Government of Canada | Gouvernement du Canada

Sondage de suivi sur la connaissance de la campagne Pensez cybersécurité

Rapport final

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

Rapport final

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) :

TABLE DES MATIÈRES

LISTE DES TABLEAUX

LISTE DES GRAPHIQUES

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 : 

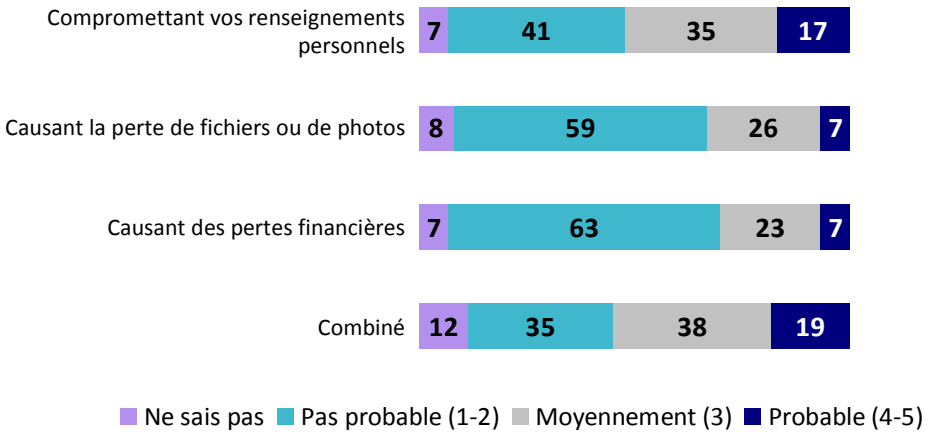
Susan Galley (vice-présidente)

RÉSULTATS DÉTAILLÉS DU SONDAGE

A. NIVEAU DE PRÉOCCUPATION/PROBABILITÉ DES MENACES

Près d'une personne sur cinq (17 %) a l'impression qu'elle sera probablement touchée par une cybermenace susceptible de compromettre ses renseignements personnels au cours de la prochaine année, alors que deux personnes sur cinq (41 %) considèrent cela comme peu probable. La plupart des Canadiens croient qu'ils ne seront pas touchés par une cybermenace, et moins d'une personne sur dix est d'avis qu'elle sera confrontée à une menace entraînant une perte financière (7 %), ou encore la perte de fichiers ou de photos (7 %). De façon générale, lors de la combinaison des probabilités associées aux trois domaines, un Canadien sur cinq (19 %) 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 (35 %) des répondants est d'avis qu'il est peu probable qu'il soit touché par l'une ou l'autre des trois cybermenaces.

Graphique 1 : Probabilité des menaces



Q11abc. Au cours de la prochaine année, à quel point avez-vous l'impression qu'il est probable que vous soyez victime d'une cybermenace...
Base : n=2710

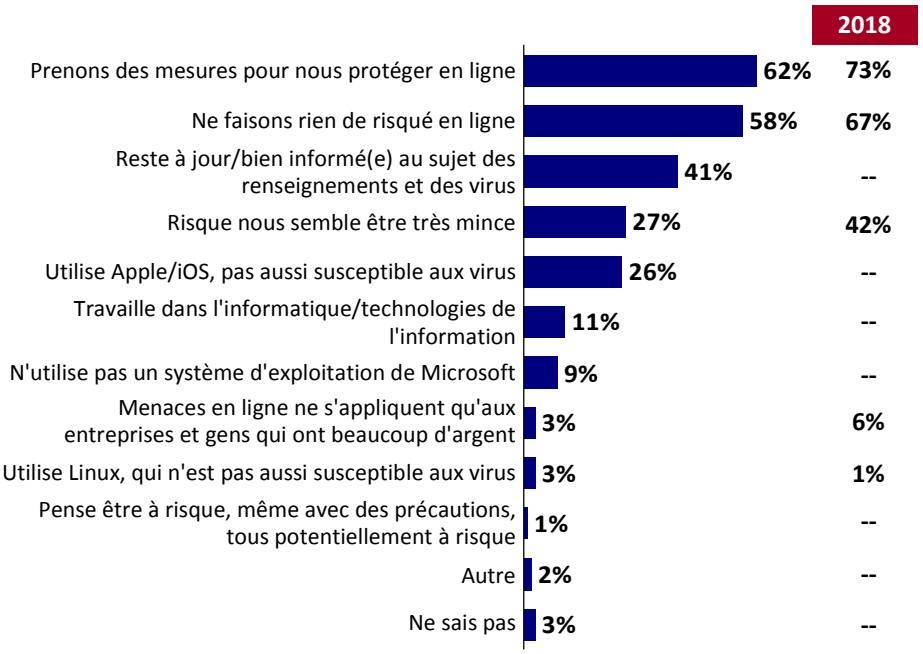
- Les personnes âgées de moins de 35 ans et les résidents de l'Alberta sont moins susceptibles que les autres répondants de croire qu'une cybermenace est susceptible de compromettre leurs renseignements personnels. Ceux qui sont plus susceptibles de croire qu'ils seront

touchés sont les résidents du Québec, les personnes ayant fait des études universitaires et celles dont le revenu du ménage est de 150 000 dollars ou plus, ainsi que les parents d'enfants âgés de cinq ans ou plus.

- En ce qui concerne la perte financière et la perte de fichiers, les personnes âgées de 25 à 34 ans, les résidents de l'Ontario, les personnes dont le revenu du ménage est de 150 000 dollars ou plus et les hommes sont moins susceptibles que leurs homologues de croire qu'ils seront touchés.

La plupart des répondants qui ne s'inquiètent pas affirment que c'est parce qu'ils prennent des mesures pour se protéger en ligne (62 %) ou parce qu'ils ne font rien de risqué en ligne (58 %). Deux personnes sur cinq (41 %) indiquent qu'elles ne se sentent pas concernées parce qu'elles restent au courant des virus. Environ le quart des répondants a l'impression qu'il est peu probable qu'il soit touché parce qu'ils considèrent que les risques comme très faibles (27 %) ou parce qu'ils utilisent Apple/iOS, qui n'est pas aussi exposé aux virus (26 %).

Graphique 2 : Raison de l'improbabilité d'être touché



QK8a. Pourquoi ne croyez-vous pas qu'il est probable que vous soyez victime d'une cybermenace?
Base : n = 1941 (peu probable qu'ils subissent une perte financière ou une perte de fichiers, ou que leurs renseignements personnels soient compromis), 2018 : n = 492 (peu probable qu'ils soient touchés par une cybermenace [mention générale])

- Les personnes âgées de 35 à 54 ans sont plus enclines à dire qu'elles prennent des mesures pour se protéger. C'est également le cas des hommes, des résidents de l'Alberta et des personnes dont le revenu du ménage ou le niveau de scolarité sont plus élevés.
- Plus de Canadiens âgés de moins de 35 ans que des autres groupes d'âge considèrent comme faible la probabilité qu'ils soient touchés par une cybermenace.
- Les gens âgés de 65 ans ou plus et les femmes ont plus tendance que les hommes et les répondants plus jeunes à déclarer ne pas adopter de comportements risqués en ligne. C'est également le cas des résidents de la Saskatchewan en comparaison avec le reste du Canada.

Plus du quart des Canadiens (27 %) estime qu'il est probable qu'un membre de sa famille ou un(e) ami(e) soit victime d'une cybermenace au cours de la prochaine année, ce qui est inférieur aux 32 % de 2018, bien qu'en 2018, la question mentionnait « vous ou un membre de votre famille ». Les Canadiens sont plus souvent pour un ami (54 %) ou un parent (48 %). Environ le tiers des répondants a l'impression qu'un collègue (35 %) ou un voisin (33 %) sera touché, alors que le quart s'inquiète pour ses enfants (26 %) ou pour ses grands-parents (23 %).

Tableau 1 : Probabilité que d'autres personnes soient touchées

--	**Total 2020**	**Total 2018***
Q12. À quel point croyez-vous qu'il est probable qu'un membre de votre famille ou qu'un(e) ami(e) soit victime d'une cybermenace cours de la prochaine année?	*n=2710*	*n=2072*
Improbable (1-2)	22 %	23 %
Moyennement probable (3)	37 %	34 %
Probable (4-5)	27 %	32 %
Je ne sais pas	13 %	12 %
Q13. Selon vous, qui sera touché(e)?	*n=740*	
Un(e) ami(e)	54 %	
Un de vos parents	48 %	
Un(e) collègue	35 %	
Un(e) voisin(e)	33 %	
Vos enfants	26 %	
Un de vos grands-parents	23 %	
Autre membre de la famille	5 %	
Époux (épouse) ou conjoint(e)	2 %	
N'importe qui peut être touché	2 %	
Autre	3 %	

--	Total 2020	Total 2018*
Je ne sais pas	9 %	
Q14. Pourquoi pensez-vous qu'ils seront touchés?	*n=740*	
Utilisation négligente, ne prend pas de mesures de sécurité ou de précaution	18 %	
Cela se produit tout le temps ou fréquemment, tout le monde est à risque	17 %	
Pas technophile, ne connaît pas bien les précautions à prendre	16 %	
Les personnes âgées sont plus susceptibles, plus à risque, font trop confiance	4 %	
Trop confiant, naïf	3 %	
Pirates et escroqueries de plus en plus sophistiqués	2 %	
Utilisation d'Internet pour toutes les transactions, utilisation de plusieurs sites	2 %	
Expérience personnelle, connaît quelqu'un qui a été victime de fraude	2 %	
Données personnelles pas assez protégées par le gouvernement ou l'entreprise, manque d'application de la loi ou de responsabilité en cas d'atteinte à la sécurité	2 %	
Autre	11 %	
Je ne sais pas	17 %	
Pas de réponse	7 %	

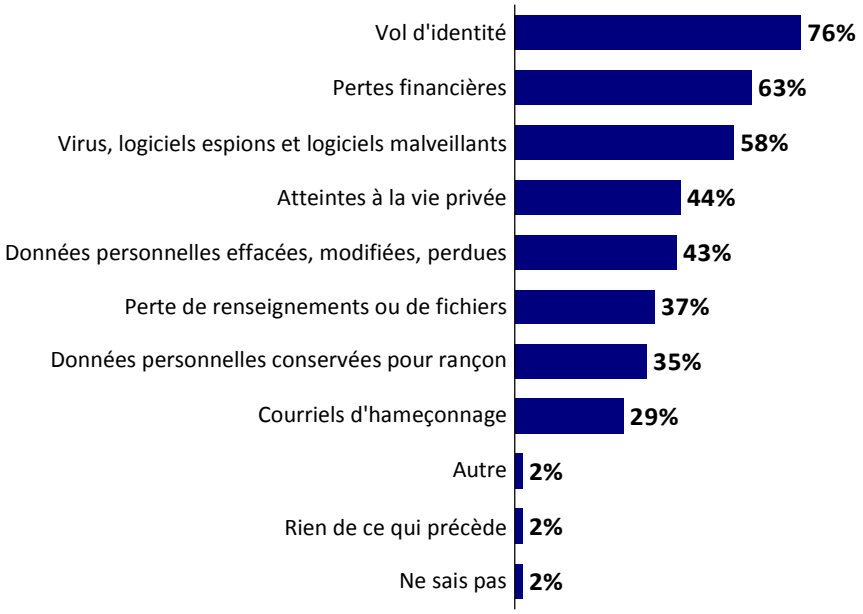
*En 2018, la question mentionnait « vous ou un membre de votre famille ».

- Les Canadiens âgés de moins de 35 ans sont moins susceptibles que ceux des autres groupes d'âge de croire que quelqu'un qu'ils connaissent sera touché par une cybermenace, ce qui est aussi plus souvent le cas au Manitoba qu'ailleurs au Canada.
- Les résidents du Québec, ceux dont le niveau de scolarité est le plus élevé (université), ceux dont le revenu du ménage est le plus élevé (150 000 dollars ou plus) et les parents d'enfants âgés de cinq ans ou plus affirment plus souvent qu'il est probable qu'une personne qu'ils connaissent soit touchée.
- Naturellement, certains groupes d'âge sont plus susceptibles d'être proches de gens qui sont plus enclins à être touchés et donc plus préoccupés. Par exemple, c'est le cas des personnes de moins de 35 ans, qui s'attendent à ce que leurs grands-parents soient touchés, alors que les 25 à 44 ans ont plus tendance que les autres groupes d'âge à avoir l'impression que cela est probable pour leurs parents ou collègues. Les groupes plus âgés (45 ans ou plus) sont plus préoccupés pour leurs enfants.

- Les hommes sont plus susceptibles que les femmes de croire qu'il est probable que leurs collègues, voisins ou amis soient touchés par une cybermenace.
- Les parents d'enfants âgés de cinq ans ou plus sont plus enclins que les répondants des autres segments à croire qu'il est possible qu'un parent ou leurs enfants, un collègue ou un voisin soient touchés.

Le vol d'identité préoccupe trois Canadiens sur quatre (76 %). Lorsqu'il est question de cybermenaces, les Canadiens sont également préoccupés par les pertes financières (63 %) ainsi que les virus, les logiciels espions et les logiciels malveillants (58 %). Environ deux personnes sur cinq se disent préoccupées par une atteinte à la vie privée (44 %), par la possibilité que leurs données personnelles soient effacées, modifiées ou perdues (43 %), par la perte de renseignements ou de fichiers (37 %) ou par le fait que leurs données personnelles soient conservées pour rançon (35 %). Trois Canadiens sur dix (29 %) se disent préoccupés par les courriels d'hameçonnage.

Graphique 3 : Nature de la préoccupation



Q15. Quels types de cybermenaces vous préoccupent le plus?
Base : n=2710

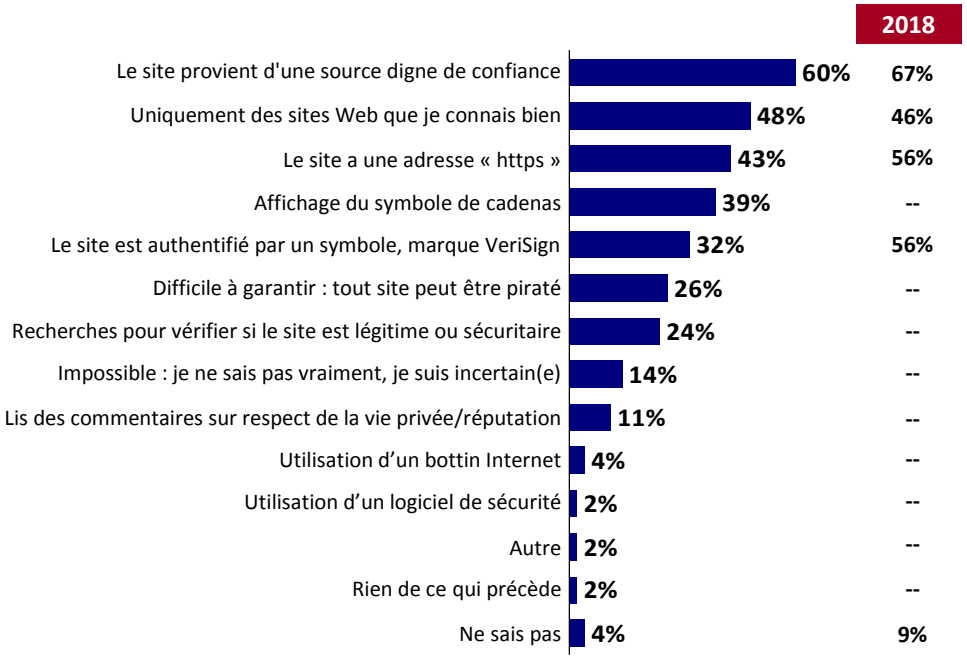
- Les courriels d’hameçonnage et les virus préoccupent davantage les personnes âgées de 55 ans et plus que les Canadiens plus jeunes.
- Le vol d’identité est une préoccupation plus répandue chez les personnes âgées de 45 à 65 ans que chez les autres groupes d’âge.
- Les pertes financières, le vol d’identité et les données personnelles conservées pour rançon sont plus souvent une source d’inquiétude chez les personnes dont le niveau de scolarité est le plus élevé (université) et dont le revenu du ménage est le plus élevé (150 000 dollars).

