécessaire si leur appareil fonctionne et 19 % ne comprennent tout simplement pas comment l'utiliser. Parmi les personnes qui n'utilisent plus l'authentification multifactorielle, la plus grande proportion (29 %) d'entre elles ont indiqué que l'authentification multifactorielle prend trop de temps.

En ce qui concerne les mots de passe, un peu plus des trois quarts (76 %) des Canadiens et des Canadiennes en ligne optent pour des mots de passe complexes en utilisant une combinaison de lettres, de chiffres et de symboles. De plus petites proportions de répondants utilisent un mot de passe unique pour chaque compte (35 %), un gestionnaire de mots de passe (30 %) ou un mot de passe de quatre à 15 caractères (27 %). Pour les comptes en ligne importants, la moitié des personnes se servent de mots de passe uniques en tout temps (31 %) ou la plupart du temps (27 %).

Alors que de nombreux Canadiens et des Canadiennes adoptent des pratiques qui aideront à protéger leurs comptes en ligne, certains ont déclaré que certaines mesures *pourraient* mettre leur compte en danger : 39 % permettent aux navigateurs ou aux applications d'inscrire automatiquement leurs mots de passe, 36 % prennent en note leurs mots de passe, 31 % utilisent le même mot de passe pour plusieurs comptes, 10 % optent pour des mots de passe simples et faciles à retenir et 2 % divulguent leur mot de passe.

De plus, les Canadiens et les Canadiennes prennent des mesures pour vérifier la légitimité d'un site Web. La majorité des répondants analysent l'aspect général du site Web (58 %) ou vérifient si la barre d'adresse (54 %) contient « https ». Bon nombre de personnes vérifient également si la barre d'adresse du site Web renferme un cadenas verrouillé (45 %) ou mènent des recherches pour valider la légitimité d'un site Web (42 %). La plupart des Canadiens et des Canadiennes en ligne reconnaissent également les signes de tentatives d'hameçonnage, y compris des allégations au sujet de comptes qu'ils n'ont pas ou des livraisons inattendues (89 %), des demandes de renseignements de nature délicate (88 %) et des messages contenant des adresses de courriel incorrectes, des liens inconnus ou des fautes d'orthographe ou de grammaire (86 %). Un nombre presque tout aussi important reconnaît que les messages proposant des offres trop bonnes pour être vraies (83 %) et renfermant des pièces jointes inattendues ou inutiles (79 %) sont également des signes de tentatives d'hameçonnage.

La cybercriminalité et les menaces

Plus des trois quarts (78 %) des Canadiens et des Canadiennes en ligne n'ont *jamais* été victimes d'une arnaque en ligne qui leur a fait perdre de l'argent ou des données. Cela dit, jusqu'à environ le quart des Canadiens ont été victimes d'autres types de cyberattaques : 28 % d'un courriel frauduleux, 25 % d'une attaque de la part d'un logiciel malveillant, 24 % d'une fraude par texto, 20 % d'une arnaque par hameçonnage, 15 % d'un piratage de compte de médias sociaux et de 6 % d'un vol d'identité. Bien que la fréquence des cyberattaques ne soit pas élevée, les deux tiers (65 %)

des Canadiens et des Canadiennes en ligne s'inquiètent de la cybercriminalité liée à l'intelligence artificielle (IA); la moitié (51 %) craignent d'être victimes de la cybercriminalité en général et un quart (24 %) pensent qu'il est probable qu'ils seront victimes d'au moins une des nombreuses cybermenaces au cours de la prochaine année : une cybermenace qui compromet la sécurité de leurs renseignements personnels (19 %), qui cause la perte de fichiers ou de photos (8 %) ou qui entraîne des pertes financières (7 %).

