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

Numéro d'enregistrement : ROP 070-21

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

This report is also available in English

Canada

Sondage de suivi sur la connaissance de la campagne Pensez cybersécurité

Rapport final

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

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

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

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

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

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

TABLES DES MATIÈRES

Liste des tableaux 4
Liste des graphiques 4
Sommaire 6

A. Contexte et objectifs 6
B. Méthodologie 6
C. Principales constatations 7
D. Note aux lecteurs 11
E. Certification de neutralité politique 12

Résultats détaillés 13

A. Niveau de préoccupation/Probabilité des menaces 13
B. Connaissance 17
C. Mesures de précaution – Comportements 24
D. Information 34
E. Expérience d'entreprises 44

Annexes 55

A. Détails méthodologiques 55
B. Questionnaire 60

LISTE DES TABLEAUX

Tableau 1 : État de préparation
Tableau 2 : Authentification à facteurs multiples
Tableau 3 : Protection du réseau sans fil
Tableau 4 : Renseignements utiles pour les petites et moyennes entreprises
Tableau 5 : Tableau démographique

LISTE DES GRAPHIQUES

Graphique 1 : Probabilité des menaces
Graphique 2 : Raison de l'improbabilité d'être touché
Graphique 3 : Nature de la préoccupation
Graphique 4 : Mesures pour s'assurer qu'un site Web est sécurisé
Graphique 5 : Fréquence de la victimisation
Graphique 6 : Mesures de protection prises par les victimes d'une cyberattaque
Graphique 7 : Mesures prises pour protéger des comptes en ligne
Graphique 8 : Mesures prises concernant les mots de passe
Graphique 9 : Fréquence des mises à jour du système d'exploitation
Graphique 10 : Stockage d'information
Graphique 11 : Fréquence de l'utilisation de dispositifs de sauvegarde
Graphique 12 : Types de risques pris
Graphique 13 : Signes d'hameçonnage
Graphique 14 : Type d'information recherché
Graphique 15 : Sources d'information
Graphique 16 : Raisons pour lesquelles les renseignements sont utiles
Graphique 17 : Type ou méthode d'information privilégiée
Graphique 18 : Attitudes envers l'information
Graphique 19 : Connaissance de la campagne Pensez cybersécurité
Graphique 20 : Raison pour la Connaissance de la campagne Pensez cybersécurité
Graphique 21 : Responsabilité pour les TI
Graphique 22 : Niveau de préoccupation
Graphique 23 : Raison du manque de préoccupation
Graphique 24 : Mesures prises pour prévenir les attaques ou s'en protéger
Graphique 25 : Instructions aux employés
Graphique 26 : Récupérer d'une attaque d'un rançongiciel

Graphique 27 : Employés travaillant du domicile
Graphique 28 : Protection des employés à domicile contre les cybermenaces

SOMMAIRE

A. CONTEXTE ET OBJECTIFS

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

Voici les objectifs de ce projet de recherche :

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

B. MÉTHODOLOGIE

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

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

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

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

C. PRINCIPALES CONSTATATIONS

Niveau de préoccupation

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

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

Connaissance

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

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

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

Mesures de précaution

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

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

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

Information

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

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

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

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

Expérience d'entreprises

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

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

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

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

D. NOTE AUX LECTEURS

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

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

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

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

E. CERTIFICATION DE NEUTRALITÉ POLITIQUE

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

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

Signé par : 

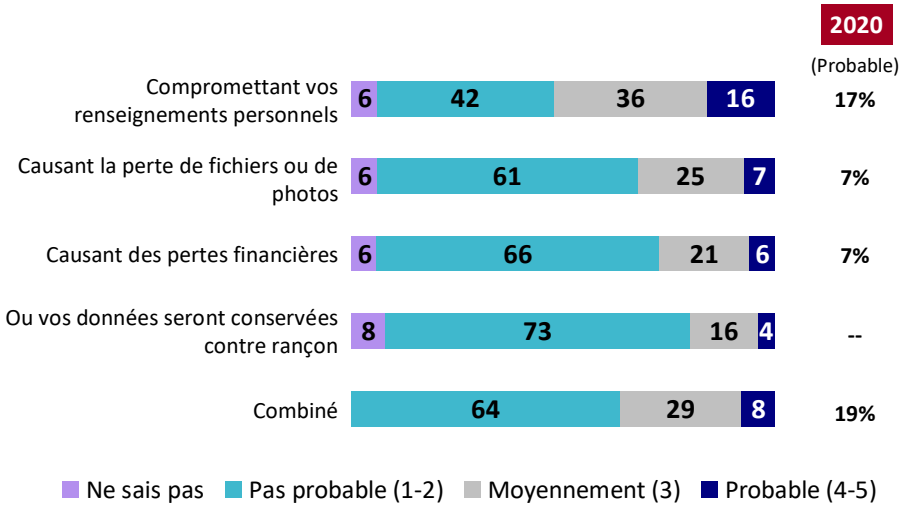
Susan Galley (Vice-présidente)