B. CONNAISSANCE

Trois Canadiens sur cinq (60 %) disent rechercher un site Web qui provient d'une source digne de confiance, comme un fournisseur de logiciels bien connu ou le gouvernement. Un peu moins de la moitié des répondants (48 %) indiquent qu'ils n'utilisent que les sites Web qu'ils connaissent bien, tandis qu'une moindre proportion (43 %) recherche spécifiquement des sites qui ont une adresse « https » pour s'assurer qu'ils sont sécurisés. Environ le tiers des répondants disent vérifier la sécurité d'un site en recherchant le symbole de cadenas (39 %) ou une authentification de la marque VeriSign (32 %). Le quart d'entre eux affirme qu'il est difficile de s'assurer qu'un site est sécurisé, car tout site peut être piraté (26 %), ou qu'il mène des recherches pour savoir si un site est légitime (24 %). Plus d'une personne sur dix indique qu'il est impossible de savoir si un site Web est sécurisé (14 %) ou affirme lire des commentaires sur le respect de la vie privée ou la réputation du site (11 %).

Bien qu'une question différente ait été posée dans le sondage de 2018 (Comment peut-on savoir si un site Web est sécurisé?), les résultats montrent un certain lien entre les deux éditions dans la mesure où la plupart des gens connaissent et prennent des mesures pour s'assurer que les sites qu'ils visitent sont dignes de confiance ou bien connus, ou même qu'ils ont une adresse « https », bien que l'authentification VeriSign soit moins apte à être vérifiée qu'en 2018.

Graphique 4 : Étapes pour vérifier qu'un site Web est sécurisé



QK11a. Quelles mesures prenez-vous pour vous assurer qu'un site Web est sécurisé?
Base : n = 2710, 2018 – Comment peut-on savoir si un site Web est sécurisé?
Base : n=1880

- La connaissance de plusieurs méthodes pour déterminer si un site est sécurisé est plus élevée chez les personnes âgées de 25 à 34 ans et chez les répondants qui ont fait des études universitaires.

Seul un Canadien sur cinq (19 %) se dit préparé pour faire face aux cybermenaces. Plus d'une personne sur quatre (27 %) affirme ne pas être préparée, et 45 % se disent assez préparés. Parmi ceux qui ne sont pas préparés, 44 % disent que c'est parce qu'il est impossible de toujours se protéger en ligne. Trois personnes sur dix (31 %) ont certaines réserves et peuvent se remettre lorsqu'elles sont victimes d'une cybermenace. Environ une personne sur cinq cite un éventail d'autres raisons, notamment un manque d'information sur les étapes à suivre (23 %), un manque de connaissances des différents types de menaces (22 %), la sensation qu'il est peu probable que cela lui arrive (18 %), un manque de temps pour se préparer (18 %), ou le fait que les renseignements qu'ils trouvent ne sont pas assez simples pour lui être utiles (18 %).

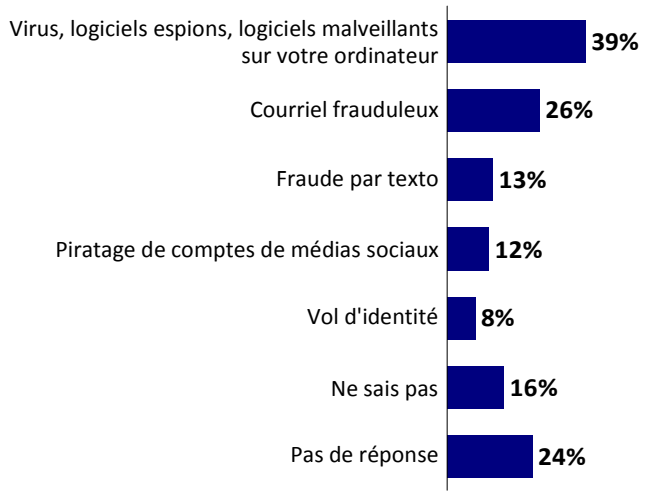
Tableau 2 : État de préparation

--	**Total 2020**
Q16. Êtes-vous bien préparé(e) pour faire face aux cybermenaces?	*n=2710*
Pas préparé(e) (1-2)	27 %
Préparé(e) (3)	45 %
Bien préparé(e) (4-5)	19 %
Je ne sais pas	8 %
Q17. Pourquoi donc?	*n=1959*
Vous ne pouvez jamais vraiment vous protéger en ligne	44 %
J'ai une copie sauvegardée et je peux m'en remettre	31 %
Je ne sais pas où obtenir des renseignements sur les mesures à prendre	23 %
Je ne connais pas les différents types de menaces	22 %
Je ne pense pas qu'il est probable que cela m'arrive	18 %
Je n'ai pas le temps ou je ne me penche jamais sur ce problème	18 %
Les renseignements que je trouve ne sont pas assez simples pour m'aider	18 %
Il est inutile d'essayer de se protéger	4 %
Rien	2 %
Autre	3 %
Je ne sais pas	6 %

- Bien qu'il n'y ait pas de proportions importantes de certains segments qui se sentent bien préparés à faire face à une cybermenace, les répondants qui sont âgés de 25 à 34 ans, les résidents du Québec et les personnes qui ont fait des études secondaires sont plus enclins que la moyenne à dire qu'ils ne sont pas préparés pour faire face à une telle menace.
- Les personnes âgées de 35 ans et moins ont plus tendance que les autres répondants à citer l'improbabilité que cela leur arrive et le manque de temps. Le temps est aussi un obstacle que les parents mentionnent plus souvent. La vision fataliste voulant que vous ne puissiez jamais vraiment vous protéger est plus répandue chez les gens âgés de 35 à 44 ans. Le manque de compréhension de la nature des menaces est plus fréquent chez les Canadiens plus âgés (65 ans et plus) et chez ceux qui n'ont fait que des études secondaires. Le fait de ne pas savoir où obtenir de l'information est une réponse plus fréquente chez les femmes que chez les hommes.

Deux Canadiens sur cinq (39 %) indiquent avoir été victimes d'un virus, d'un logiciel espion ou d'un logiciel malveillant sur leur ordinateur. Plus du quart (26 %) déclare avoir été victime d'un courriel frauduleux. Parmi les autres cyberattaques figurent les fraudes par texto (13 %) ou le piratage de compte de médias sociaux (12 %). Un peu moins d'une personne sur dix (8 %) a été victime d'un vol d'identité. En tout, environ quatre personnes sur dix déclarent ne pas savoir si elles ont été touchées (16 %) ou ne répondent pas à la question (24 %).

Graphique 5 : Fréquence de la victimisation

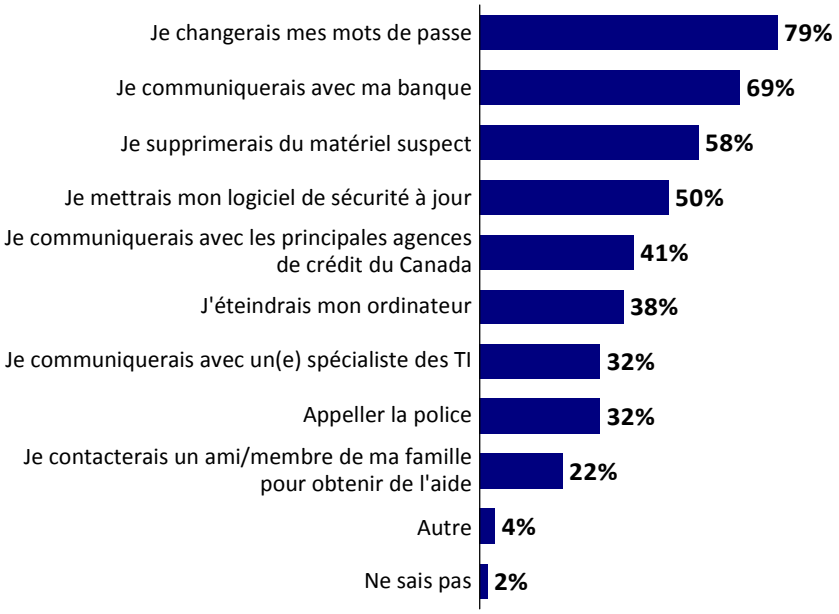


Q18. Avez-vous déjà été victime de l'une des cyberattaques suivantes?
Base : n=2710

- Les personnes les plus susceptibles d'avoir été victimes d'un courriel frauduleux sont âgées de moins de 25 ans ou de plus de 65 ans, tout comme les résidents du Québec.
- La fréquence à laquelle les gens sont victimes de fraudes par texto est également plus élevée chez les moins de 25 ans et chez les résidents de la Saskatchewan et du Québec.
- Les virus, les logiciels espions et les logiciels malveillants sont plus susceptibles de constituer un problème en Alberta qu'ailleurs au Canada, ainsi que chez les hommes.
- Les personnes âgées de moins de 45 ans, en particulier celles de moins de 25 ans, sont plus souvent victimes de piratage de comptes de médias sociaux que les Canadiens âgés de 45 ans et plus.

S'ils savaient ou soupçonnaient avoir été victimes d'une cyberattaque, la plupart (79 %) des Canadiens affirment qu'ils changeraient leurs mots de passe. Plus de deux personnes sur trois (69 %) communiqueraient avec leur banque. Plus de la moitié supprimerait du matériel suspect (58 %) ou mettrait à jour son logiciel de sécurité (50 %). Les autres mesures prévues sont la prise de contact avec les principales agences de crédit du Canada (comme TransUnion et Equifax) (41 %) ou la mise hors circuit de l'ordinateur concerné (38 %). Le tiers contacterait un spécialiste des TI (32 %) ou appellerait la police (32 %). Un peu moins d'une personne sur quatre (22 %) demanderait l'aide d'un ami ou d'un membre de leur famille.

Graphique 6 : Mesures de protection prises par les victimes d'une cyberattaque



Q19. Si vous saviez ou soupçonniez avoir été victime d'une cyberattaque, quelles mesures prendriez-vous pour vous protéger?
Base : n=2710

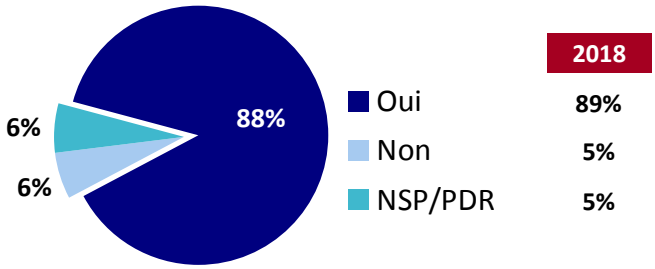
- La modification des mots de passe est une mesure que mentionnent plus souvent les personnes âgées de 25 à 44 ans que les autres groupes d'âge, ainsi que les parents. Les gens âgés de 35 à 44 ans auraient plus tendance à communiquer avec leur banque, alors que les moins de 25 ans sont moins enclins à le faire.

- La suppression d’éléments suspects est une mesure que les 55 à 64 ans seraient plus susceptibles de prendre que les autres groupes d’âge. Les personnes âgées de 55 ans et plus auraient aussi plus tendance que les jeunes Canadiens à éteindre leur ordinateur. Il s’agit également d’une mesure plus fréquente au Manitoba et moins fréquente au Québec.
- Les Canadiens âgés de 35 à 54 ans, les parents, les résidents du Québec, les personnes dont le niveau de scolarité est plus élevé (postsecondaire) et ceux dont le revenu est moyen ou élevé (80 000 dollars ou plus) seraient beaucoup plus enclins à communiquer avec des agences de crédit.

C. PRÉCAUTIONS – COMPORTEMENTS

Près de neuf Canadiens sur dix (88 p. cent, une proportion semblable aux 89 p. cent de 2018) disent prendre des précautions pour protéger leurs comptes en ligne, leurs comptes de médias sociaux, leurs appareils et leurs réseaux.

Graphique 7 : Mesures prises pour protéger des comptes en ligne



Q1. Prenez-vous des précautions pour protéger vos comptes en ligne, vos comptes de médias sociaux, vos appareils et vos réseaux?
Base : n=2710

- Les Canadiens les plus susceptibles de prendre des précautions pour protéger leurs comptes en ligne, bien que la proportion soit élevée dans tous les segments, sont les gens âgés de 35 à 54 ans, ainsi que les résidents de la Colombie-Britannique et de l'Ontario. Les hommes ont aussi plus tendance à déclarer prendre des précautions, tout comme les gens dont le niveau de scolarité et le revenu sont plus élevés.
- Les personnes âgées de moins de 25 ans, les résidents du Québec et les personnes n'ayant fait que des études secondaires sont moins susceptibles de dire qu'ils prennent des précautions.

Le changement des mots de passe des comptes est l'une des mesures que les Canadiens prennent pour se protéger. Cependant, environ un quart seulement le font au moins quelques fois par année (19 %) ou plus souvent (7 %). Une personne sur dix (12 %) affirme changer ses mots de passe une fois par année, tandis que 15 % estiment le faire tous les deux ou trois ans. Une personne sur cinq (19 %) change un mot de passe chaque fois qu'elle est invitée à le faire et 14 % le font quand ils y pensent, sans calendrier précis. Près d'une personne sur dix (9 %) affirme ne jamais changer ses mots de passe et 3 % ne les changent que lorsqu'ils apprennent l'existence d'une brèche de sécurité aux nouvelles.

Près de deux répondants sur trois (64 %) changent certains mots de passe plus que d'autres. Les comptes bancaires en ligne (62 %) sont les plus hauts dans la liste des priorités. Moins de gens modifient plus souvent les mots de passe de leur compte de messagerie professionnel (34 %) ou personnel (26 %). Le quart d'entre eux modifient plus souvent les mots de passe de ses comptes de magasinage en ligne (25 %) ou de ses comptes de médias sociaux (24 %).

Tableau 3 : Changement des mots de passe

--	**Total 2020**
Q2. En général, à quelle fréquence changez-vous les mots de passe de vos comptes?	*n=2710*
Jamais	9 %
Après quelques années	15 %
Une fois par année	12 %
Quelques fois par année	19 %
Plus souvent que quelques fois par année	7 %
Quand on m'invite à le faire	19 %
Quand j'y pense, pas à intervalle fixe	14 %
Lorsque j'apprends l'existence d'une brèche de sécurité aux nouvelles	3 %
Je ne sais pas	2 %
Q3. Changez-vous certains mots de passe plus souvent que d'autres?	*n=2457*
Oui	64 %
Non	28 %
Je ne sais pas	6 %
Pas de réponse	2 %

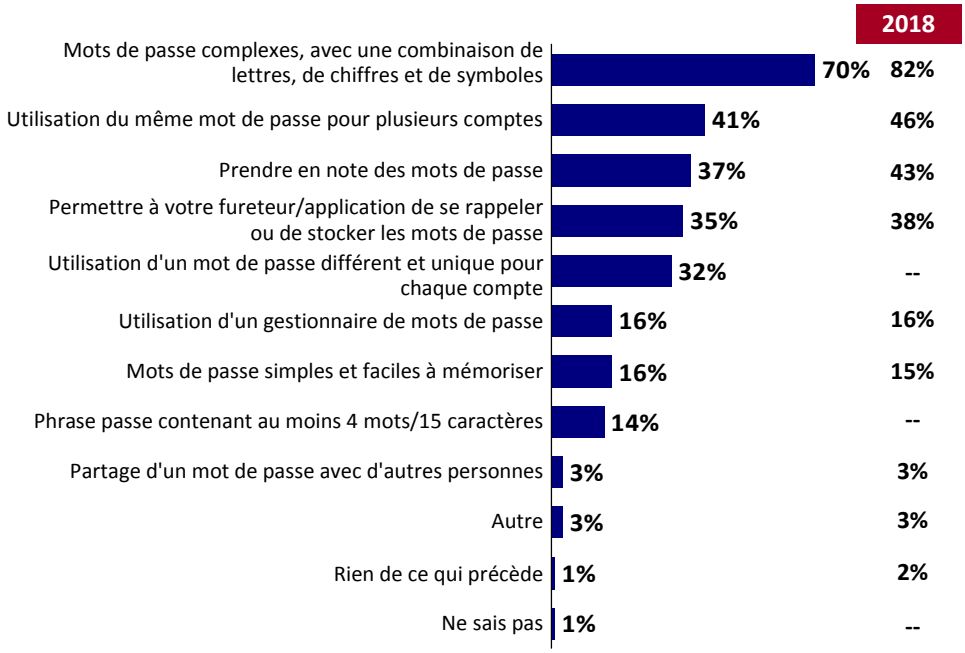
--	Total 2020
Q4. Quels mots de passe changez-vous le plus souvent?	*n=1569*
Comptes de services bancaires en ligne	62 %
Courriel au travail	34 %
Courriel à la maison	26 %
Comptes de magasinage en ligne	25 %
Comptes de médias sociaux	24 %
Comptes de courriel au travail	2 %
Comptes de réseau scolaire, courriel de l'université	1 %
Lors d'une invitation à le faire, gestionnaire de mots de passe, lors de l'oubli d'un mot de passe	1 %
Autre	5 %
Je ne sais pas	3 %

- Les personnes âgées de 45 à 54 ans changent plus souvent leurs mots de passe quelques fois par année. Les résidents du Québec, ainsi que ceux qui ont fait des études secondaires ou moins, sont plus susceptibles de ne jamais changer leurs mots de passe.
- Les résidents de la Colombie-Britannique et les personnes âgées de 18 à 24 ans déclarent changer leurs mots de passe une fois par année, tandis que les 25 à 34 ans, les hommes et les personnes qui ont fait des études universitaires disent changer leurs mots de passe tous les deux ou trois ans. Les femmes, les gens qui ont fait des études universitaires et ceux qui gagnent plus de 150 000 dollars par année sont plus susceptibles de mettre à jour un mot de passe lorsqu'on les invite à le faire.
- La probabilité de changer certains mots de passe plus que d'autres augmente avec le niveau de revenu, les personnes ayant les revenus les plus bas (40 000 dollars ou moins) étant les moins enclines à le faire, tandis que celles dont le revenu est le plus élevé (150 000 dollars ou plus) ont plus tendance à le faire.
- Les personnes qui ont fait des études universitaires de même que les parents sont aussi plus susceptibles de signaler qu'elles changent plus souvent certains mots de passe que d'autres répondants, alors que les personnes âgées de 65 ans et plus et les résidents du Québec affirment plus souvent ne pas le faire.
- Sans surprise, les jeunes âgés de 18 à 24 ans modifient plus souvent que les autres répondants les mots de passe de leurs comptes scolaires et de médias sociaux, alors que les 25 à 54 ans (âge où l'on travaille généralement) et les parents sont plus susceptibles de signaler le changement plus fréquent du mot de passe de leur courriel au travail. Les personnes âgées de 55 ans et plus modifient plus souvent que les autres les mots de passe de leurs comptes de magasinage en ligne, et celles âgées de 65 ans ou plus modifient plus souvent les mots de passe de leurs comptes de services bancaires en ligne.