Lorsqu'on leur a demandé quels types de cybermenaces les inquiètent *le plus*, 76 % des Canadiens et des Canadiennes en ligne ont mentionné le vol d'identité. En outre, environ six personnes sur 10 sont préoccupées d'abord et avant tout par les pertes financières (63 %) ainsi que les virus, les logiciels espions et les logiciels malveillants (59 %). La moitié (49 %) craignent les atteintes à la vie privée, 44 % les attaques par rançongiciel, 43 % la perte de données personnelles et 39 % la perte d'informations ou de fichiers. Les Canadiens et les Canadiennes sont moins susceptibles d'être préoccupés par les tentatives d'hameçonnage; 35 % ont déclaré que c'est le type de menace qui les préoccupe le plus. Les niveaux plus faibles d'inquiétude peuvent être attribuables à la confiance qu'ont les Canadiens et les Canadiennes en ligne en leur capacité à identifier une tentative d'hameçonnage ou un lien malveillant. Près des trois quarts (73 %) sont convaincus qu'ils peuvent y parvenir.

En ce qui concerne les attaques par rançongiciel, 2 % des personnes sondées ont été victimes d'une telle attaque, 4 % pensent qu'il est probable qu'elles soient victimes d'une telle attaque au cours de la prochaine année et 24 % pensent qu'elles sont vulnérables à ce type d'attaque. Si elles étaient victimes d'une attaque par rançongiciel, la majorité des personnes en ligne réinitialiseraient leurs mots de passe (56 %), prendraient une photo du message du rançongiciel (54 %) ou le signaleraient à la police locale (52 %).

La majorité des Canadiens et des Canadiennes en ligne ont déclaré être assez (44 %) ou bien (27 %) préparés pour faire face aux cybermenaces. Le quart (26 %) ont dit qu'ils ne se sentaient pas préparés et ont principalement invoqué deux raisons : la futilité (il n'est pas possible de se protéger en ligne) et le manque de connaissances (ne pas savoir où obtenir cette information, ne pas connaître les différentes menaces et ne pas avoir d'information simple à sa disposition).

Les communications et la campagne Pensez cybersécurité

Sept Canadiens et Canadiennes sur 10 (70 %) sont convaincus qu'ils peuvent se protéger en ligne s'ils disposent de renseignements fiables concernant les mesures à prendre. Près des deux tiers (63 %) estiment savoir comment trouver de l'information pratique pour assurer leur protection en ligne et exactement la moitié (50 %) jugent qu'ils disposent de suffisamment d'information sur les mesures à prendre pour se protéger contre les cybermenaces.

Soixante et un pour cent des Canadiens et des Canadiennes préféreraient obtenir de l'information pour se protéger contre les cybermenaces au moyen de sites Web. Quatre sur 10 ont exprimé une préférence pour les listes de choses à faire (41 %) et les vidéos didactiques (41 %). Environ le tiers (35 %) seraient intéressés par des fiches d'information ou des infographies.

Très peu de gens (4 %) ont entendu parler de la campagne Pensez cybersécurité. Parmi les personnes qui étaient au courant de la campagne lorsqu'on faisait un rappel assisté (11 %), un peu plus du tiers (36 %) ont indiqué avoir lu quelque chose à ce sujet dans les médias sociaux. Environ

le quart ont vu un segment aux nouvelles ou dans le journal (27 %), en ont entendu parler dans une émission de radio ou un balado (25 %) ou ont visionné une vidéo en ligne (25 %). Un nombre moins important de personnes ont visité le site Web de pensezcybersecurite.ca (16 %) ou ont entendu parler de la campagne par une autre personne (8 %).

Les entreprises et la cybersécurité

Plus des trois quarts des propriétaires et gestionnaires ou superviseurs d'entreprise (78 %) ont déclaré que leur entreprise avait pris des mesures pour se protéger contre les cybermenaces. Au moins la moitié des personnes sondées ont indiqué que leur entreprise exigeait une protection par mot de passe sur tous les appareils (57 %), qu'elle effectuait les mises à jour de logiciels de sécurité sur tous les ordinateurs (55 %) et qu'elle se servait d'un mot de passe ou de l'authentification de l'utilisateur pour l'accès sans fil et à distance (51 %).

Lorsqu'il s'agit de protéger leur entreprise contre les cybermenaces, environ quatre personnes sur 10 ont déclaré que leur organisation pourrait tirer parti de directives pour réagir à une cyberattaque (44 %), d'une liste des types de menaces qui existent et des signaux à surveiller (42 %) ou des mesures pour protéger les appareils mobiles dans un lieu public (38 %).