RÉSULTATS DÉTAILLÉS

A. NIVEAU DE PRÉOCCUPATION/PROBABILITÉ DES MENACES

Plus d'un répondant sur dix (16 %) croit qu'il est probable qu'il soit touché par une cybermenace susceptible de compromettre ses renseignements personnels au cours de la prochaine année, alors que deux personnes sur cinq (42 %) considèrent cela comme peu probable. La plupart des Canadiens croient que les cybermenaces ne les toucheront pas, et moins d'une personne sur dix est d'avis qu'elle sera confrontée à une menace qui entraînera la perte de fichiers ou de photos (7 %), des pertes financières (6 %), ou encore la possibilité que des données de son entreprise soient conservées en vue d'obtenir une rançon (4 %). De façon générale, en combinant les quatre domaines, moins d'un répondant sur dix (8 %) croit qu'il est probable qu'il soit la victime d'une cybermenace au cours de la prochaine année, en grande partie en raison de la probabilité plus élevée que des renseignements personnels soient compromis. Les résultats sont très semblables à ceux de 2020. Cependant, il s'agit de la première année où la menace de données détenues contre une rançon est évaluée.

Graphique 1 : Probabilité des menaces



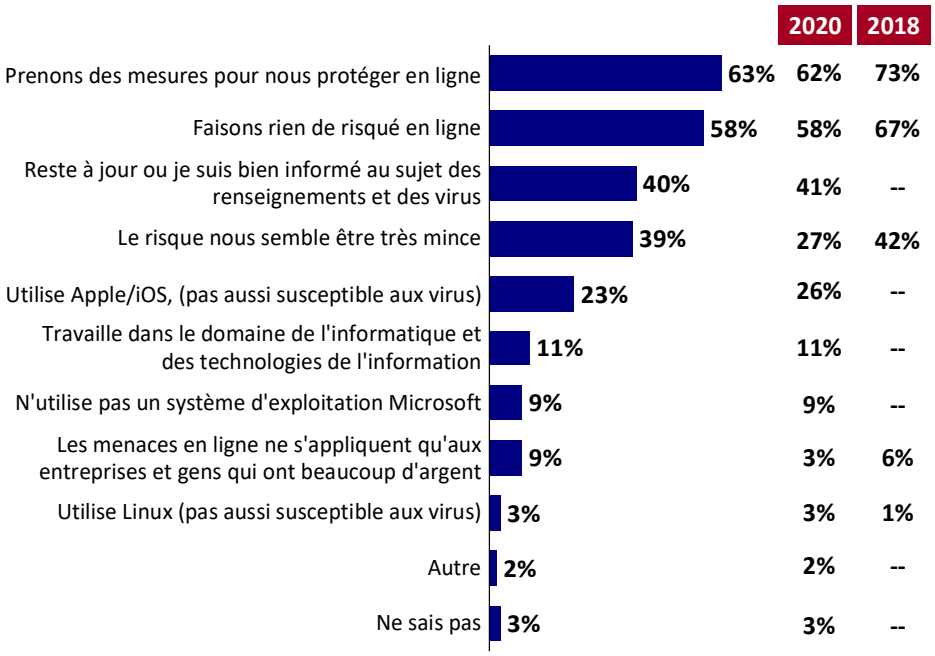
Q11abc. Au cours de la prochaine année, à quel point avez-vous l'impression qu'il est probable que vous soyez victime d'une cybermenace...?
Base : n=2050

- Les jeunes répondants, tout comme les hommes, sont plus susceptibles de dire qu'il est peu probable que l'un des quatre événements évalués se produise.
- Ceux qui ont des revenus annuels plus élevés (plus de 150 000 dollars) sont plus enclins à dire qu'il est peu probable qu'ils soient victimes d'une cybermenace causant la perte de fichiers ou de photos, des pertes financières, ou de données détenues contre une rançon.
- Les résidents du Québec ont plus tendance que les répondants des autres régions à croire qu'ils seront victimes d'une cybermenace causant des pertes financières.