- Les hommes, les gens qui ont fait des études universitaires et ceux qui gagnent au moins 80 000 dollars par année déclarent également plus souvent que les autres changer le mot de passe de leur courriel au travail.

En ce qui concerne les mots de passe, la plupart des Canadiens (70 %) disent essayer d'utiliser des mots de passe complexes, avec une combinaison de lettres, de chiffres et de symboles. Deux répondants sur cinq (41 %) utilisent le même mot de passe pour plusieurs comptes. Environ le tiers d'entre eux prend en note ses mots de passe (37 %), permet à un navigateur ou à une application de mémoriser ou de stocker ses mots de passe (35 %), ou utilise un mot de passe différent et unique pour chaque compte (32 %). Moins d'une personne sur cinq utilise un gestionnaire de mots de passe (16 %), utilise des mots de passe simples et faciles à mémoriser (16 %) ou utilise une phrase passe contenant au moins quatre mots et 15 caractères (14 %).

Graphique 8 : Mesures prises concernant les mots de passe



Q5. Lorsque vient le temps de choisir vos mots de passe, lesquelles des mesures suivantes prenez-vous?
Base : n=2710

- Les personnes âgées de 25 à 34 ans sont plus susceptibles de prendre la plupart des mesures indiquées. Une tendance semblable est observée chez les personnes ayant le niveau de scolarité le plus élevé (diplôme universitaire) et les revenus les plus élevés (150 000 dollars ou plus). Les personnes moins instruites (études secondaires ou moins),

celles dont le revenu est plus bas (40 000 dollars ou moins) et les gens les plus jeunes (18 à 24 ans) sont plus susceptibles d'utiliser des mots de passe simples et faciles à mémoriser.

- Les personnes âgées de 18 à 24 ans sont plus enclines à utiliser le même mot de passe pour plusieurs comptes, alors que celles âgées de 55 ans et plus sont plus susceptibles de prendre leurs mots de passe en note. Les femmes ont plus tendance à adopter ces deux comportements que leurs homologues masculins, qui préfèrent utiliser des gestionnaires de mots de passe et des mots de passe uniques pour chaque compte.
- Les parents ont également plus tendance que leurs pairs d'utiliser des gestionnaires de mots de passe.

Un peu plus de la moitié des Canadiens (53 %) utilisent une authentification multifactorielle. Pour ce faire, ils ont le plus souvent recours à un code reçu par message texte (79 %). Trois répondants sur cinq utilisent un mot de passe (65 %), un code reçu par courriel (64 %) ou un NIP (63 %). Plus de la moitié (57 %) d'entre eux utilisent des empreintes digitales. Deux personnes sur cinq (41 %) utilisent un code reçu par une application d'authentification, tandis que trois répondants sur dix (29 %) utilisent un code reçu par appel téléphonique. Une personne sur cinq utilise la reconnaissance faciale (23 %) ou une phrase passe (20 %). Un moins grand nombre utilise un périphérique jeton (14 %), la reconnaissance vocale (9 %), une carte à puce (7 %) ou une clé USB (4 %).

Tableau 4 : Authentification multifactorielle

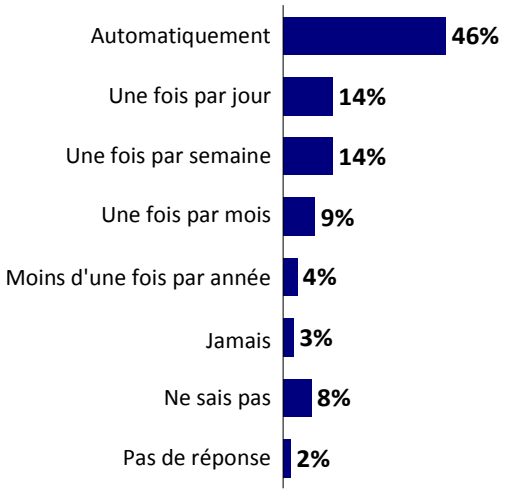
--	**Total 2020**
Q6. Utilisez-vous une authentification multifactorielle?	*n=2710*
Oui	53 %
Non	31 %
Je ne sais pas	14 %
Pas de réponse	2 %
Q7. Lesquels des facteurs d'authentification suivants avez-vous utilisés?	*n=1423*
Code reçu par texto	79 %
Mots de passe	65 %
Code reçu par courriel	64 %
NIP	63 %
Empreintes digitales	57 %
Code reçu par une application d'authentification	41 %
Code reçu par appel téléphonique	29 %

--	Total 2020
Reconnaissance faciale	23 %
Phrases passe	20 %
Périphériques jetons	14 %
Reconnaissance vocale	9 %
Cartes à puce	7 %
Clés USB	4 %
Autre	2 %
Je ne sais pas	1 %
Pas de réponse	1 %

- Les Canadiens qui sont les plus susceptibles d'utiliser l'authentification multifactorielle sont les personnes âgées de 25 à 54 ans, les parents, les hommes, les résidents de l'Alberta et les gens qui gagnent au moins 80 000 dollars par année. Les personnes les moins susceptibles d'utiliser ce type d'authentification sont les gens âgés de 55 à 64 ans et les résidents du Québec.
- Bien que l'utilisation de mots de passe soit courante dans tous les sous-groupes, ceux qui authentifient leurs mots de passe par le biais d'un code reçu par message texte sont plus susceptibles d'avoir entre 25 et 44 ans, d'être des résidents de l'Ontario, d'avoir fait des études universitaires ou d'avoir un revenu d'au moins 80 000 dollars par année. Les personnes âgées de 25 à 34 ans sont aussi plus susceptibles de recevoir un code par courriel ou par une application d'authentification, alors que les gens âgés de 35 à 44 ans ont plus tendance à recevoir un code par courriel ou à utiliser une carte à puce ou un périphérique jeton.
- L'authentification par empreintes digitales est plus utilisée par les 18 à 24 ans et les 35 à 44 ans, ainsi que par les parents. La reconnaissance faciale est également utilisée plus souvent par les jeunes de 18 à 24 ans et par les résidents du Canada atlantique. Les personnes qui gagnent 150 000 dollars ou plus par année sont plus aptes à utiliser ces deux méthodes.
- Les résidents de l'Ontario, les hommes ainsi que les gens dont le niveau de scolarité est plus élevé (université) ou dont le revenu est plus élevé (150 000 dollars ou plus par année) ont plus tendance que les autres répondants à utiliser un périphérique jeton. Les hommes sont aussi plus susceptibles que les femmes de recevoir un code par téléphone ou par une application d'authentification, ou d'utiliser une carte à puce. À l'échelle des régions, les résidents du Québec sont plus enclins que ceux des autres régions du pays à utiliser une carte à puce.

Pour près de la moitié des répondants (46 %), les mises à jour du système d'exploitation se font automatiquement. Pour d'autres, les mises à jour sont généralement activées dans un délai d'un jour (14 %), d'une semaine (15 %), d'un mois (9 %) ou d'un an (4 %). Une faible proportion (3 %) affirme ne jamais activer les mises à jour.

Graphique 9 : Fréquence des mises à jour du système d'exploitation



Q8. Les appareils vous invitent souvent à mettre à jour le système d'exploitation (SE). Quand activez-vous cette mise à jour?
Base : n=2710

- Les personnes âgées de 35 à 44 et les 55 ans ou plus sont plus susceptibles que les autres groupes d'âge de se fier à des horaires automatisés pour mettre à jour leur système d'exploitation. Cela est aussi plus fréquent au Québec et chez les hommes que chez leurs homologues.
- Les personnes qui effectuent des mises à jour hebdomadaires ou moins fréquentes sont plus souvent âgées de moins de 25 ans, alors que celles qui le font mensuellement sont plus souvent âgées de 25 à 34 ans.

Neuf Canadiens sur dix (90 %) sécurisent leur réseau Wi-Fi à domicile avec un mot de passe unique, bien que 29 % utilise le mot de passe par défaut. Sept personnes sur dix (68 %) créent un mot de passe. Seulement 17 % ont un réseau d'invités avec un mot de passe distinct.

Tableau 5 : Protection du réseau sans fil

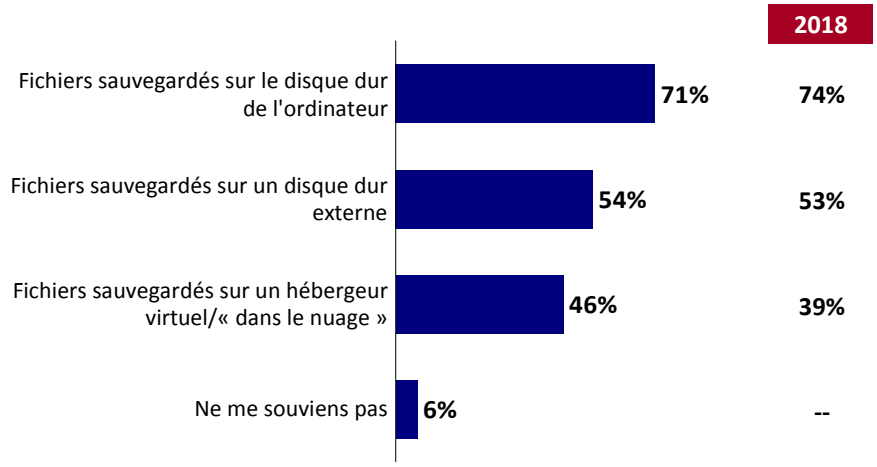
--	**Total 2020**	**Total 2018**
QB2B. Protégez-vous le réseau sans fil de votre maison avec un mot de passe unique?	*n=2710*	*n=1801*
Oui	90 %	96 %
Non	4 %	3 %
Je n'ai pas un réseau sans fil à la maison	3 %	--
Je ne sais pas	2 %	1 %
Pas de réponse	1 %	--
Q9. Le mot de passe que vous utilisez est-il celui fourni par défaut avec l'appareil (p. ex., un routeur) ou s'agit-il d'un nouveau mot de passe que vous avez créé vous-même?	*n=2430*	
Oui, mot de passe par défaut	29 %	
Non, je l'ai créé moi-même	68 %	
Je ne sais pas	2 %	
Pas de réponse	1 %	
Q10. Utilisez-vous un réseau pour invités avec un mot de passe distinct pour vos appareils intelligents et pour les visiteurs?	*n=2710*	
Oui	17 %	
Non	77 %	
Je ne sais pas	4 %	
Pas de réponse	3 %	

- Même si presque tout le monde sécurise son réseau sans fil à domicile, cette pratique est plus répandue chez les Canadiens âgés de 25 à 54 ans, chez les Ontariens ainsi que chez les répondants dont le niveau de scolarité et le revenu du ménage sont le plus élevés. Même parmi ceux qui sont les moins susceptibles de le faire, l'incidence est à peine inférieure à 90 %, sauf chez ceux qui n'ont fait que des études secondaires ou dont le revenu du ménage est plus faible, où elle est de seulement 82 %.

- Le mot de passe par défaut est utilisé un peu plus souvent par les gens âgés de moins de 25 ans ou de 55 à 64 ans. Cette pratique est aussi plus fréquente au Québec que dans d'autres régions, ainsi que chez les femmes, comparativement aux hommes.
- Bien que relativement peu de gens utilisent un mot de passe pour invités, cette pratique est un peu plus répandue chez les 35 à 44 ans, chez les parents et chez les gens aux revenus les plus élevés.

Près de trois Canadiens sur quatre (71 %) sauvegardent leurs fichiers sur le disque dur d'un ordinateur. Plus de la moitié (54 %) stockent leurs données sur un disque dur externe et une proportion moindre (46 %) a recours à un hébergeur virtuel ou à un nuage. Les résultats étaient très semblables en 2018, mais une proportion un peu plus élevée de Canadiens se fient au nuage en 2020.

Graphique 10 : Stockage d'information



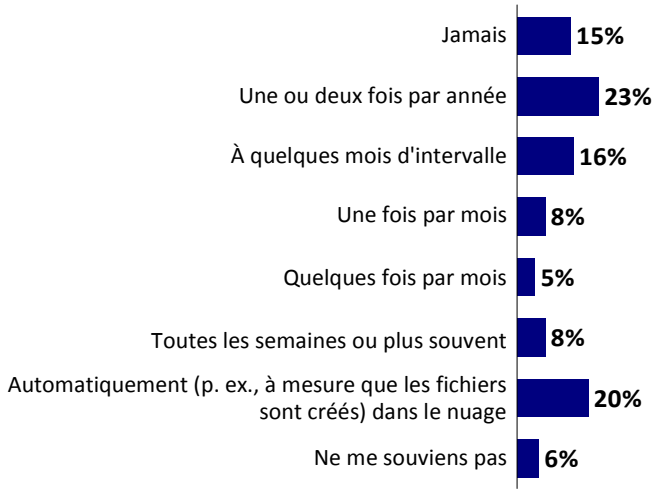
QD1B. En ce qui concerne le stockage de l'information à des fins personnelles, est-ce que vous sauvegardez vos données sur le disque dur de votre ordinateur, sur un disque dur externe (stockage supplémentaire/d'appoint) ou sur un hébergeur virtuel (c.-à-d. de l'informatique en nuage).
Base : n=2710

- Le niveau de scolarité, l'âge, le revenu et le sexe sont tous des facteurs importants lorsqu'il est question de l'utilisation de l'une ou l'autre des options de stockage de l'information signalées ci-dessus. Les Canadiens âgés de 54 ans ou moins ainsi que les parents sont plus susceptibles que leurs homologues plus âgés d'utiliser un nuage. Les hommes ont plus tendance que les femmes à utiliser des disques durs d'ordinateurs ou des disques durs externes. Les gens qui ont fait des études universitaires et ceux dont le revenu annuel du

ménage est d'au moins 80 000 dollars sont plus enclins à mentionner toutes les options présentées.

Une personne sur cinq (20 %) sauvegarde automatiquement ses données et ses fichiers personnels sur un nuage à partir d'un ordinateur, d'un téléphone intelligent ou de tout autre appareil mobile. Une proportion semblable (23 %) sauvegarde manuellement ses fichiers une ou deux fois par année, alors qu'un moins grand nombre de répondants le fait à des intervalles de quelques mois (16 %), une fois par mois (8 %), quelques fois par mois (5 %), ou une fois par semaine ou plus (8 %). Certains Canadiens (15 %) ne sauvegardent jamais leurs fichiers.