En ce qui a trait aux activités courantes de leur entreprise, près du quart des entreprises sondées sont préoccupées par les interruptions de travail (23 %) et presque autant s'inquiètent des atteintes à la réputation de l'organisation (22 %) ou des pertes financières (22 %). Seize pour cent craignent que les données de leur entreprise ne soient détenues en vue d'obtenir une rançon.

Six entreprises sur 10 sont au moins modérément préparées à se défendre contre les attaques par rançongiciel. Les mesures mises en œuvre par au moins un tiers des entreprises pour se protéger contre ce type d'attaque comprennent l'utilisation de logiciels antivirus (52 %), la mise à jour des systèmes d'exploitation, des logiciels et des applications (50 %), l'utilisation de l'AMF (46 %), la sauvegarde de fichiers (46 %) et la sauvegarde de fichiers à l'extérieur du Web (36 %). Bien qu'ils soient préparés dans une certaine mesure, un peu plus de la moitié des propriétaires et des gestionnaires d'entreprise prévoient qu'il faudrait déployer des efforts (38 %) pour se remettre d'une attaque par rançongiciel ou qu'il serait difficile (17 %) de s'en remettre.

Les parents et la cybersécurité

Comme nous l'avons mentionné, la présente étude comprenait un suréantillonnage des parents. Les parents ont tendance à différer des Canadiens et des Canadiennes en ligne qui n'ont pas d'enfants en ce qui concerne leur niveau perçu de connaissances en matière de sécurité en ligne et le rôle qu'ils jouent dans le soutien des autres personnes branchées. Les parents sont plus susceptibles de se décrire comme étant branchés à Internet tout le temps, possédant un niveau avancé de connaissances concernant la sécurité en ligne et agissant à titre de soutien pour les membres de leur famille en matière de sécurité en ligne.

Malgré leurs connaissances, les parents ont moins tendance à prendre des précautions pour protéger leurs comptes en ligne, à installer les plus récentes mises à jour de logiciels ou d'applications et à utiliser un mot de passe unique pour chaque compte. Cela dit, lorsqu'il s'agit d'éviter les sites Web dangereux et de repérer les messages d'hameçonnage, les parents sont plus enclins à vérifier le sceau de confiance de site Web et d'analyser l'aspect général du site Web. Ils ont aussi plus conscience que les offres trop belles pour être vraies, les pièces jointes inattendues

et la conception graphique non professionnelle sont des signes de tentatives d'hameçonnage. Comme on pouvait s'y attendre, les parents sont également plus confiants dans leur capacité à identifier une tentative d'hameçonnage ou un lien malveillant et ils sont moins susceptibles de s'inquiéter de la cybercriminalité liée à l'IA.

Observations finales

En général, une grande majorité de la population canadienne prend des précautions pour assurer sa sécurité en ligne, la plupart des gens installant régulièrement des mises à jour et utilisant l'authentification multifactorielle. Bon nombre des personnes sondées se servent la plupart du temps de mots de passe uniques pour des comptes en ligne importants et de mots de passe complexes. Voici les observations finales :