La plupart des répondants qui n'ont pas de craintes affirment que c'est parce qu'ils prennent des mesures pour se protéger en ligne (63 %) ou parce qu'ils ne font rien de risqué en ligne (58 %). Deux répondants sur cinq croient qu'il est peu probable qu'ils soient victimes d'une cybermenace parce qu'ils restent informés au sujet des virus (40 %), ou ils estiment que le risque leur semble très mince (39 %). Environ une personne sur quatre croit qu'il est peu probable qu'elle soit victime d'une cybermenace parce qu'elle utilise Apple/iOS, qui n'est pas aussi susceptible aux virus (23 %).

La plupart des résultats sont semblables à ceux obtenus dans les éditions des années précédentes, à l'exception de la proportion de gens qui estiment que le risque est très mince, qui était en baisse en 2020 (27 %), mais qui est revenue à un niveau semblable à celui de 2018.

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



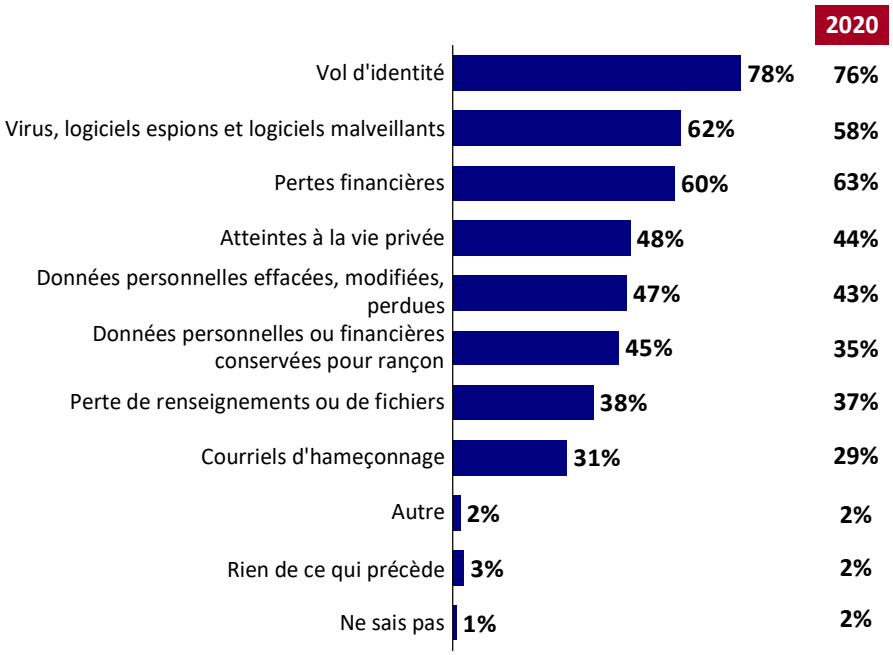
QK8a. Pourquoi ne croyez-vous pas qu'il est probable que vous soyez victime d'une cybermenace?
Base : =1694 (indique une probabilité d'être victime d'une cybermenace); 2020 : n=1941 (indique improbable d'être affecté par une perte financière ou de fichiers, ou avoir ses données personnelles compromises); 2018 : n=492 (indique improbable d'être affecté par des menaces en ligne (en général)

- Les hommes et les personnes ayant un niveau de scolarité plus élevé ont plus tendance à dire qu'ils prennent des mesures pour se protéger.
- Les Canadiens âgés de 25 à 34 ans sont plus enclins à dire qu'il est peu probable qu'ils soient victimes d'une cybermenace parce qu'ils restent à jour ou qu'ils y travaillent dans le domaine des TI.
- Ceux dont le niveau de scolarité ou le revenu est moins élevé sont plus susceptibles de dire que les cybermenaces ne s'appliquent qu'aux entreprises et aux gens qui ont beaucoup d'argent. Ceux dont le revenu annuel est plus élevé (80 000 dollars et plus) sont plus susceptibles que ceux qui ont un revenu moins élevé de déclarer qu'il est peu probable qu'ils soient victimes d'une cybermenace parce qu'ils prennent des mesures pour se protéger en ligne ou parce qu'ils restent à jour.