Graphique 11 : Fréquence de l'utilisation de dispositifs de sauvegarde



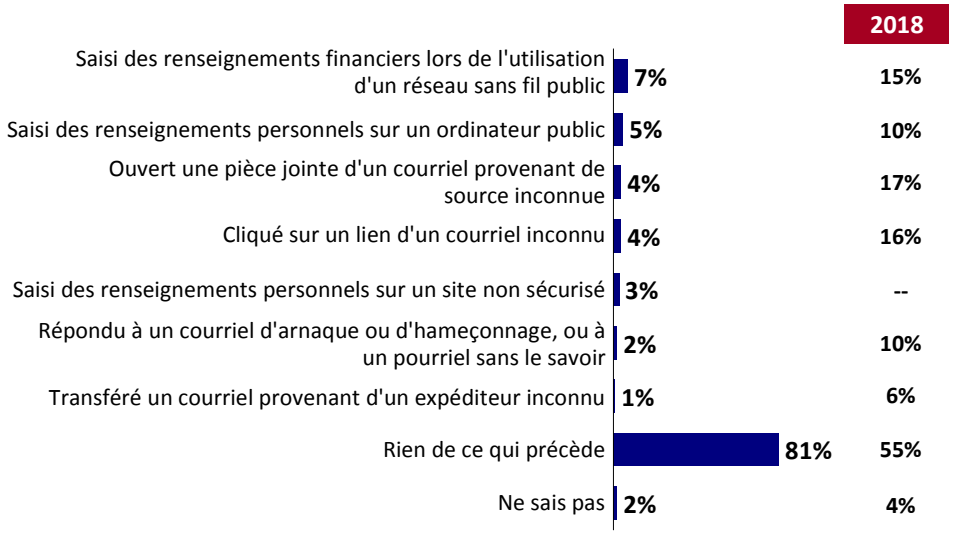
QB5X. À quelle fréquence sauvegardez-vous des données ou des fichiers personnels stockés sur votre ordinateur, sur votre téléphone intelligent ou sur un autre appareil mobile?
Base : n=2710

- Les Canadiens plus jeunes (moins de 25 ans) sont plus susceptibles que ceux des autres groupes d'âge de sauvegarder leurs fichiers une ou deux fois par année, alors que les parents, les personnes âgées de 25 à 54 ans et celles dont le niveau de scolarité ou le revenu sont plus élevés ont plus tendance à sauvegarder automatiquement leurs fichiers (car elles sont aussi plus susceptibles d'utiliser un nuage). Les Canadiens plus âgés, tout comme les femmes, les résidents du Québec et les Canadiens ayant un revenu moins élevé ou un niveau de scolarité moins élevé, sont plus susceptibles que ceux des autres segments de dire qu'ils ne sauvegardent jamais leurs fichiers.

Huit Canadiens sur dix (81 %) déclarent ne pas s'être comportés d'une façon risquée en matière de cybersécurité. Moins d'une personne sur dix saisit des renseignements financiers sur un réseau sans fil public (7 %) ou sur un ordinateur public (5 %), ouvre des pièces jointes de courriels provenant d'une source inconnue (4 %), clique sur le lien d'un courriel ou d'un texto inconnu (4 %), saisit des renseignements personnels sur un site non sécurisé (3 %) ou répond sans le savoir à un courriel d'arnaque ou d'hameçonnage, ou à un pourriel (2 %).

Une question semblable était posée en 2018, bien qu'elle demandait si cela s'était « déjà » produit, plutôt que de faire allusion au dernier mois. Même si la question n'est pas tout à fait comparable, elle donne une idée de la fréquence de certains comportements (p. ex., le fait d'ouvrir une pièce jointe ou de cliquer sur un lien, de répondre à un courriel d'hameçonnage ou à un pourriel, ou de transférer un courriel provenant d'un expéditeur inconnu). L'utilisation d'un réseau sans fil public et de renseignements personnels sur un appareil public se produit encore assez souvent, même au cours du mois précédent.

Graphique 12 : Types de risques pris



QB11. Au cours du dernier mois, avez-vous…
Base : n=2710. Base de 2018 : 2072

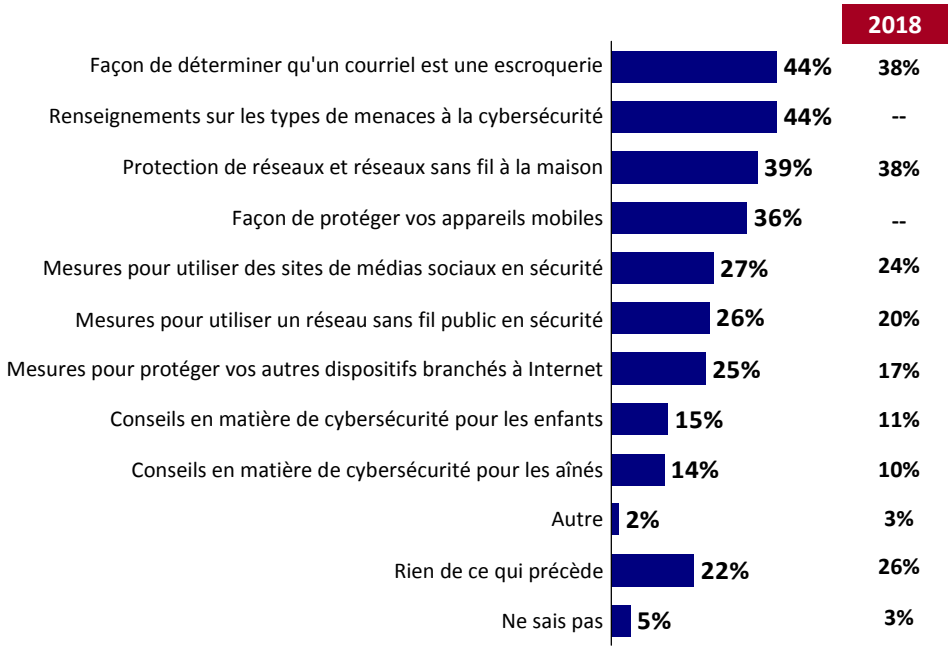
- Les personnes âgées de moins de 25 ans (ainsi que celles dont le revenu du ménage est inférieur à 40 000 dollars) sont plus susceptibles que les autres d'avoir saisi des renseignements personnels sur un site non sécurisé ou sur un ordinateur public, ou d'avoir saisi des renseignements financiers sur un réseau sans fil public. Les Canadiens plus âgés (55 ans et plus) sont plus enclins que ceux des autres groupes d'âge à dire qu'ils ne l'ont pas fait.

D. INFORMATION

Moins de la moitié des Canadiens recherchent de l'information sur la façon de savoir si un courriel est frauduleux (44 %) ou sur les types de cybermenaces qui existent (44 %). Plus du tiers des répondants recherche des renseignements sur la sécurité des réseaux sans fil domiciliaires (39 %) ou sur la protection des appareils mobiles (36 %). Le quart des répondants recherche des renseignements sur l'utilisation sécuritaire des sites de médias sociaux (27 %), sur les mesures à prendre pour utiliser en toute sécurité un réseau sans fil public (26 %) ou les mesures à prendre pour protéger d'autres appareils connectés à Internet, comme les télévisons intelligentes, les systèmes de sécurité du domicile, les moniteurs d'activité physique et les appareils à commande vocale (25 %). Plus d'une personne sur dix recherche des conseils sur la cybersécurité des enfants (15 %) ou des personnes âgées (14 %), tandis qu'une personne sur cinq (22 %) ne recherche jamais de renseignements sur la cybersécurité.

Bien qu'ils reflètent les réponses à une question quelque peu différente, les résultats de 2020 suggèrent que plusieurs sujets font plus souvent l'objet de recherches qu'en 2018 (façon de reconnaître un courriel frauduleux, d'utiliser en toute sécurité un réseau sans fil public ou de protéger d'autres appareils branchés à Internet).

Graphique 13 : Type d'information recherché



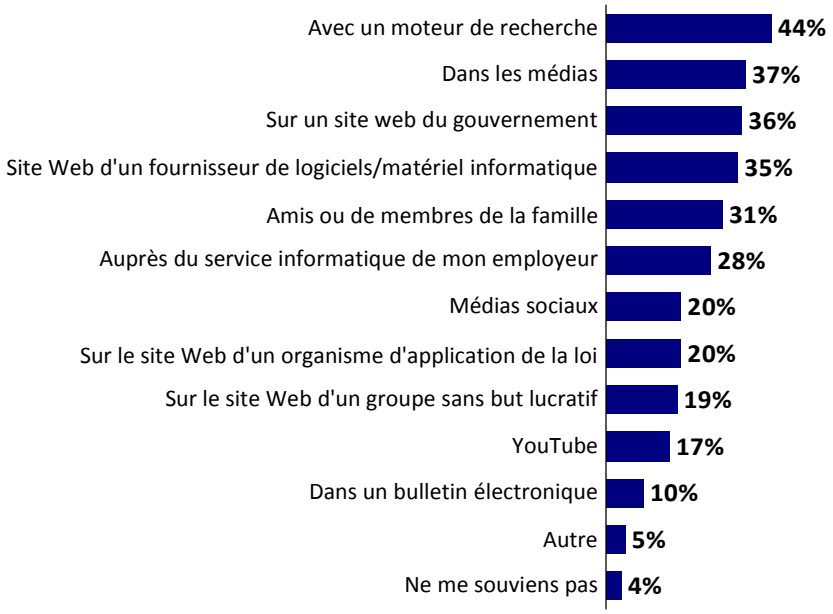
QIC5a. Avez-vous déjà recherché les types de renseignements suivants sur la cybersécurité? 2018 : S'il y en a, sur quels types de renseignements traitant de cybersécurité parmi les suivants avez-vous déjà fait des recherches?
Base : n=2710. Base de 2018 : 2072

- Les Canadiens plus jeunes (moins de 25 ans) sont moins susceptibles que ceux des autres groupes d'âge d'avoir recherché de l'information sur les types de cybermenaces. Les Canadiens âgés de 65 ans ou plus ont plus tendance que les autres à avoir recherché des renseignements sur la sécurité Internet pour les aînés et moins susceptibles d'avoir recherché des mesures à suivre pour utiliser en toute sécurité un réseau sans fil public ou des sites de médias sociaux. Les personnes âgées de 35 à 54 ans sont plus susceptibles d'avoir recherché de l'information sur la sécurité du réseau sans fil à domicile ou des conseils sur la cybersécurité des enfants.
- Les parents ont également plus tendance que les autres Canadiens à rechercher de l'information sur la protection de réseaux sans fil à la maison, d'appareils mobiles et d'autres dispositifs branchés à Internet, comme des télévisions intelligentes, des systèmes de sécurité résidentiels et des dispositifs de reconnaissance vocale, ainsi que des conseils sur la cybersécurité des enfants et des mesures pour utiliser des sites de médias sociaux en toute sécurité.

- Les hommes, ainsi que les répondants dont le niveau de scolarité ou le revenu du ménage sont plus élevés, sont plus enclins que les femmes et les gens dont le niveau de scolarité ou le revenu du ménage sont plus bas à déclarer rechercher de l'information sur la plupart des domaines mentionnés.
- Les résidents du Québec sont moins enclins que les autres Canadiens à rechercher de l'information sur la plupart des domaines évoqués.

Quarante-quatre pour cent des Canadiens recherchent de l'information sur la cybersécurité à l'aide d'un moteur de recherche. Environ trois personnes sur dix trouvent de l'information dans les médias, notamment sur un site Web d'actualités (37 %), d'un gouvernement (36 %) ou d'un fournisseur de logiciels ou de matériel informatique (35 %), ou auprès d'amis et de membres de leur famille (31 %). Le quart des répondants (28 %) recherche de l'information par l'intermédiaire du service des TI de son employeur. Une personne sur cinq mentionne comme source les médias sociaux (20 %), le site Web d'un organisme d'application de la loi (20 %), le site Web d'un groupe sans but lucratif (19 %) ou sur YouTube (17 %). Dix pour cent trouvent de l'information dans un bulletin électronique.

Graphique 14 : Sources d'information

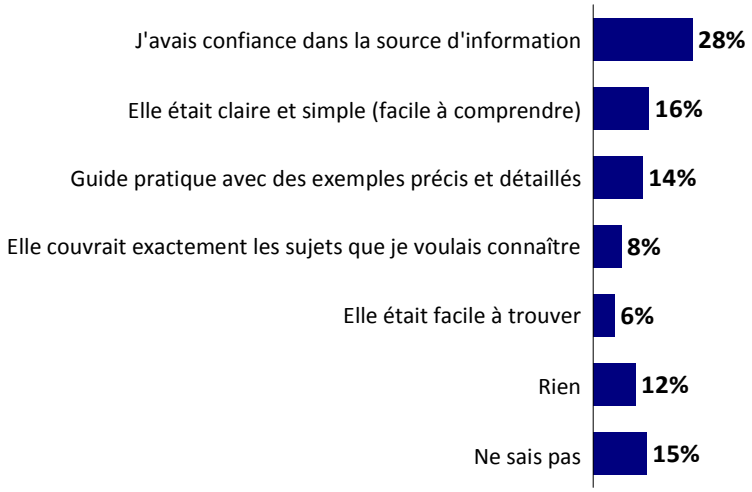


QIC5b. Où êtes-vous allé chercher cette information?
Base : N=1977 (toute personne recherchant de l'information sur l'un des sujets énumérés dans le tableau 13)

- Les personnes âgées de moins de 25 ans sont plus susceptibles que celles des autres groupes d'âge de rechercher de l'information dans les médias sociaux ou sur YouTube. Les personnes âgées de 25 à 54 ans, les parents ainsi que les répondants dont le niveau de scolarité ou le revenu du ménage sont plus élevés ont plus tendance que leurs homologues à dire qu'elles recherchent de l'information auprès du service des TI de leur employeur. Les Canadiens plus âgés (55 ans et plus) sont plus enclins à rechercher de l'information auprès de leurs amis ou de membres de leur famille, ou dans un bulletin électronique. Les 55 à 64 ans ont plus tendance que les répondants des autres segments à rechercher des renseignements sur le site Web d'un fournisseur ou du gouvernement.
- Les hommes sont plus enclins que les femmes à trouver de l'information par le biais d'un moteur de recherche, du site Web d'un fournisseur, du site Web d'un organisme sans but lucratif ou d'un bulletin électronique.
- Les personnes ayant un niveau de scolarité plus élevé et les résidents de la Colombie-Britannique sont plus susceptibles que les autres répondants d'utiliser le site Web d'un groupe sans but lucratif.
- Les résidents de l'Ontario sont plus susceptibles que ceux des autres régions à utiliser YouTube.

Un peu plus d'une personne sur quatre (28 %) considère l'information qu'elle recherche comme utile parce qu'elle se fie à la source d'information. Le fait que l'information est claire et simple (16 %) ou le fait que l'information constitue un guide pratique avec des exemples précis et détaillés (14 %) sont d'autres raisons pour lesquelles les répondants considèrent les renseignements comme utiles. Moins d'une personne sur dix fait confiance à l'information parce qu'elle couvre exactement les sujets qu'elle veut connaître (8 %) ou parce qu'elle est facile à trouver (6 %).

Graphique 15 : Raisons pour lesquelles les renseignements sont utiles



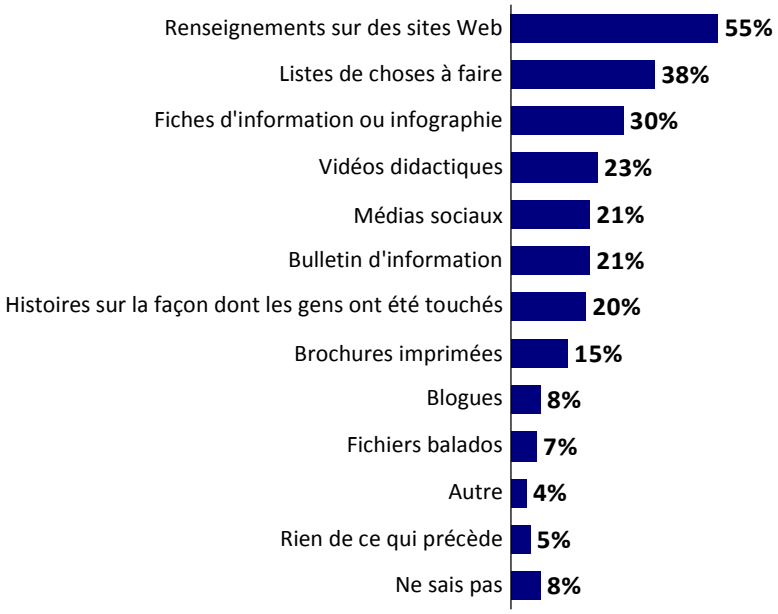
QIC8b. Quels aspects de cette information étaient utiles?
Base : n=2710

- Les Canadiens plus jeunes sont plus susceptibles que ceux âgés de 25 ans ou plus de dire que l'information est claire et facile à comprendre (ce groupe est plus enclin à recourir aux médias sociaux ou à YouTube).
- Les personnes qui ont fait des études universitaires sont plus susceptibles que les personnes dont le niveau de scolarité est plus bas d'affirmer qu'elles se fient à la source d'information ou que l'information est utile parce qu'elle utilise des exemples précis et détaillés.