- *Une minorité importante de Canadiens et de Canadiennes en ligne continuent d'adopter des pratiques pouvant les rendre vulnérables à la cybercriminalité.* Au cours des dernières années, on a observé une baisse constante de la proportion de Canadiens et de Canadiennes utilisant le même mot de passe pour plusieurs comptes et une augmentation du recours à des mots de passe plus longs et à des gestionnaires de mots de passe. Cela dit, près du quart des personnes en ligne optent rarement pour des mots de passe uniques. Bon nombre d'entre elles disent que les mots de passe uniques sont difficiles à retenir et environ un tiers permettent à leur navigateur Web ou à une application de stocker leurs mots de passe ou se servent du même mot de passe pour plusieurs comptes. Bien que le stockage de mots de passe dans les navigateurs et les applications et la réutilisation du même mot de passe facilitent la tâche au titulaire du compte, cela se fait au détriment de la sécurité. Les navigateurs et les applications sont vulnérables aux cyberattaques et un mot de passe compromis pourrait mettre en danger simultanément de nombreux comptes en ligne.
- *Bien qu'il y ait place à l'amélioration en ce qui concerne la gestion des mots de passe, les Canadiens et les Canadiennes en ligne semblent très habiles à identifier les tentatives d'hameçonnage et à valider la légitimité des sites Web.* En effet, quoique cela puisse être le résultat du volume croissant de pourriels transmis aux gens, les personnes en ligne sont mieux en mesure de cerner les risques. La grande majorité des Canadiens et des Canadiennes reconnaissent les signes courants de tentatives d'hameçonnage et bon nombre d'entre eux scrutent régulièrement l'aspect général d'un site Web, vérifient si la barre d'adresse contient « https » ou le symbole du cadenas ou mènent des recherches pour confirmer la légitimité d'un site Web.
- *La peur est un facteur de motivation : les préoccupations des Canadiens et des Canadiennes en ligne au sujet de la cybercriminalité l'emportent sur la probabilité qu'ils en soient victimes.* Les taux de victimisation étaient faibles, la plupart des Canadiens ayant déclaré qu'ils n'avaient *jamais* été victimes d'une arnaque en ligne ayant causé une perte d'argent ou de renseignements personnels. En revanche, les deux tiers s'inquiètent de la cybercriminalité liée à l'IA. La moitié des répondants craignent la cybercriminalité en général, et bon nombre d'entre eux pensent qu'ils pourraient être victimes d'au moins une cybermenace au cours de la prochaine année, ce qui est peu probable selon le nombre de cas signalés.
- *La campagne Pensez cybersécurité est bien adaptée aux préférences des Canadiens et des Canadiennes en ligne en matière d'information, mais la campagne demeure méconnue***.** En ce qui concerne les besoins d'information, les Canadiens et les Canadiennes en ligne cherchent principalement des renseignements sur la façon de se protéger en ligne en consultant des sites

Web. Une forte minorité préfère les listes de choses à faire ou les vidéos didactiques, ainsi que les fiches d'information ou les infographies. Ces formats se prêtent bien aux campagnes d'information numériques comme Pensez cybersécurité. Cela dit, la campagne demeure méconnue, ce qui laisse croire qu'il serait nécessaire d'accroître les efforts de publicité ou de renforcement de l'image de marque afin de présenter la campagne comme une seule source d'information canadienne sur la cybersécurité. La campagne pourrait également offrir à la population canadienne une vidéo d'information ou une liste de choses à faire si on est victime de cybercriminalité. Bien que la majorité des victimes de cybercriminalité aient signalé l'incident, plus d'une personne sur 10 ne l'a pas fait. Ces répondants ont principalement indiqué qu'ils ne savaient pas quoi faire dans un tel cas (à qui le signaler ou comment le faire).

- *Plusieurs sous-groupes de Canadiens et de Canadiennes en ligne sont plus vulnérables que d'autres à la cybersécurité, en particulier les femmes, les personnes âgées de 65 ans et plus et les répondants entre 18 et 34 ans.*
    - Lorsqu'il s'agit de se protéger en ligne, les femmes sont plus susceptibles de se sentir mal préparées pour faire face à une cybermenace. Elles ont également plus tendance à compter sur les autres pour obtenir de l'aide et à trouver que la plupart des informations sur la sécurité en ligne portent à confusion. En outre, elles ont parlé de pratiques en ligne pouvant mettre à risque leurs comptes et leurs appareils. Les femmes sont moins susceptibles de savoir comment installer les plus récentes mises à jour de logiciels et d'applications et sont plus enclines à installer une mise à jour seulement après avoir cliqué sur « me le rappeler plus tard ». En outre, elles ont davantage tendance à utiliser des mots de passe uniques, à garder leurs mots de passe simples, à réutiliser des mots de passe et à permettre aux navigateurs ou aux applications de stocker leurs mots de passe. À la lumière des résultats, il pourrait être nécessaire de fournir des produits d'information clairs et concis sur la sécurisation des appareils et des comptes en ligne pour aider cette population en ligne à assurer sa sécurité et à se préparer aux cybermenaces.
    - Bien que bon nombre de Canadiens et de Canadiennes de 65 ans et plus prennent des mesures pour assurer la sécurité de leurs comptes et de leurs appareils, ils sont plus susceptibles que les jeunes d'avoir besoin de soutien pour des tâches informatiques de base, telles que la création de comptes en ligne, l'installation des plus récentes mises à jour de logiciels et la sauvegarde des données. De plus, ils sont moins susceptibles que les jeunes de connaître les signes courants des tentatives d'hameçonnage et de prendre des mesures pour vérifier la légitimité d'un site Web. Par ailleurs, ils ont plus tendance à *ignorer* s'ils sont vulnérables ou non à une attaque par rançongiciel. Si l'on se fie aux résultats de la recherche, les personnes en ligne de 65 ans et plus pourraient tirer profit de listes de vérification leur permettant de cerner les cyberrisques et de déterminer les mesures à prendre pour se protéger et protéger leurs renseignements.
    - Les Canadiens et Canadiennes de moins de 35 ans présentent plusieurs points de vulnérabilité dans leur comportement en ligne. Ils sont moins susceptibles que les personnes plus âgées de toujours installer les plus récentes mises à jour. Ils ont plus tendance à cliquer sur « me rappeler plus tard » à quelques reprises avant d'installer les mises à jour ou à n'installer ces dernières que lorsqu'ils sont loin de leur appareil ou ne l'utilisent pas. De plus, ils sont plus enclins que les Canadiens et Canadiennes plus âgés à utiliser rarement des mots de passe uniques pour les comptes en ligne importants et ils sont plus susceptibles que tous les autres groupes d'âge de permettre