Le vol d'identité préoccupe plus de trois Canadiens sur quatre (78 %). En ce qui concerne les cybermenaces, les Canadiens sont également préoccupés par les virus, par les logiciels espions ou par les logiciels malveillants en général (62 %) ainsi que par les pertes financières (60 %). Environ deux personnes sur cinq se disent préoccupées par une possible atteinte à leur vie privée (48 %), par la possibilité que leurs données personnelles soient effacées, modifiées ou perdues (47 %), par la possibilité que leurs données personnelles soient conservées pour obtenir une rançon (45 %) ou par la perte potentielle de renseignements ou de fichiers (38 %). Les courriels d'hameçonnage préoccupent trois Canadiens sur dix (31 %).

La plupart des préoccupations sont signalées dans une proportion un peu plus élevée qu'en 2020, l'augmentation la plus notable figurant dans la catégorie de la possibilité que leurs données personnelles ou financières soient conservées pour obtenir une rançon (45 %, contre 35 % en 2020).

Graphique 3 : Nature de la préoccupation



Q15. Quels types de cybermenaces vous préoccupent le plus?
Base : n=2050; 2020 : n=2710

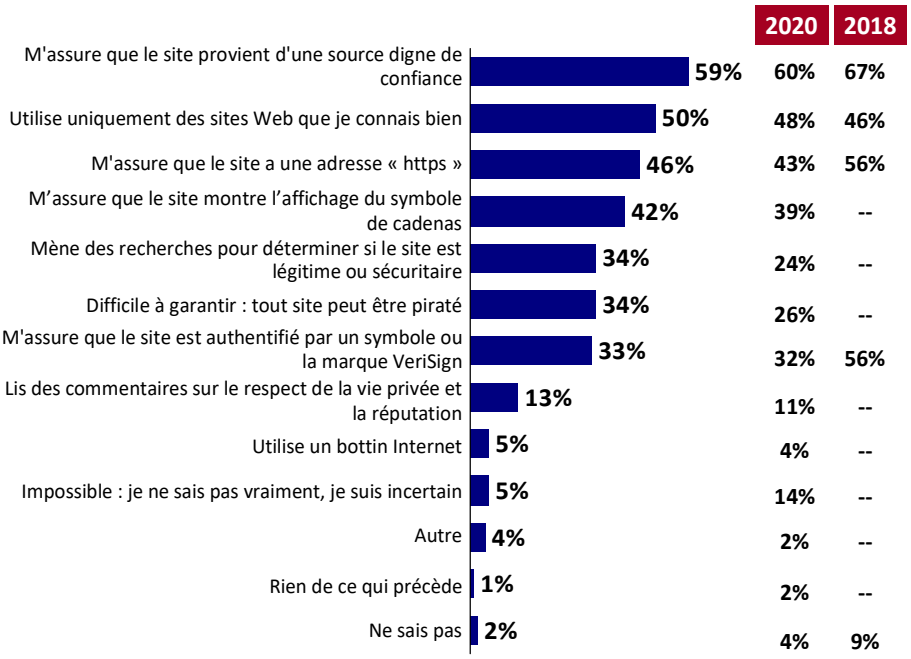
- Les courriels d'hameçonnage et les virus préoccupent davantage les personnes âgées de 55 ans et plus que les Canadiens plus jeunes.
- Le vol d'identité est une préoccupation plus répandue chez les personnes âgées de 45 à 54 ans que dans les autres groupes d'âge.
- Les pertes financières, l'atteinte à la vie privée et les rançongiciels sont plus susceptibles de préoccuper les Canadiens âgés de 25 à 34 ans que les autres groupes d'âge.
- Le vol d'identité, les renseignements personnels détenus pour obtenir une rançon et la perte de renseignements ou de fichiers sont plus souvent des préoccupations chez les personnes ayant le plus haut niveau de scolarité (université) que chez les autres Canadiens.

B. CONNAISSANCE

Trois Canadiens sur cinq (59 %) disent rechercher des sites Web d'une source fiable, comme ceux de fournisseurs de logiciels connus ou des sites Web de gouvernements. La moitié des répondants (50 %) déclare n'utiliser que des sites Web qu'ils connaissent, tandis qu'une moindre proportion (46 %) recherche spécifiquement des adresses « https » pour s'assurer qu'un site Web est sécurisé. Plus de deux personnes sur cinq s'assurent que les sites Web qu'elles visitent affichent le symbole du cadenas (42 %). Environ un répondant sur trois mène des recherches afin de déterminer si un site est légitime ou sécuritaire (34 %) ou s'assure que le site est authentifié par un symbole ou la marque VeriSign (33 %), ou croit qu'il est généralement difficile de garantir la sécurité et que n'importe quel site peut être piraté (33 %). Plus d'une personne sur dix affirme lire des commentaires sur le respect de la vie privée ou sur la réputation d'un site Web (13 %).