Plus de la moitié (55 %) des Canadiens préfèrent obtenir de l'information sur la protection contre les cybermenaces sur un site Web. Trois personnes sur dix préfèrent les listes de choses à faire (38 %), ou encore les fiches d'information et les infographies (30 %). Une personne sur cinq dit préférer les vidéos didactiques (23 %), les médias sociaux (21 %), les bulletins d'information, comme les abonnements par courriel (21 %), ou les histoires sur la façon dont les gens ont été touchés par une cybermenace (20 %). Un moins grand nombre cite les

brochures imprimées (15 %), les fichiers balados (8 %) ou les blogues (7 %) comme un moyen privilégié d'obtenir de l'information.

Graphique 16 : Type ou méthode d'information privilégiée



Q20. Comment préférez-vous obtenir de l'information pour vous protéger contre les cybermenaces?
Base : n=2651

- Les Canadiens plus jeunes (moins de 25 ans) sont plus susceptibles que ceux des autres groupes d'âge de préférer les fiches d'information ou les infographies, les histoires sur la façon dont les gens ont été touchés ou les médias sociaux. Les parents sont également plus enclins que d'autres personnes à mentionner les médias sociaux. Les Canadiens plus âgés (55 ans et plus) sont plus susceptibles que les plus jeunes de préférer les listes de choses à faire, les brochures imprimées ou les bulletins d'information.
- Les personnes âgées de 35 à 44 ans, ainsi que les hommes, les résidents de l'Ontario et les résidents dont le niveau de scolarité ou le revenu du ménage sont plus élevés ont plus tendance que leurs homologues à préférer trouver de l'information dans des sites Web.
- En plus des Canadiens plus âgés, les résidents du Québec, les femmes et ceux dont le niveau de scolarité est plus élevé sont plus susceptibles de préférer les listes de choses à faire.

Près du tiers des Canadiens (30 %) affirment aider d'autres personnes à se protéger contre les cybermenaces, notamment leurs parents (61 %) ou des amis (59 %). Près de la moitié (48 %) des gens qui aident d'autres personnes en matière de cybersécurité portent assistance à des membres de leur famille. Le tiers (33 %) dit aider des collègues et trois répondants sur dix (29 %) affirment aider leurs enfants. Environ une personne sur cinq aide ses voisins (21 %) ou ses grands-parents (17 %). Neuf pour cent aident des propriétaires de petites entreprises.

Tableau 6 : Aider d'autres personnes avec la cybersécurité

--	**Total 2020**
Q21. Aidez-vous d'autres personnes avec la cybersécurité?	*n=2710*
Oui	30 %
Non	64 %
Je ne sais pas	4 %
Pas de réponse	2 %
Q22. Qui aidez-vous?	*n=803*
Vos parents	61 %
Des ami(e)s	59 %
D'autres membres de votre famille	48 %
Des collègues	33 %
Vos enfants	29 %
Des voisin(e)s	21 %
Vos grands-parents	17 %
Propriétaires de petite entreprise	9 %
Autre	2 %

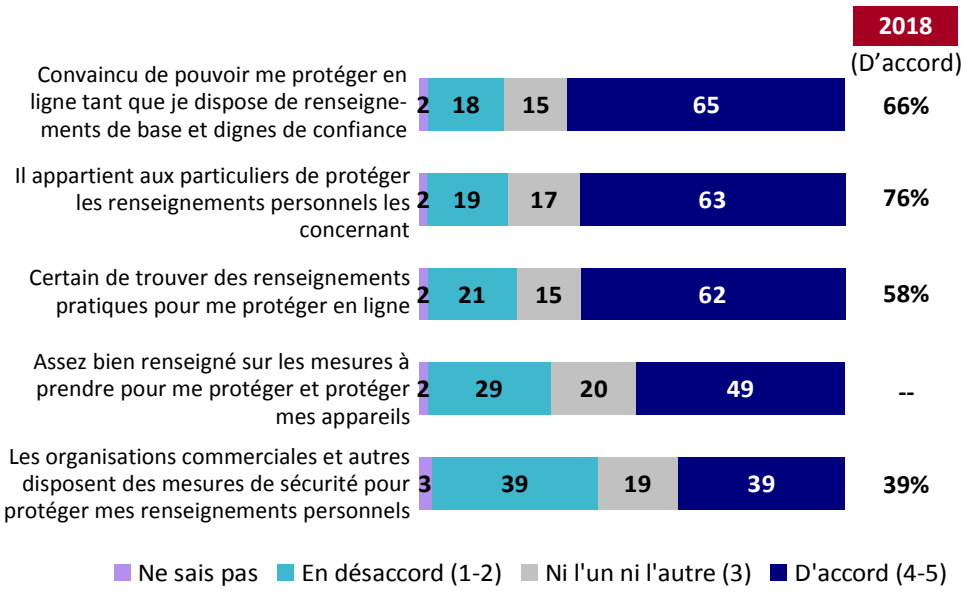
- Les Canadiens âgés de 25 à 44 ans, les parents, les hommes, les résidents de l'Ontario et les gens dont le niveau de scolarité ou le revenu du ménage sont plus élevés ont plus tendance que les autres à déclarer aider d'autres personnes avec la cybersécurité.
- Les Canadiens âgés de 18 à 44 ans sont plus susceptibles que les autres groupes d'âge d'aider leurs parents, tandis que ceux âgés de 35 à 54 ans aident généralement leurs enfants. Les Canadiens plus jeunes (18 à 34 ans) sont aussi plus susceptibles d'aider leurs grands-parents que les autres segments d'âge.
- Les parents ont aussi plus tendance que les autres segments à dire qu'ils aident leurs enfants, leurs parents et les grands-parents.

- Les hommes sont plus susceptibles que les femmes d'aider leurs amis, leurs voisins ou d'autres membres de leur famille.
- Les répondants du Québec sont plus enclins que les résidents des autres régions à aider d'autres membres de leur parenté.

Près des deux tiers des Canadiens (65 %) sont convaincus de pouvoir se protéger en ligne, à condition d'avoir accès à des renseignements de base et fiables sur les mesures à prendre. Une moindre proportion est d'accord pour dire qu'il appartient aux personnes de protéger leur vie privée (63 %) ou croit savoir comment trouver des renseignements pratiques pour se protéger en ligne (62 %). Cependant, seule la moitié d'entre eux (49 %) estime posséder suffisamment de renseignements sur la façon de prendre des mesures pour se protéger contre les cybermenaces. Deux personnes sur cinq (39 %) croient que les entreprises d'autres organisations prennent des mesures de sécurité adéquates pour protéger leurs renseignements personnels.

Les résultats de 2018 sont semblables pour trois des quatre questions qui revenaient dans la version de 2020, bien que les Canadiens soient cette année moins enclins à convenir qu'il appartient aux gens de protéger leur vie privée, alors que 76 % des répondants affirmaient cela en 2018.

Graphique 17 : Attitudes envers l'information

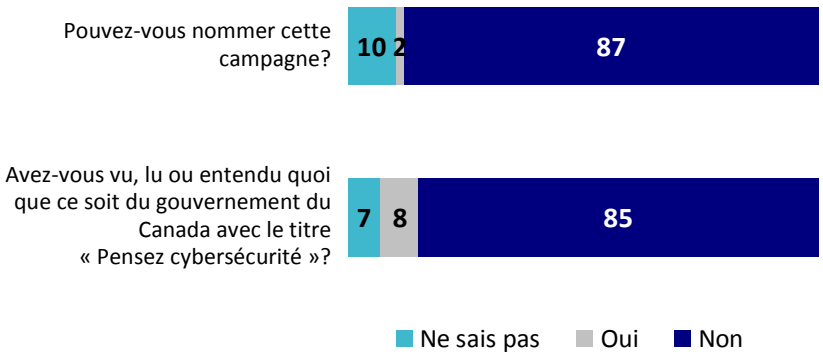


QA13, A11B, A118, Q120, A110. Veuillez indiquer dans quelle mesure vous êtes d'accord ou en désaccord avec les énoncés ci-dessous.
Base : n=2710, Base de 2018 – 2072

- Les personnes âgées de 18 à 44 ans sont plus susceptibles que celles des autres groupes d'âge de convenir qu'elles possèdent assez d'information pour prendre des mesures et pour savoir comment trouver des renseignements pratiques. Les Canadiens plus jeunes (moins de 25 ans) sont plus susceptibles que les autres de croire que les entreprises disposent de mesures de protection adéquates pour protéger leurs renseignements personnels.
- Les parents ont aussi plus tendance que les autres segments à déclarer savoir comment trouver des renseignements pratiques en ligne.
- Les hommes et les répondants dont le revenu du ménage est plus élevé ont plus tendance que leurs homologues à convenir qu'ils possèdent assez d'information pour prendre des mesures, qu'ils savent comment trouver des renseignements pratiques et qu'ils peuvent se protéger en ligne.
- Les résidents du Québec sont moins susceptibles que les résidents des autres régions de se fier à leur capacité à trouver des renseignements pratiques.

Très peu de Canadiens (2 %) sont aptes à nommer une campagne de sensibilisation du gouvernement du Canada qui a été créée pour informer la population canadienne sur la cybersécurité et sur les mesures simples qu'ils peuvent prendre pour se protéger en ligne. Une plus grande proportion (8 %) indique connaître la campagne Pensez cybersécurité du gouvernement du Canada une fois que celle-ci est nommée.

Graphique 18 : Connaissance de la campagne Pensez cybersécurité



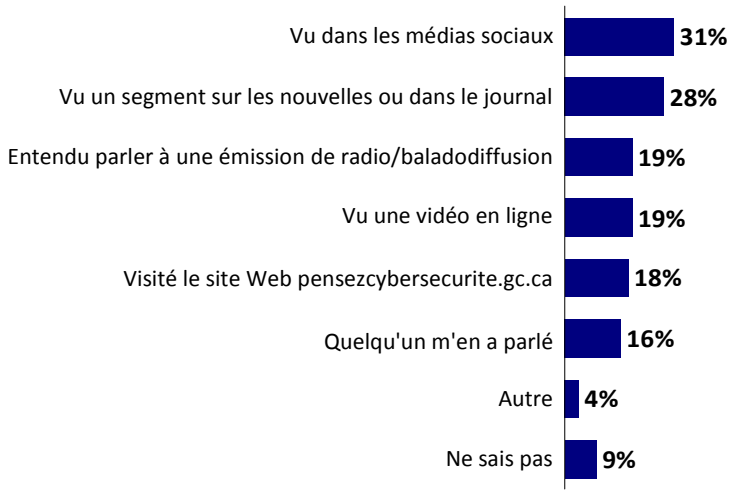
Q23. Une campagne de sensibilisation du gouvernement du Canada a été créée pour informer les Canadiens sur la cybersécurité et sur les mesures simples qu'ils peuvent prendre pour se protéger en ligne. Pouvez-vous nommer cette campagne?
Base : n=2683

QGOCAD. Avez-vous vu, lu ou entendu quoi que ce soit du gouvernement du Canada avec le titre Pensez cybersécurité qui abordait les menaces en ligne et la façon de vous en protéger?
Base : n=2710

- Lorsqu'ils sont informés de la campagne Pensez cybersécurité, les Canadiens plus jeunes (moins de 25 ans), les parents, les gens dont le revenu est plus élevé (150 000 dollars) ainsi que les résidents du Manitoba et du Québec sont plus susceptibles d'affirmer qu'ils en ont entendu parler.

Parmi ceux qui disent connaître la campagne Pensez cybersécurité, 31 % ont lu quelque chose dans les médias sociaux et 28 % ont vu quelque chose dans les nouvelles ou dans un journal. Moins d'une personne sur cinq en a entendu parler à une émission de radio ou dans un fichier balado (19 %), dans une vidéo en ligne (18 %), sur le site Web pensezcybersécurité.ca (18 %) ou par l'entremise de quelqu'un (16 %).

Graphique 19 : Connaissance de la campagne Pensez cybersécurité



QGOCADA. Où l'avez-vous vu, lu ou entendu?
Base : n=210

E. EXPÉRIENCE D'ENTREPRISES

Près de la moitié des propriétaires ou des gestionnaires d'entreprise (47 %) sont responsables des TI de leur entreprise. Plus d'un employé sur cinq (23 %) affirme qu'un employé de l'organisation se consacre aux TI. Plus d'une personne sur dix (14 %) confie cette tâche à une entreprise de TI et 5 % n'ont aucun responsable des TI.

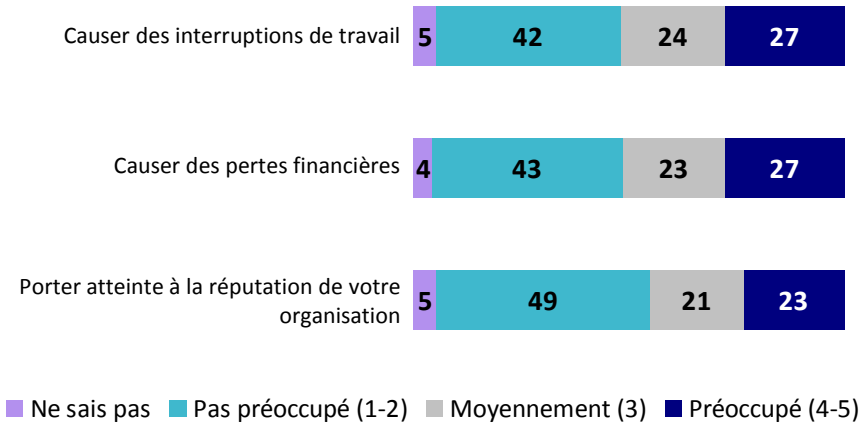
Graphique 20 : Responsabilité pour les services des TI

QBUS4. Qui est responsable des TI de votre société?
Base : n=356

- Les propriétaires et les gestionnaires d'entreprises plus âgés (65 ans et plus) sont plus susceptibles que les plus jeunes répondants d'affirmer être responsables des TI de leur entreprise. Ceux qui ont un revenu plus élevé (150 000 dollars ou plus) sont plus susceptibles que ceux dont le revenu est plus bas de dire qu'ils confient leurs TI à une entreprise.

Lorsqu'il est question de préoccupations liées aux activités quotidiennes, plus du quart des propriétaires ou des gestionnaires d'entreprise se préoccupent des interruptions de travail (27 %) ou des pertes financières (27 %) que peuvent causer les cybermenaces. Un peu moins de répondants (23 %) sont préoccupés par l'atteinte à la réputation de l'organisation.

Graphique 21 : Niveau de préoccupation

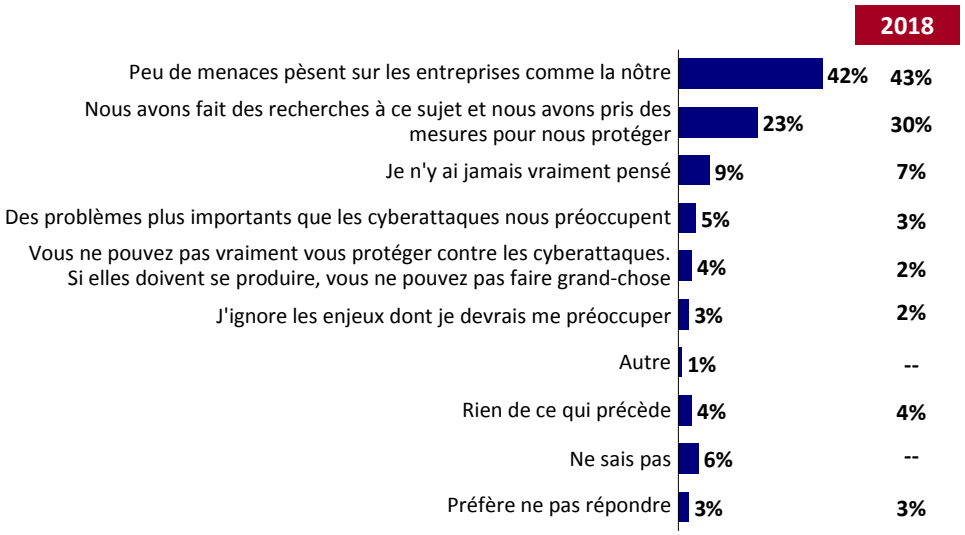


QBUS5A1-A3. En ce qui concerne les diverses préoccupations liées aux activités quotidiennes de votre organisation, à quel point êtes-vous préoccupé(e) par le fait qu'une cybermenace puisse.
Base : n=360

- Les hommes sont plus susceptibles que les femmes de se préoccuper des interruptions de travail.