à leur navigateur ou à leurs applications de stocker leurs mots de passe. Ils pourraient être utiles d'élaborer des rappels à l'intention de ce groupe d'âge concernant l'importance d'utiliser des mots de passe complexes et de tenir la sécurité des appareils et des applications à jour, d'autant plus que ces personnes sont moins susceptibles de croire qu'elles pourraient être victimes de cybercriminalité ou être visées par une cybermenace.

Notes à l'intention du lecteur

- Les prochaines sections renferment les constatations détaillées. Les résultats sont présentés dans le corps du texte et s'appuient généralement sur un graphique ou un tableau.
- Tous les résultats sont exprimés en pourcentage, sauf indication contraire. Tout au long du rapport, les pourcentages peuvent ne pas toujours totaliser 100 en raison de l'arrondissement ou des réponses multiples offertes par les répondants.
- Parfois, le nombre de répondants change dans le rapport parce que des questions ont été posées à des sous-échantillons de la population de l'enquête. Par conséquent, les lecteurs doivent en être conscients et faire preuve de prudence lorsqu'ils interprètent les résultats qui sont tirés d'un plus petit nombre de répondants.
- Les différences entre les sous-groupes, qui reposent généralement sur les résultats généraux, sont mentionnées dans le rapport.
    - Lorsque les différences entre les sous-groupes ne sont pas abordées pour certaines questions, on peut supposer qu'il n'y a pas de différences significatives entre les sous-groupes de répondants.
    - En cas de différences entre les sous-groupes, si une ou plusieurs catégories d'un sous-groupe ne sont pas mentionnées dans une discussion sur les différences (p. ex., si deux groupes d'âge sur trois font l'objet d'une comparaison), on peut supposer que des différences significatives n'ont été observées que dans les catégories indiquées.
    - Seules les différences entre les sous-groupes qui sont statistiquement significatives au niveau de confiance de 95 %, qui se rapportent à un échantillon de sous-groupe supérieur à n=30 ou qui illustrent ou font partie d'un modèle ou d'une tendance sont présentées dans le rapport.
- Le cas échéant, les résultats sont comparés à ceux de sondages similaires menés en 2018, 2020 et 2022.
- Le questionnaire du sondage est annexé au rapport.

Valeur du contrat

La valeur du contrat était de 81 085,41 $ (incluant les taxes applicables).

Déclaration de neutralité politique

En ma qualité de cadre supérieure de Phoenix Strategic Perspectives, je certifie par la présente que les produits livrés sont en tout point conformes aux exigences du gouvernement du Canada en matière de neutralité politique qui sont décrites 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. Plus particulièrement, les produits finaux ne comprennent pas de renseignements sur les intentions de vote aux élections, les préférences de partis politiques, les positions vis-à-vis de l'électorat ou l'évaluation de la performance d'un parti politique ou de son dirigeant.

Alethea Woods
Présidente
Phoenix Strategic Perspectives Inc.