Même si la question était différente dans le sondage de 2018 (Comment peut-on savoir si un site Web est sécurisé?), les résultats présentent une certaine ressemblance avec les autres éditions du sondage. Cependant, plus de répondants disent effectuer des recherches ou croient qu'il est difficile d'avoir la garantie qu'un site ne peut être piraté en 2022 qu'en 2020.

Graphique 4 : Mesures pour s’assurer qu’un site Web est sécurisé



QK11a. Quelles mesures prenez-vous pour vous assurer qu’un site Web est sécurisé?

Base : n=2050; 2020 : n=2710; 2018 – Comment peut-on savoir si un site Web est sécurisé? 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 celles qui ont fait des études universitaires.
- Les résidents du Québec sont plus susceptibles de chercher un site Web avec une adresse « https », alors que ceux de l’Ontario sont plus enclins que les répondants des autres régions à dire qu’ils recherchent le symbole du cadenas.

Seul un Canadien sur cinq (22 %) se sent prêt à faire face aux cybermenaces. Plus d'une personne sur quatre (28 %) affirme ne pas être préparée, et 43 pour cent se disent un peu préparés. Parmi ceux qui ne sont pas préparés, 41 pour cent sont d'avis que c'est parce qu'il est impossible de toujours se protéger en ligne. Trois personnes sur dix (35 %) ont des copies de sécurité et pourraient se remettre d'une cybermenace. Environ une personne sur cinq cite une autre raison, notamment un manque d'information sur les mesures à prendre (26 %), l'impression qu'il est peu probable que cela se produise (26 %), le manque de temps pour se préparer (20 %), le manque de connaissances sur les différents types de menaces (19 %), ou le fait que les renseignements qu'ils trouvent ne sont pas assez simples pour être utiles (18 %). Une plus grande proportion de Canadiens ne croit pas qu'elle sera victime d'une cybermenace en 2022 (26 %) qu'en 2020 (18 %).

Tableau 1 : État de préparation

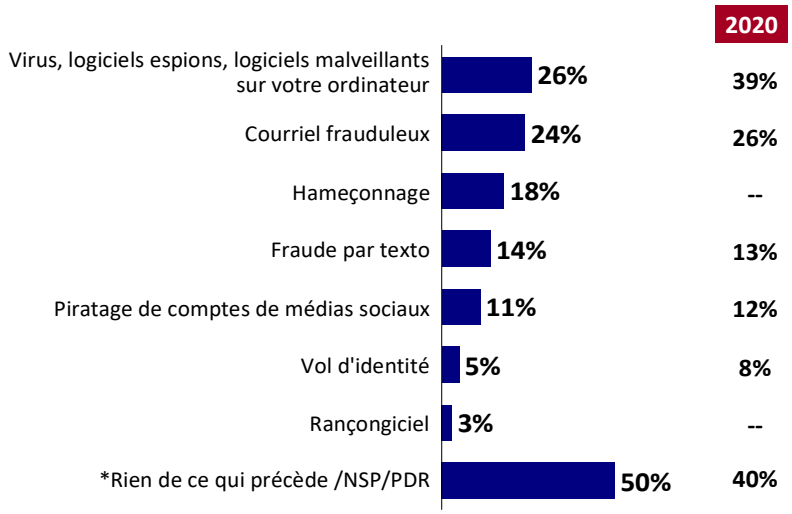
--	**Total 2022**	**Total 2020**
Q16. Êtes-vous bien préparé(e) pour faire face aux cybermenaces?	*n=2050*	*n=2710*
Pas préparé(e) (1-2)	28 %	27 %
Préparé(e) (3)	43 %	45 %
Bien préparé(e) (4-5)	22 %	19 %
Je ne sais pas	7 %	8 %
Q17. Pourquoi donc?	*n=1453*	*n=1959*
Vous ne pouvez jamais vraiment vous protéger en ligne	41 %	44 %
J'ai une copie sauvegardée et je peux m'en remettre	35 %	31 %
Je ne sais pas où obtenir des renseignements sur les mesures à prendre	26 %	23 %
Je ne pense pas qu'il est probable que cela m'arrive	26 %	18 %
Je n'ai pas le temps ou je ne me penche jamais sur ce problème	20 %	18 %
Je ne connais pas les différents types de menaces	19 %	22 %
Les renseignements que je trouve ne sont pas assez simples pour m'aider	18 %	18 %
Il est inutile d'essayer de se protéger	3 %	4 %
Rien	2 %	2 %
Autre	2 %	3 %
Je ne sais pas	4 %	6 %