Parmi les gens qui ne s'inquiètent pas, plus de deux personnes sur cinq (42 %) disent croire que peu de menaces pèsent sur les entreprises comme la leur. Une personne sur cinq (23 %) affirme avoir effectué des recherches et pris des mesures pour protéger son entreprise. Une personne sur dix (9 %) signale qu'elle n'a jamais vraiment pensé à la cybersécurité. Parmi les autres mentions, certains répondants disent que des problèmes plus importants que les cyberattaques les préoccupent (5 %), croient qu'il n'y a pas grand-chose à faire pour prévenir une cyberattaque (4 %) ou sont incertains des problèmes qui devraient les inquiéter (3 %).

Graphique 22 : Raison du manque de préoccupation



QBUS5b. Pourquoi donc?
Base : n=203

- Les répondants dont le niveau de scolarité ou le revenu sont plus élevés ont un peu moins tendance à s'inquiéter, car ils font des recherches et prennent des mesures pour se protéger.
- Les hommes et les gens âgés de 25 à 34 ans sont plus susceptibles que les autres répondants de dire qu'ils ne sont pas inquiets parce qu'ils n'y ont jamais pensé. Les femmes qui sont des propriétaires ou des gestionnaires d'entreprise sont moins susceptibles que les autres de s'inquiéter parce qu'elles estiment que peu de menaces pèsent sur les entreprises comme la leur.

Plus de la moitié des propriétaires ou des gestionnaires d'entreprise déclarent que leur entreprise a un système de protection par mot de passe sur tous ses appareils (57 %), qu'elle utilise un mot de passe ou un système d'authentification d'utilisateur pour l'accès sans fil et à distance (52 %) ou qu'elle utilise un logiciel de sécurité à jour sur tous leurs appareils (51 %). Un peu moins de la moitié (49 %) prennent les mesures nécessaires pour sauvegarder les renseignements sur tous leurs appareils, tandis que deux répondants sur cinq (39 %) installent des logiciels de filtrage antipourriel pour se protéger contre les cybermenaces. Environ une personne sur cinq utilise un logiciel de cryptage (23 %), suit des protocoles de suppression d'information lorsque des employés quittent l'organisation (18 %), adopte une politique de cybersécurité pour les employés (18 %), fournit une formation sur la cybersécurité à ses employés (15 %) ou évite d'utiliser un compte d'administrateur pour accéder au Web (15 %).

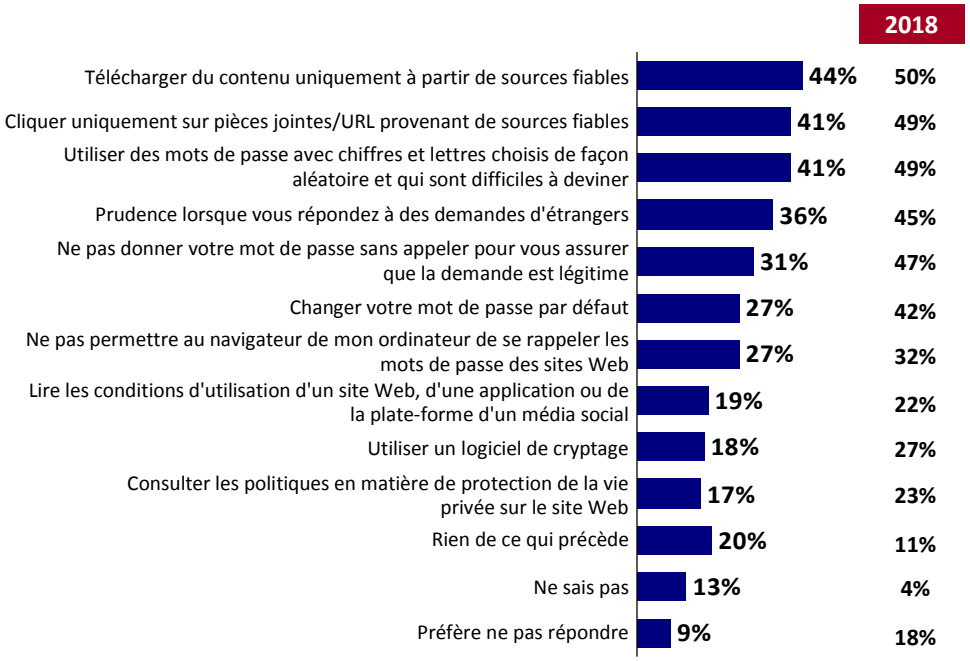
Graphique 23 : Mesures prises pour prévenir les attaques ou s'en protéger

QBUS1. En ce qui concerne votre travail de propriétaire ou gestionnaire d'entreprise, quelles mesures parmi les suivantes votre entreprise a-t-elle prises pour se protéger contre les menaces en ligne?
Base : n=360

- Les représentants commerciaux dont le niveau de scolarité et le revenu sont plus élevés ont plus tendance que les autres répondants à garder les logiciels de sécurité à jour, à installer des logiciels de filtrage antipourriel, à adopter une politique de cybersécurité pour tous les employés et à utiliser une protection par mot de passe sur tous les dispositifs.

Environ deux propriétaires ou gestionnaires d'entreprise sur cinq déclarent que les employés sont tenus de télécharger du contenu uniquement à partir de sources fiables (44 %), de cliquer uniquement sur les pièces jointes ou URL provenant de sources fiables (41 %) ou d'utiliser des mots de passe qui contiennent des chiffres et lettres choisis de façon aléatoire et qui sont difficiles à deviner (41 %). Environ le tiers des répondants demandent aux employés de faire preuve de prudence lorsqu'ils répondent à des demandes d'étrangers (36 %) ou de ne pas donner leur mot de passe sans appeler pour s'assurer que la demande est légitime (31 %). Un peu plus du quart demande à ses employés de changer leur mot de passe par défaut (27 %) ou de ne pas permettre au navigateur de leur ordinateur de se rappeler les mots de passe des sites Web (27 %). Une personne sur cinq demande à ses employés de lire les conditions d'utilisation d'un site Web, d'une application ou de la plate-forme d'un média social (19 %), d'utiliser un logiciel de cryptage (18 %) ou de consulter les politiques en matière de protection de la vie privée sur le site Web (17 %). Une personne sur cinq (20 %) ne fournit aucune directive à ses employés pour protéger l'entreprise contre les cybermenaces.

Graphique 24 : Instructions aux employés



QBUS2. Quelles instructions parmi les suivantes fournissez-vous aux employés pour protéger votre organisation contre les cybermenaces et pour protéger vos renseignements personnels?
Base : n=360

- Les personnes dont le niveau de scolarité est plus élevé sont plus enclines que les autres répondants à fournir la plupart des instructions à leurs employés.

Deux propriétaires ou gestionnaires d'entreprise sur cinq disent que leur organisation bénéficierait d'une liste de types de menaces qui existent et de signaux à rechercher (41 %), de directives pour réagir à une cyberattaque (40 %) ou de mesures pour protéger les appareils mobiles dans un lieu public (39 %). 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 chiffrer des ordinateurs, des portables et des dispositifs de stockage (34 %), à des pratiques exemplaires sur l'utilisation de dispositifs de stockage ou à des directives sur l'utilisation d'appareils personnels pour le travail (31 %). Environ une personne sur quatre indique que son organisation tirerait profit de conseils et de ressources sur le type de logiciel ou de matériel permettant de sécuriser des réseaux (29 %), de pratiques exemplaires sur la façon pour les employés de gérer les mots de passe (29 %), de directives pour mettre en place des règles relatives à la politique d'utilisation sécuritaire des courriels (28 %), de pratiques exemplaires pour une politique d'utilisation d'Internet claire (27 %), de directives sur la façon d'établir une politique solide en matière de médias sociaux (26 %) ou de conseils pour communiquer aux employés l'importance de suivre des politiques de cybersécurité (25 %). Un peu moins de répondants considèrent comme important d'avoir des renseignements sur les mesures à adopter pour gérer les renseignements liés au travail que possèdent les employés qui quittent l'organisation (22 %).

Tableau 7 : Renseignements utiles pour les petites et moyennes entreprises

--	**Total 2020**	**Total 2018**
QBUS3. De quels types de renseignements parmi les suivants croyez-vous que votre organisation tirerait profit pour se protéger contre les cybermenaces?	*n=360*	*n=533*
Liste de types de menaces qui existe et signaux à rechercher	41 %	47 %
Directives pour réagir à une cyberattaque	40 %	46 %
Mesures pour protéger les appareils mobiles dans un environnement public	39 %	40 %
Pratiques exemplaires sécuritaires en informatique en nuage (avec la définition)	36 %	35 %
Ressources sur la façon de crypter des ordinateurs, portables et dispositifs de stockage	34 %	37 %
Meilleures pratiques pour l'utilisation de dispositifs de stockage (p. ex., clés USB)	34 %	40 %
Directives sur l'utilisation de dispositifs personnels au travail	31 %	40 %
Conseils et ressources pour le type de logiciel ou matériel permettant de sécuriser des réseaux	29 %	36 %

--	Total 2020	Total 2018
Meilleures pratiques sur la façon pour les employés de gérer les mots de passe	29 %	37 %
Directives pour mettre en place des règles relatives à la politique d'utilisation sécuritaire des courriels	28 %	39 %
Meilleures pratiques pour une politique claire d'utilisation d'Internet	27 %	37 %
Directives sur la façon d'établir une politique solide en matière de médias sociaux	26 %	37 %
Conseils pour communiquer aux employés l'importance de suivre de politiques de cybersécurité	25 %	32 %
Mesures pour gérer les renseignements liés au travail que possèdent les employés qui quittent l'organisation	22 %	33 %
Autre	3 %	4 %
Aucune de ces réponses	9 %	8 %
Je ne sais pas	13 %	12 %
Je préfère ne pas répondre	7 %	7 %

- Les répondants d'entreprises âgés de 55 à 64 ans ainsi que ceux dont le niveau de scolarité est plus élevé sont plus susceptibles de déclarer que leur organisation tirerait profit de la plupart des types d'information.

ANNEXES

A. QUESTIONNAIRE DE SONDAGE (FRANÇAIS)

INTRO

WEB INTRO

Les Associés de recherche EKOS mènent pour le compte du gouvernement fédéral un sondage dans l'ensemble du Canada sur des questions relatives à l'utilisation de la technologie (p. ex., ordinateurs personnels, téléphones cellulaires, téléphones intelligents, télévisions intelligentes, tablettes, etc). Le sondage devrait vous prendre environ 20 minutes. Vous êtes libre d'y participer et vos réponses vont demeurer absolument confidentielles et anonymes. Les renseignements que vous fournirez seront traités conformément aux dispositions de la Loi sur la protection des renseignements personnels et des autres lois de même nature. Le sondage est enregistré auprès du système national d'enregistrement des sondages. **Quelques rappels avant de commencer: -** Sur chaque écran, après avoir sélectionné votre réponse, cliquez sur le bouton « Continuer » au bas de l'écran pour vous déplacer vers l'avant dans le questionnaire. **-** Si vous quittez le sondage avant d'avoir terminé, vous pourrez y revenir plus tard au moyen de l'adresse URL et vous obtiendrez la page où vous étiez en quittant. Les réponses que vous aurez données jusque-là auront été sauvegardées. **-** Pour toute question sur la façon de remplir le questionnaire, veuillez téléphoner à Prob*it*, au numéro 866.211.8881, ou envoyer un courriel à online@ekos.ca. Nous vous remercions à l'avance de votre participation.

D2

Laquelle des catégories suivantes décrit le mieux votre situation d'emploi actuelle? Êtes-vous...?

Employé à temps plein (35 heures ou plus par semaine)	1
Employé à temps partiel (moins de 35 heures par semaine)	2
Travailleur autonome	3
Étudiant à temps plein (qui ne travaille pas)	4
Sans emploi mais qui en cherche	5
Non membre de la population active (p. ex., sans emploi mais qui n'en cherche pas, personne ou parent au foyer à temps plein)	6
À propos de la prestation d'invalidité	7
Congé de maternité ou parental	8
Retraité	9
Autre réponse (veuillez préciser)	77
Pas de réponse	99

QEMP

Employed, D2

Combien d'employés y a-t-il dans l'ensemble des succursales de votre organisation, y compris ceux qui travaillent à temps plein et à temps partiel?

Veuillez préciser	77
Aucune	98
Je ne sais pas/ Pas de réponse	99

QEMPA

DK/NR, QEMP

Croyez-vous que le nombre d'employés dans tous les succursales de votre organisation est supérieur ou inférieur à 100?

Supérieur à 100	1
Inférieur à 100	2
Je ne sais pas/ Pas de réponse	99

QEMPB [1,2]

Full/part-time employed, D2; Fewer than 250 employees, QEMP

Assumez-vous l'une ou l'autre des responsabilités suivantes?

Sélectionner toute réponse pertinente

Gestion d'employés ou supervision du travail d'autres employés	1
Participation aux décisions relatives aux processus et procédures que suivent des employés de votre organisation	2
Rien de ce qui précède	99

D5

Y a-t-il des enfants de moins de 18 ans qui vivent sous votre toit?

Oui	1
Non	2
Pas de réponse	99

QCHILDA [1,5]

Parents, D5

Quels sont les âges des enfants dans votre ménage?

Choisir toutes les réponses pertinentes

Moins de 5 ans	1
6 à 12 ans	2
13 à 15 ans	3
16 à 18 ans	4
19 à 24 ans	5
25 ans ou plus	6
Pas de réponse	9

D4

Quelle est votre année de naissance?

Année	1
Pas de réponse	9999

QAGEY

Hesitant, D4; <18 or NR, terminate

À quelle catégorie d'âge appartenez-vous?

Moins de 18 ans	1
18 à 24	2
25 à 34	3
35 à 44	4

45 à 54	5
55 à 64	6
65 et plus	7
Préfère ne pas répondre	99

Q1

Opening

Prenez-vous des précautions pour protéger vos comptes en ligne, vos comptes de médias sociaux, vos appareils et vos réseaux?

Oui	1
Non	2
Je ne sais pas	98
Pas de réponse	99

Q2

Passwords

En général, à quelle fréquence changez-vous les mots de passe de vos comptes?

Jamais	1
Après quelques années	2
Une fois par année	3
Quelques fois par année	4
Plus de quelques fois par année	5
Quand on m'invite à le faire	6
Quand j'y pense, pas à intervalle fixe	7
Lorsque j'apprends l'existence d'une brèche de sécurité aux nouvelles	8
Je ne sais pas	99

Q3

Changez-vous certains mots de passe plus souvent que d'autres?

Oui	1
Non	2
Je ne sais pas	98
Pas de réponse	99

Q4 [1,8]

Yes, Q3

Quels mots de passe changez-vous le plus souvent?

Veuillez choisir toutes les réponses pertinentes

Courriel à la maison	1
Courriel au travail	2
Comptes de médias sociaux	3
Comptes de services bancaires en ligne	4
Comptes de magasinage en ligne	5
Autre (veuillez préciser)	77
Je ne sais pas	99

Q5 [1,13]

Lorsque vient le temps de choisir vos mots de passe, lesquelles des mesures suivantes prenez-vous?

Veuillez choisir toutes les réponses pertinentes

Mots de passe simples et faciles à mémoriser	1
Mots de passe complexes, avec une combinaison de lettres, de chiffres et de symboles	2
Phrase passe contenant au moins 4 mots et 15 caractères	3
Utilisation du même mot de passe pour plusieurs comptes	4
Utilisation d'un mot de passe différent et unique pour chaque compte	5
Partage d'un mot de passe avec d'autres personnes	6
Prendre en note des mots de passe	7
Utilisation d'un gestionnaire de mots de passe	8
Permettre à votre fureteur ou à une application de se rappeler ou de stocker les mots de passe	9
Autre	77
Rien de ce qui précède	98
Je ne sais pas	99

Q6

MFA

Utilisez-vous <abbr title="Authentification à facteurs multiples signifie que vous avez besoin de plus d'un facteur d'authentification pour vous connecter à un appareil ou à un compte. Par exemple, pour déverrouiller votre téléphone, vous devez saisir un mot de passe et utiliser votre empreinte digitale", style = "colour: blue; border-bottom: 1px dotted black;">une authentification à facteurs multiples?</abbr>

Mobile only :

Multi-factor authentication means that you need more than one authentication factor to log in to a device or an account. For example, to unlock your phone, you need to enter a passcode and scan your fingerprint

Oui	1
Non	2
Je ne sais pas	98
Pas de réponse	99

Q7 [1,15]

Yes, Q6

Lesquels des facteurs d'authentification suivants avez-vous utilisés?

Veuillez choisir toutes les réponses pertinentes

Mots de passe	1
Phrases passe	2
NIP	3
Code reçu par courriel	4
Code reçu par message texte	5
Code reçu par appel téléphonique	6
Code reçu par une application d'authentification	7
Cartes à puce	8
Clés USB	9

Périphériques jetons	10
Empreintes digitales	11
Reconnaissance faciale	12
Reconnaissance vocale	13
Autre (veuillez préciser)	77
Je ne sais pas	98
Pas de réponse	99

Q8

Auto updates

Les appareils vous invitent souvent à mettre à jour le système d'exploitation (SE). Quand activez-vous cette mise à jour?

Automatiquement	1
Une fois par jour	2
Une fois par semaine	3
Une fois par mois	4
Moins d'une fois par année	5
Jamais	6
Je ne sais pas	98
Pas de réponse	99

B2B

Protégez-vous le réseau sans fil de votre maison avec un mot de passe unique?

Oui	1
Non	2
Je n'ai pas un réseau sans fil à la maison	3
Je ne sais pas	98
Pas de réponse	99

Q9

Yes, B2B

Le mot de passe que vous utilisez est-il celui fourni par défaut avec l'appareil (p. ex., un routeur) ou s'agit-il d'un nouveau mot de passe que vous avez créé vous-même?

Mot de passe par défaut	1
Mot de passe créé	2
Je ne sais pas	98
Pas de réponse	99

Q10

Utilisez-vous un réseau pour invités avec un mot de passe distinct pour vos appareils intelligents et pour les visiteurs?

Oui	1
Non	2
Je ne sais pas	98
Pas de réponse	99

D1B [1,5]

En ce qui concerne le stockage de l'information à des fins personnelles, est-ce que vous sauvegardez vos données sur le disque dur de votre ordinateur, sur un disque dur externe (stockage supplémentaire/d'appoint) ou sur un hébergeur virtuel (c.-à-d. de l'informatique en nuage)

Veuillez choisir toutes les réponses pertinentes

Fichiers sauvegardés sur le disque dur de l'ordinateur	1
Fichiers sauvegardés sur un disque dur externe	2
Fichiers sauvegardés sur un hébergeur virtuel/« dans le nuage »	3
Je ne me souviens pas	99

B5X

À quelle fréquence faites-vous des copies de sauvegarde de vos données ou de vos fichiers personnels sur votre ordinateur, votre téléphone intelligent ou votre tablette?

Jamais	1
Une ou deux fois par année	2
À quelques mois d'intervalle	3
Une fois par mois	4
Quelques fois par mois	5
Toutes les semaines ou plus souvent	6
Automatiquement (p. ex., à mesure que les fichiers sont créés) dans le nuage	7
Je ne me souviens pas	99

B11 [1,10]

Phishing

Au cours du dernier mois, avez-vous...

Veuillez choisir toutes les réponses pertinentes

ouvert une pièce jointe d'un courriel provenant de source inconnue?	1
cliqué sur un lien d'un courriel inconnu?	2
transféré un courriel provenant d'un expéditeur inconnu?	3
saisi des renseignements personnels sur un site non sécurisé?	4
saisi des renseignements personnels sur un ordinateur public?	5
saisi des renseignements financiers lors de l'utilisation d'un réseau sans fil public?	6
répondu à un courriel d'arnaque ou d'hameçonnage, ou à un pourriel sans le savoir?	7
Rien de ce qui précède	97
Je ne sais pas	98

K11A [1,20]

Quelles mesures prenez-vous pour vous assurer qu'un site Web est sécurisé?

Veuillez choisir toutes les réponses pertinentes

J'utilise uniquement des sites Web que je connais bien	1
Je m'assure que le site provient d'une source digne de confiance (p. ex., un fournisseur de services Internet ou de logiciels bien connu, le gouvernement, etc.)	2
Je m'assure que le site a une adresse « https »	3
Je m'assure que le site est authentifié par un symbole ou la marque VeriSign	4
Je mène des recherches pour déterminer si le site est légitime ou sécuritaire	5

Je mène des recherches pour déterminer si le site est légitime ou sécuritaire	6
J'utilise un bottin Internet	7
Je lis des commentaires sur le respect de la vie privée et la réputation	8
Impossible : je ne sais pas vraiment, je suis incertain(e)	9
Difficile à garantir : tout site peut être piraté	10
Autre réponse (veuillez préciser)	77
Rien de ce qui précède	98
Je ne sais pas	99

Q11A

Threats

Au cours de la prochaine année, à quel point avez-vous l'impression qu'il est probable que vous soyez victime d'une cybermenace...

compromettant vos renseignements personnels?

Pas du tout probable 1	1
2	2
Moyennement probable 3	3
4	4
Extrêmement probable 5	5
Je ne sais pas	99

Q11B

Threats

Au cours de la prochaine année, à quel point avez-vous l'impression qu'il est probable que vous soyez victime d'une cybermenace...

causant des pertes financières?

Pas du tout probable 1	1
2	2
Moyennement probable 3	3
4	4
Extrêmement probable 5	5
Je ne sais pas	99

Q11C

Threats

Au cours de la prochaine année, à quel point avez-vous l'impression qu'il est probable que vous soyez victime d'une cybermenace...

causant la perte de fichiers ou de photos?

Pas du tout probable 1	1
2	2
Moyennement probable 3	3
4	4
Extrêmement probable 5	5
Je ne sais pas	99

Q12

À quel point croyez-vous qu'il est probable qu'un membre de votre famille ou un(e) de vos ami(e)s soit victime d'une cybermenace au cours de la prochaine année?

Pas du tout probable 1	1
2	2
Moyennement probable 3	3
4	4
Extrêmement probable 5	5
Je ne sais pas	99

Q13 [1,9]

Likely (4-5), Q12

Selon vous, qui sera touché(e)?

Un(e) collègue	1
Un(e) voisin(e)	2
Un(e) ami(e)	3
Un de vos parents	4
Un de vos enfants	5
Un de vos grands-parents	6
Autre :	77
Je ne sais pas	99

Q14

Likely (4-5), Q12

Pourquoi pensez-vous qu'ils seront touchés?

Veuillez préciser :	77
Je ne sais pas	98
Pas de réponse	99

K8A [1,11]

Unlikely (1-2), Q11

Pourquoi ne croyez-vous pas qu'il est probable que vous soyez victime d'une cybermenace?

Veuillez choisir toutes les réponses pertinentes

Nous prenons des mesures pour nous protéger en ligne	1
Nous ne faisons rien de risqué en ligne	2
Le risque nous semble être très mince	3
Les menaces en ligne ne s'appliquent qu'aux entreprises et gens qui ont beaucoup d'argent	4
Je reste à jour ou je suis bien informé(e) au sujet des renseignements et des virus	5
Je travaille dans le domaine de l'informatique et des technologies de l'information	6
J'utilise Apple/iOS, qui n'est pas aussi susceptible aux virus	7
J'utilise Linux, qui n'est pas aussi susceptible aux virus	8
Je n'utilise pas un système d'exploitation de Microsoft	9
Autre réponse (veuillez préciser)	77
Je ne sais pas	99

Q15 [1,11]

Quels types de cybermenaces vous préoccupent le plus?

Veuillez choisir toutes les réponses pertinentes

Courriels d'hameçonnage	1
Virus, logiciels espions et logiciels malveillants	2
Vol d'identité	3
Atteintes à la vie privée	4
Pertes financières	5
Données personnelles conservées pour rançon	6
Perte de renseignements ou de fichiers	7
Données personnelles effacées, modifiées, perdues	8
Autre (veuillez préciser)	77
Rien de ce qui précède	98
Je ne sais pas	99

Q16

À quel point êtes-vous bien préparé(e) pour faire face aux cybermenaces?

Pas du tout préparé(e)	1
Pas préparé(e)	2
Assez préparé(e)	3
Bien préparé(e)	4
Très bien préparé(e)	5
Je ne sais pas	99

Q17 [1,12]

Not prepared, Q16

Pourquoi donc?

Veuillez choisir toutes les réponses pertinentes

Je ne pense pas qu'il est probable que cela m'arrive	1
Je n'ai pas le temps ou je ne me penche jamais sur ce problème	2
Je ne connais pas les différents types de menaces	3
Je ne sais pas où obtenir des renseignements sur les mesures à prendre	4
Les renseignements que je trouve ne sont pas assez simples pour m'aider	5
Vous ne pouvez jamais vraiment vous protéger en ligne	6
Il est inutile d'essayer de se protéger	7
J'ai une copie sauvegardée et je peux m'en remettre	8
Rien	9
Autre (préciser)	77
Je ne sais pas	99

Q18 [1,7]

Avez-vous déjà été victime de l'une des cyberattaques suivantes?

Veuillez choisir toutes les réponses pertinentes

Courriel frauduleux	1
Fraude par texto	2
Virus, logiciels espions, logiciels malveillants sur votre ordinateur	3
Vol d'identité	4
Piratage de comptes de médias sociaux	5
Je ne sais pas	98
Pas de réponse	99

Q19 [1,13]

Si vous saviez ou pensiez avoir été victime d'une cyberattaque, quelles mesures prendriez-vous pour vous protéger?

Veuillez choisir toutes les réponses pertinentes

J'éteindrais mon ordinateur	1
Je supprimerais du matériel suspect (courriel, texte, contenu téléchargé, etc.)	2
Je mettrais mon logiciel de sécurité à jour	3
Je changerais mes mots de passe	4
Je communiquerais avec ma banque	5
Je communiquerais avec les principales agences de crédit du Canada (TransUnion, Equifax)	6
Je communiquerais avec un(e) spécialiste des TI	7
Je communiquerais avec un(e) ami(e) ou un membre de ma famille pour obtenir de l'aide	8
J'appellerais la police	9
Rien	10
Autre (préciser)	77
Je ne sais pas	99

Q20 [1,13]

Comment préférez-vous obtenir de l'information pour vous protéger contre les cybermenaces?

Veuillez choisir toutes les réponses pertinentes

Fichiers balados	1
Blogues	2
Fiches d'information ou infographie	3
Listes de choses à faire	4
Vidéos didactiques	5
Histoires sur la façon dont les gens ont été touchés	6
Renseignements sur des sites Web	7
Brochures imprimées	8
Bulletin d'information (p. ex., abonnement à un courriel)	9
Médias sociaux	10
Autre (préciser)	77
Rien de ce qui précède	97
Je ne sais pas	99

Q21

Where do you go for Information

Aidez-vous d'autres personnes avec la cybersécurité?

Oui	1
Non	2
Je ne sais pas	98
Pas de réponse	99

Q22 [1,11]

Yes, Q21

Qui aidez-vous?

Veuillez choisir toutes les réponses pertinentes

Des propriétaires de petite entreprise	1
Des collègues	2

Des voisin(e)s	3
Des ami(e)s	4
Vos parents	5
Vos enfants	6
Vos grands-parents	7
D'autres membres de votre famille	8
Autre :	77
Je ne sais pas	99

IC5A [1,12]

Avez-vous déjà recherché les types de renseignements suivants sur la cybersécurité?

Veuillez choisir toutes les réponses pertinentes

Façon de déterminer qu'un courriel est une escroquerie	1
Mesures que vous pouvez prendre pour utiliser un réseau sans fil public en toute sécurité	2
Mesures que vous pouvez prendre pour utiliser des sites de médias sociaux en toute sécurité	3
Protection de réseaux et réseaux sans fil à la maison	4
Mesures que vous pouvez prendre pour protéger vos autres dispositifs branchés à Internet (p. ex., télévision intelligente, systèmes de sécurité du domicile, moniteurs d'activité physique, appareils à commande vocale comme Google Home et Amazon Echo)	5
Façon de protéger vos appareils mobiles	6
Conseils en matière de cybersécurité pour les enfants	7
Conseils en matière de cybersécurité pour les aînés	8
Renseignements sur les types de menaces à la cybersécurité (p. ex. courriels d'hameçonnage, logiciels malveillants, etc.)	9
Autre (veuillez préciser) :	77
Rien de ce qui précède	98
Je ne sais pas	99

IC5B [1,14]

1-9,77, IC5A

Où avez-vous trouvé cette information?

Veuillez choisir toutes les réponses pertinentes

Avec un moteur de recherche	1
Sur le site Web d'un fournisseur de logiciels ou de matériel informatique	2
Auprès d'amis ou de membres de la famille	3
Dans les médias	4
Sur le site Web d'un groupe sans but lucratif	5
Dans un bulletin électronique	6
Sur un site web du gouvernement	7
Sur le site Web d'un organisme d'application de la loi	8
Auprès du service informatique de mon employeur	9
Médias sociaux	10
YouTube	11
Autre réponse (veuillez préciser)	77
Je ne me souviens pas	99

IC8B

Quels aspects de cette information étaient utiles?

J'avais confiance dans la source d'information	1
Guide pratique avec des exemples précis et détaillés	2
Elle couvrait exactement les sujets que je voulais connaître	3
Elle était claire et simple (facile à comprendre)	4
Elle était facile à trouver	5
Autre (préciser)	77
Rien	97
Je ne sais pas	99

QA13

Who do you trust

Veuillez indiquer dans quelle mesure vous êtes d'accord ou en désaccord avec les énoncés ci-dessous.

Il appartient aux particuliers de protéger les renseignements personnels les concernant.

Tout à fait en désaccord 1	1
2	2
3	3
Ni l'un ni l'autre 4	4
5	5
6	6
Tout à fait d'accord 7	7
Je ne sais pas	99

QA111B

Who do you trust

Veuillez indiquer dans quelle mesure vous êtes d'accord ou en désaccord avec les énoncés ci-dessous.

J'ai l'impression d'être assez bien renseigné(e) sur les mesures à prendre pour me protéger et pour protéger mes appareils contre les cybermenaces

Tout à fait en désaccord 1	1
2	2
3	3
Ni l'un ni l'autre 4	4
5	5
6	6
Tout à fait d'accord 7	7
Je ne sais pas	99

QA118

Who do you trust

Veuillez indiquer dans quelle mesure vous êtes d'accord ou en désaccord avec les énoncés ci-dessous.

Je suis convaincu de pouvoir me protéger en ligne en autant que je disposerai de renseignements de base et dignes de confiance sur les mesures à prendre.

Tout à fait en désaccord 1	1
2	2
3	3

Ni l'un ni l'autre 4	4
5	5
6	6
Tout à fait d'accord 7	7
Je ne sais pas	99

QA120

Who do you trust

Veuillez indiquer dans quelle mesure vous êtes d'accord ou en désaccord avec les énoncés ci-dessous.

Je suis certain(e) de savoir comment trouver des renseignements pratiques que je peux utiliser pour me protéger en ligne

Tout à fait en désaccord 1	1
2	2
3	3
Ni l'un ni l'autre 4	4
5	5
6	6
Tout à fait d'accord 7	7
Je ne sais pas	99

QA110

Who do you trust

Veuillez indiquer dans quelle mesure vous êtes d'accord ou en désaccord avec les énoncés ci-dessous.

J'estime que les organisations commerciales et autres disposent des mesures de sécurité voulues pour protéger mes renseignements personnels.

Tout à fait en désaccord 1	1
2	2
3	3
Ni l'un ni l'autre 4	4
5	5
6	6
Tout à fait d'accord 7	7
Je ne sais pas	99

BUS1 [1,20]

Responsible, QEMPB; Self-employed, D2

En ce qui concerne votre travail de propriétaire ou gestionnaire d'entreprise, quelles mesures parmi les suivantes votre entreprise a-t-elle prises pour se protéger contre les menaces en ligne?

Veuillez choisir toutes les réponses pertinentes

Garder les logiciels de sécurité à jour sur tous les dispositifs	1
Installer des logiciels de filtrage antipourriel	2
Exiger une protection par mot de passe sur tous les dispositifs	3
Effectuer des copies de sécurité de tous les dispositifs	4
Utiliser un logiciel de cryptage	5
Ne pas utiliser un compte d'administrateur pour accéder au Web	6
Utiliser un mot de passe ou un système d'authentification d'utilisateur pour l'accès sans fil et à distance	7

Suivre des protocoles de suppression d'information lorsque des employés quittent l'organisation	8
9	9
10	10
Rien de ce qui précède	97
Je ne sais pas	98
Je préfère ne pas répondre	99

BUS2 [1,20]

Responsible, QEMPB; Self-employed, D2

Quelles instructions parmi les suivantes fournissez-vous aux employés pour protéger votre organisation contre les cybermenaces et pour protéger vos renseignements personnels?