- Bien qu'il n'y ait pas de proportions importantes de certains segments qui se sentent bien préparées pour faire face à une cybermenace, les résidents du Québec, les femmes et les personnes qui n'ont fait que des études secondaires ont plus tendance que la moyenne à dire qu'ils ne sont pas préparés pour y faire face.
- Les personnes âgées de 34 ans et moins ont plus tendance que les répondants des autres groupes d'âge à citer l'improbabilité d'une cyberattaque et le manque de temps. Les Canadiens âgés (65 ans et plus) ont plus tendance à dire qu'ils ne savent pas où trouver de l'information ou que l'information qu'ils trouvent n'est pas assez simple pour leur être utile.
- Les hommes sont plus susceptibles de dire qu'ils ne pensent pas que cela leur arrivera, ou qu'ils ont une copie de sécurité et qu'ils pourraient se remettre d'une cyberattaque. Les femmes ont tendance à dire qu'elles ne savent pas où obtenir de l'information, que l'information n'est pas simple ou qu'elles ne connaissent pas les différents types de menaces.

Un Canadien sur quatre dit avoir été victime d'un virus, d'un logiciel espion ou d'un logiciel malveillant sur son ordinateur, alors que plus du quart a été victime d'une fraude par courriel. Parmi les autres cyberattaques figurent l'hameçonnage (18 %), les fraudes par texto (14 %) et le piratage d'un compte d'un média social (11 %). Peu de répondants ont été victimes d'un vol d'identité (5 %) ou d'un rançongiciel (3 %). La moitié des répondants affirment n'avoir pas été victimes de cyberattaques (43 %), ne pas être sûrs (5 %) ou ne pas vouloir répondre (2 %).

Moins de Canadiens qu'en 2020 disent avoir été victimes d'un virus, d'un logiciel espion ou d'un logiciel malveillant (26 % par rapport à 39 % il y a deux ans). Nouveau en 2022, l'hameçonnage s'ajoute aux options présentées aux répondants, tout comme « Aucune de ces réponses », ce qui permet de séparer les personnes qui ne savent de celles qui ne veulent pas répondre.

Graphique 5 : Fréquence de la victimisation



* « Rien de ce qui précède » a été rajouté en 2022

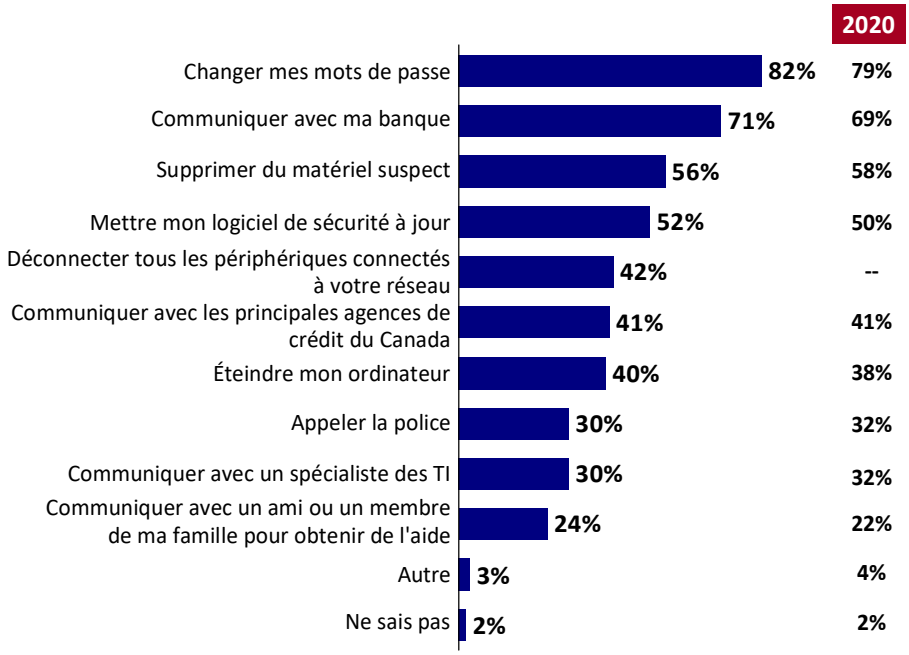
Q18. Avez-vous déjà été victime de l'une des cyberattaques suivantes?
Base : n=2050; 2020 : n=2710