Veuillez choisir toutes les réponses pertinentes

Utiliser des mots de passe qui contiennent des chiffres et lettres choisis de façon aléatoire et qui sont difficiles à deviner	1
Consulter les politiques en matière de protection de la vie privée sur le site Web	2
Lire les conditions d'utilisation d'un site Web, d'une application ou de la plate-forme d'un média social	3
Changer votre mot de passe par défaut	4
Ne pas donner votre mot de passe sans appeler pour vous assurer que la demande est légitime	5
Télécharger du contenu uniquement à partir de sources fiables	6
Cliquer uniquement sur les pièces jointes ou URL provenant de sources fiables	7
Ne pas permettre au navigateur de mon ordinateur de se rappeler les mots de passe des sites Web	8
Faire preuve de prudence lorsque vous répondez à des demandes d'étrangers	9
Utiliser un logiciel de cryptage	10
Rien de ce qui précède	97
Je ne sais pas	98
Je préfère ne pas répondre	99

BUS3 [1,20]

Responsible, QEMPB; Self-employed, D2

De quels types de renseignements parmi les suivants croyez-vous que votre organisation tirerait profit pour se protéger contre les cybermenaces?

Veuillez choisir toutes les réponses pertinentes

Liste de types de menaces qui existe et signaux à rechercher	1
Conseils pour communiquer aux employés l'importance de suivre de politiques de cybersécurité	2
Pratiques exemplaires pour une politique d'utilisation d'Internet claire	3
Directives pour mettre en place des règles relatives à la politique d'utilisation sécuritaire des courriels	4
Directives sur la façon d'établir une politique solide en matière de médias sociaux	5
Conseils et ressources pour le type de logiciel ou matériel permettant de sécuriser des réseaux	6
Pratiques exemplaires sur la façon pour les employés de gérer les mots de passe	7
Mesures pour protéger les appareils mobiles dans un lieu public	8
Mesures pour gérer les renseignements liés au travail que possèdent les employés qui quittent l'organisation	9
Directives pour réagir à une cyberattaque	10
Pratiques exemplaires sécuritaires en informatique en nuage (avec la définition)	11

Pratiques exemplaires pour l'utilisation de dispositifs de stockage (p. ex., clés USB)	12
Ressources sur la façon de crypter des ordinateurs, portables et dispositifs de stockage	13
Directives sur l'utilisation de dispositifs personnels au travail	14
Autre	77
Rien de ce qui précède	97
Je ne sais pas	98
Je préfère ne pas répondre	99

BUS4 [1,20]

Responsible, QEMPB; Self-employed, D2

Qui est responsable des TI de votre société?

Veuillez choisir toutes les réponses pertinentes

Moi	1
Un autre employé (préciser le rôle au sein de la société) BOXBUS4	2
Un employé de l'organisation qui se consacre au TI	3
Firme de TI en sous-traitance	4
Personne	5
Autre	77
Rien de ce qui précède	97
Je ne sais pas	98
Je préfère ne pas répondre	99

BUS5A1

Responsible, QEMPB; Self-employed, D2

En ce qui concerne les diverses préoccupations liées aux activités quotidiennes de votre organisation, à quel point êtes-vous préoccupé(e) par le fait qu'une cybermenace puisse...

causer des interruptions de travail?

Pas du tout préoccupé(e) 1	1
2	2
3	3
Moyennement préoccupé(e) 4	4
5	5
6	6
Cela vous préoccupe énormément 7	7
Je ne sais pas	98
Je préfère ne pas répondre	99

BUS5A2

Responsible, QEMPB; Self-employed, D2

En ce qui concerne les diverses préoccupations liées aux activités quotidiennes de votre organisation, à quel point êtes-vous préoccupé(e) par le fait qu'une cybermenace puisse...

porter atteinte à la réputation de votre organisation?

Pas du tout préoccupé(e) 1	1
2	2
3	3
Moyennement préoccupé(e) 4	4
5	5
6	6

Cela vous préoccupe énormément 7	7
Je ne sais pas	98
Je préfère ne pas répondre	99

BUS5A3

Responsible, QEMPB; Self-employed, D2

En ce qui concerne les diverses préoccupations liées aux activités quotidiennes de votre organisation, à quel point êtes-vous préoccupé(e) par le fait qu'une cybermenace puisse...

causer des pertes financières?

Pas du tout préoccupé(e) 1	1
2	2
3	3
Moyennement préoccupé(e) 4	4
5	5
6	6
Cela vous préoccupe énormément 7	7
Je ne sais pas	98
Je préfère ne pas répondre	99

BUS5B

Unconcerned, BUS5A

Pourquoi est-ce le cas?

Je n'y ai jamais vraiment pensé	1
J'ignore les enjeux dont je devrais me préoccuper	2
Nous avons fait des recherches à ce sujet et nous avons pris des mesures pour nous protéger	3
Peu de menaces pèsent sur les entreprises comme la nôtre	4
Des problèmes plus importants que les cyberattaques nous préoccupent	5
Vous ne pouvez pas vraiment vous protéger contre les cyberattaques. Si elles doivent se produire, vous ne pouvez pas faire grand-chose	6
Autre	77
Rien de ce qui précède	97
Je ne sais pas	98
Je préfère ne pas répondre	99

Q23

Awareness of GCS

Une campagne de sensibilisation du gouvernement du Canada a été créée pour informer les Canadiens sur la cybersécurité et sur les mesures simples qu'ils peuvent prendre pour se protéger en ligne. Pouvez-vous nommer cette campagne?

Oui :	77
Non	2
Je ne sais pas	98
Pas de réponse	99

GOCAD

Avez-vous vu, lu ou entendu quoi que ce soit du gouvernement du Canada avec le titre « Pensez cybersécurité » qui abordait les menaces en ligne et la façon de vous en protéger?

Oui	1
Non	2
Je ne sais pas	99

GOCADA [1,8]

Yes, GOCAD

Où l'avez-vous vu, lu ou entendu?

J'ai visité le site Web pensezcybersecurite.gc.ca	1
J'en ai entendu parler à une émission de radio ou dans une baladodiffusion	2
Je l'ai vu dans les médias sociaux	3
J'ai vu une vidéo en ligne	4
Quelqu'un m'en a parlé	5
J'ai vu un segment sur les nouvelles ou dans le journal	6
Autre (préciser)	77
Je ne sais pas	99

DEMIN

Les dernières questions que voici sont à votre sujet et les renseignements serviront uniquement à des fins statistiques, pour comprendre les résultats du sondage.

QGENDR

À quel sexe vous identifiez-vous?

Homme	1
Femme	2
Je préfère m'identifier comme (veuillez préciser):	77
Je préfère ne pas répondre	99

D3

Quel est le plus haut niveau de scolarité que vous avez atteint?

École primaire ou moins	1
École secondaire	2
Un peu d'études postsecondaires	3
Collège, école technique ou de métier	4
Programme universitaire de premier cycle	5
Programme universitaire de 2e ou 3e cycles, ou professionnel	6
Je préfère ne pas répondre	99

D6

Laquelle des catégories suivantes décrit le mieux le revenu global de votre ménage, c'est-à-dire, le revenu de toutes les personnes qui composent votre ménage, avant impôts?

Moins de 20 000$	1
De 20 000$ à un peu moins de 40 000$	2
De 40 000$ à un peu moins de 60 000$	3
De 60 000$ à un peu moins de 80 000$	4
De 80 000$ à un peu moins de 100 000$	5

De 100 000$ à un peu moins de 150 000$	6
150 000$ et plus	7
Je préfère ne pas répondre	99

THNKSP

Children under 18, QCHILDA

Merci d'avoir rempli le sondage. Dans le cadre de cette étude, nous aimerions également parler avec des jeunes de 16 à 24 ans. En gage de reconnaissance pour leur temps, tous les participants au sondage âgées de 16 à 24 recevrons un chèque-cadeau de 10 dollars d'Amazon. Accepteriez-vous d'inclure votre fils ou votre fille de 16 à 24 ans à participer à cette étude?

Oui	1
Non	2

THNKSP2

Children under 18, QCHILDA; Yes, THNKSP

Nous aimerions vous envoyer une invitation par courriel à transmettre à votre fils ou votre fille de 16 à 24 ans pour participer à ce sondage. Veuillez nous fournir votre adresse courriel.

Courriel :	1
Réfuse	2

THNK

<THNK: [THNKSP = 1 and QCHILDA = 4,5]We have sent you an invitation to forward to your son or daughter, aged 16-24 to participate in this study. If you have more than son or daughter, aged 16-24 at home, please forward the invitation to the young person aged 16-24 who most recently celebrated a birthday.[ELSE]> Le gouvernement du Canada vous remercie beaucoup, tout comme EKOS, de nous avoir accordé de votre temps.

Le sondage est maintenant terminé. Il a été effectué pour le compte de Sécurité publique Canada. Dans les prochains mois, un rapport renfermant les observations de la présente étude sera disponible auprès de Bibliothèque et Archives Canada. Nous vous sommes très reconnaissants d'avoir pis part à cette étude. Veuillez cliquer sur le bouton « continuer » pour soumettre vos réponses.

THNK2

Screened out

Merci de votre collaboration! D'après les renseignements que vous avez donnés, vous n'êtes malheureusement pas admissible au reste de ce sondage.

B. DÉTAILS MÉTHOLOGIQUES

L'échantillon se compose de 2 710 entretiens réalisés avec des Canadiens âgés de 18 ans ou plus qui utilisent régulièrement Internet, y compris plus de 350 entrevues avec des jeunes âgés de 16 à 24 ans, et 350 Canadiens qui occupent un poste de direction dans une PME comptant entre un et cent employés. Dans un premier temps, l'échantillon réunissait une sélection aléatoire de membres du panel Prob*it* de partout au pays. Les panellistes 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. Il s'agit de la même base de sondage et du même processus d'échantillonnage utilisés pour mener des enquêtes au téléphone, considérés comme représentatifs de la population. Une fois sélectionnées, nous avons communiqué avec eux par téléphone et les avons recrutés en leur demandant de créer un profil de base (c.-à-d. en répondant au questionnaire de base du sondage), qui comprenait un éventail de renseignements démographiques les décrivant. Nous leur demandions également s'ils souhaitaient répondre au sondage au téléphone ou en ligne. Tous les membres de l'échantillon étaient admissibles à une participation, y compris ceux qui ne possèdent qu'un téléphone cellulaire, ceux qui n'ont pas accès à Internet et ceux qui préféraient simplement répondre au téléphone plutôt qu'en ligne. Ce panel se compose d'un échantillon totalement représentatif de la population canadienne à partir duquel il est possible de sélectionner des échantillons aléatoires et de recueillir des données d'une façon plus délibérée et en temps plus opportun que ce qui serait possible dans un sondage téléphonique traditionnel. Ce panel de 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.

En particulier, dans le cadre du sondage, un échantillon de 15 312 personnes a été créé à partir du volet en ligne seulement du panel Prob*it,* en vue de la réalisation des sondages en ligne seulement, étant donné qu'il s'agissait de la portion précise de la population canadienne qui était ciblée par la campagne de communications. Le taux de participation s'est établi à 18 pour cent[3]. L'échantillon du sondage final, en vertu duquel 2 710 sondages ont été achevés, présente un niveau de précision de +/- 1,9 pour cent pour l'échantillon dans son ensemble et de +/- 3 à 6 pour cent pour la plupart des sous-groupes pouvant être isolés dans l'analyse (y compris l'ensemble des régions, des groupes d'âge, des niveaux de scolarité et des niveaux de revenu).

[3] Parmi l'échantillon de 15 312 cas, 179 se sont avérés non distribuables (échantillon valide de 15 133 cas) et 76 cas ont été supprimés parce qu'ils étaient considérés comme hors du domaine.

Le prétest a mené à 14 entretiens en anglais et à 10 en français. Des questions supplémentaires ont été intégrées à la version du prétest du questionnaire pour recueillir les impressions des répondants sur la durée, le rythme, la clarté des libellés et d'autres aspects. Des changements mineurs ont été apportés à la suite des essais, bien que quelques questions aient été enlevées pour réduire la durée du sondage.

Le sondage, qui s'est déroulé entre le 16 et le 29 mars 2020, faisait appel à un questionnaire bilingue hébergé sur un serveur Web sécurisé sous le contrôle des Associés de recherche EKOS. Le courriel d'invitation comprenait une description et une explication de l'objectif du sondage (dans les deux langues), ainsi qu'un lien vers le site du sondage. La base de données du sondage a été mise au point en ayant recours à un numéro d'identification personnel (NIP) de façon à ce que seules les personnes détenant un NIP aient accès au sondage (le NIP était inclus dans le courriel d'invitation). Le questionnaire comprenait une préface qui présentait brièvement l'étude et la raison d'être de la recherche. Le message insistait également sur la nature volontaire et confidentielle du sondage. La collecte des données du sondage s'est faite dans le respect de toutes les normes de l'industrie en vigueur. Tous les membres invités du panel étaient informés de leur droit sous le régime des lois de protection de la vie privée ainsi que de la façon d'obtenir une copie de leurs réponses et des résultats du sondage.

À la suite de la collecte des renseignements, la base de données a fait l'objet d'une analyse dans le but d'en examiner la qualité, les valeurs aberrantes, les exigences en matière de codage, la pondération à la construction de variables indépendantes, ainsi que les tendances des sous-groupes (p. ex. selon l'âge, le sexe, etc.). La pondération de l'échantillon se fondait sur les paramètres de la population selon le plus récent recensement sur l'âge, le sexe, et les régions du pays.

Le tableau suivant présente le profil de l'échantillon. Le tableau comprend la distribution non pondérée de caractéristiques démographiques liées à la région, au genre et à l'âge (utilisées dans la pondération des données), ainsi que la distribution pondérée relativement à la présence d'enfants à la maison, à l'âge des enfants, au niveau de scolarité, et au revenu annuel du ménage.

Tableau 1 : Tableau démographique

Tableau 1a : Province/Territoire (non pondérés)

-	**Total**
n=	*2710*
Colombie-Britannique et Yukon	13%
Alberta et Territoires-du-Nord-Ouest	12%
Saskatchewan et Manitoba	10%
Ontario	34%
Québec et Nunavut	23%
Atlantique	9%

Tableau 1b : Sexe (non pondéré)

-	**Total**
Homme	48 %
Femme	59 %

Tableau 1c : Âge (non pondéré)

-	**Total**
16-24	13%
25-34	12%
35-44	16%
45-54	21%
55-64	19%
65 et +	20%

Tableau 1d : Enfants du ménage âgés de moins de 18 ans

-	**Total**
n=	*2710*
Oui	27%
Non	72%
Je préfère ne pas répondre	1%

Tableau 1e : Âge des enfants à la maison

-	**Total**
n=	*2710*
Moins de 6 ans	31%
6 à 12	48%
13 à 15	32%
16 ans ou plus	39%
Je préfère ne pas répondre	1%

Tableau 1f : Niveau de scolarité atteint

-	**Total**
n=	*2710*
École secondaire ou moins	10%
Un peu d'études postsecondaires	10%
Certificat ou diplôme d'un établissement collégial ou d'une école de métiers	29%
Diplôme d'études de premier cycle	30%
Diplôme d'études supérieures ou professionnel	19%
Je préfère ne pas répondre	1%

Tableau 1g : Revenu annuel du ménage

-	**Total**
n=	*2710*
Moins de 20 000 $	5%
Entre 20 000 $ et 39 999 $	10%
Entre 40 000 $ et 59 999 $	12%
Entre 60 000 $ et 79 999 $	14%
Entre 80 000 $ et 99 999 $	13%
Entre 100 000 $ et 149 999 $	18%
150 000 $ ou plus.	14%
Je ne sais pas/Pas de réponse	14%

La comparaison de chaque échantillon non pondéré avec les données du recensement de 2016 de Statistique Canada laisse entrevoir des sources semblables de biais systématique dans chaque sondage, conformément au modèle qui se dégage de la plupart des sondages à l'intention du grand public. Les membres des échantillons des sondages sont un peu plus scolarisés que ce que l'on retrouve dans l'ensemble de la population puisque 49 pour cent disent avoir un diplôme universitaire contre 25 pour cent dans la population générale. Les ménages comprenant des enfants de moins de 18 ans sont également sous-représentés dans chaque échantillon (26 p. cent, comparativement à 35 p. cent dans la population). Comme décrit précédemment, chaque échantillon a été pondéré en fonction de l'âge, du sexe et de la région.