- Comparativement aux autres groupes d'âge, les personnes âgées de 55 ans et plus sont plus susceptibles d'avoir été victimes d'un courriel frauduleux.
- Les résidents du Manitoba et du Québec sont plus susceptibles d'avoir été victimes d'un courriel frauduleux ou d'une fraude par texto que les autres Canadiens.
- L'incidence du piratage de comptes des médias sociaux est plus élevée chez les moins de 25 ans.
- Les virus, les logiciels espions et les logiciels malveillants sont plus susceptibles de constituer un enjeu en Alberta qu'ailleurs au Canada, ainsi que chez les hommes.
- Les gens de la catégorie de revenu la plus élevée (150 000 dollars et plus) ont plus tendance à affirmer qu'ils n'ont pas été victimes de l'une ou l'autre des cyberattaques mentionnées.

S'ils savaient ou soupçonnaient qu'ils ont été victimes d'une cyberattaque, la plupart des Canadiens (82 %) affirment qu'ils changeraient leurs mots de passe. Plus de deux personnes sur trois (71 %) agiraient de façon proactive en communiquant avec leur banque. Plus de la moitié supprimerait du matériel suspect (56 %) ou mettrait son logiciel de sécurité à jour (52 %). Les autres mesures prévues sont la déconnexion de tous les périphériques connectés à leur réseau (42 %), 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 (40 %). Trois personnes sur dix communiqueraient avec un spécialiste des TI (30 %) ou appelleraient la police (30 %). Un peu moins d'une personne sur quatre (24 %) demanderait l'aide d'un ami ou d'un membre de sa famille.

Les résultats sont très semblables à ceux obtenus en 2020. Toutefois, la déconnexion de tous les périphériques connectés au réseau était une nouvelle mesure en 2022.

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



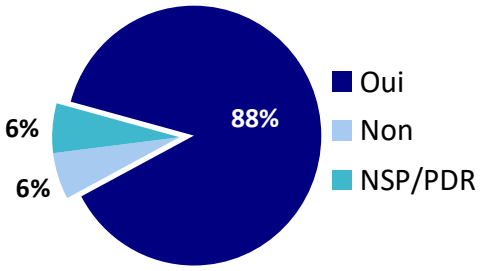
Q19. Si vous saviez ou soupçonniez avoir été victime d'une cyberattaque, quelles mesures prendriez-vous pour vous protéger?
Base : n=2050; 2020 : n=2710

- Les Canadiens âgés de 25 à 44 ans sont plus susceptibles de dire qu'ils changeraient leurs mots de passe, ou encore qu'ils communiqueraient avec leur banque ou avec les principales agences de crédit du Canada. Les Canadiens âgés de 55 ans et plus ont tendance à dire qu'ils éteindraient leur ordinateur ou qu'ils communiqueraient avec un spécialiste des TI.
- À l'échelle régionale, les résidents de l'Ontario ont plus tendance à dire qu'ils éteindraient leur ordinateur ou qu'ils supprimeraient du contenu suspect. Les Québécois sont plus susceptibles de dire qu'ils communiqueraient avec des agences de crédit.
- Les femmes sont plus susceptibles que les hommes de demander de l'aide de l'extérieur, ou encore de communiquer avec un spécialiste des TI, avec un ami ou un membre de sa famille, ou avec la police.
- Les répondants qui ont un niveau de scolarité supérieur sont plus enclins à mentionner la plupart des mesures évaluées. Ceux dont le revenu annuel est plus élevé (80 000 dollars ou plus) sont plus susceptibles de dire qu'ils changeraient leurs mots de passe, ou encore qu'ils communiqueraient avec leur banque ou avec les principales agences de crédit du Canada.

C. MESURES DE PRÉCAUTION – COMPORTEMENTS

Près de neuf Canadiens sur dix (88 %, en harmonie avec les résultats obtenus en 2018 et en 2020) disent prendre des mesures 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



	2020	2018
Oui	88%	89%
Non	6%	5%
NSP/PDR	6%	5%

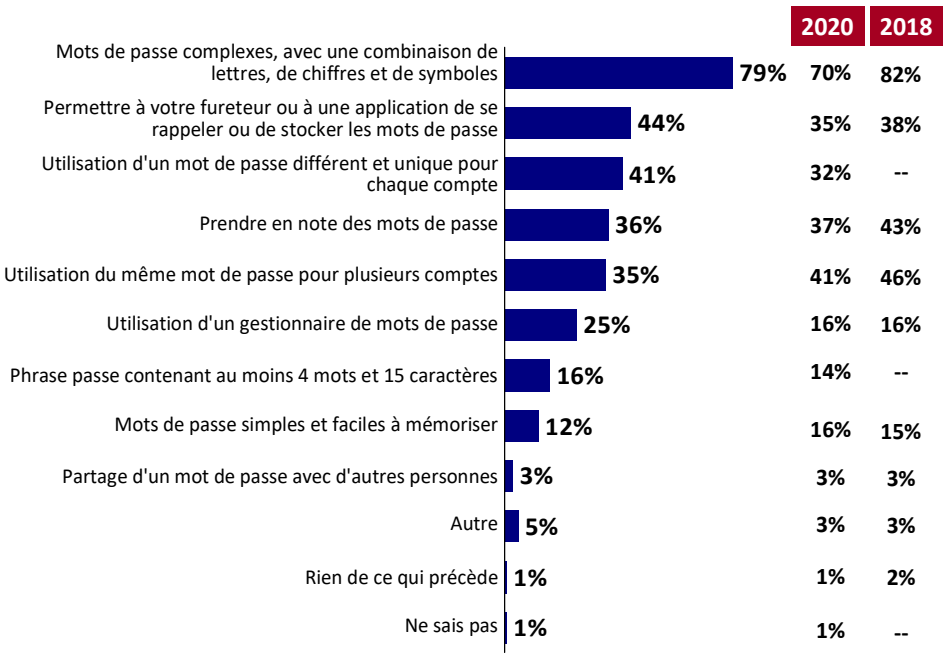
Q1. Prenez-vous des précautions pour protéger vos comptes en ligne, vos comptes de médias sociaux, vos appareils et vos réseaux?
Base : n=2050; 2020 : n=2710; 2018 : n=2072

- Bien que la proportion soit élevée dans l'ensemble de l'échantillon, les hommes sont plus susceptibles de déclarer prendre des mesures de précaution, tout comme les répondants dont le niveau de scolarité et le revenu sont élevés.
- À l'échelle régionale, les répondants de l'Alberta sont les moins susceptibles de prendre des mesures de précaution.

En ce qui concerne les mots de passe, la plupart des Canadiens (79 %) disent essayer d'utiliser des mots de passe complexes, avec une combinaison de lettres, de chiffres et de symboles. Deux personnes sur cinq permettent à leur fureteur ou à une application de se rappeler ou de stocker des mots de passe (44 %), ou utilisent un mot de passe différent et unique pour chaque compte (41 %). Environ un répondant sur trois prend en note ses mots de passe (36 %) ou utilise le même mot de passe pour plusieurs comptes (35 %). Une personne sur quatre utilise un gestionnaire de mots de passe (25 %), et un moins grand nombre utilise une phrase comportant au moins quatre mots et quinze caractères (16 %) ou a recours à des mots de passe simples et faciles à mémoriser (12 %).

Plus de Canadiens permettent à leur fureteur ou à une application de se rappeler ou de stocker des mots de passe (en hausse par rapport aux 35 % de 2020 et aux 38 % de 2018), utilisent un mot de passe différent et unique pour chaque compte (en hausse par rapport à 32 %) ou ont recours à un gestionnaire de mots de passe (en hausse par rapport à 16 %).

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=2050; 2020 : n=2710; 2018 : n=2072

- Les Canadiens âgés de moins de 45 ans sont plus susceptibles d'utiliser le même mot de passe pour plusieurs comptes, d'utiliser un gestionnaire de mots de passe ou de permettre au fureteur ou à une application de stocker leurs mots de passe. Les personnes âgées de 55 ans et plus sont plus enclines à prendre en note leurs mots de passe.
- Les résidents de l'Ontario ont plus tendance que les autres Canadiens à permettre à leur fureteur ou à une application de stocker des mots de passe ou d'utiliser le même mot de passe pour plusieurs comptes. Ceux de la Colombie-Britannique tendent davantage à utiliser un mot de passe différent et unique pour chaque compte.
- Les gens qui ont un diplôme universitaire et un revenu plus élevé sont plus susceptibles de mentionner la plupart des mesures. Cependant, ceux dont le revenu est inférieur sont plus susceptibles de dire qu'ils prennent en note leurs mots de passe.

Un peu plus de deux personnes sur trois (69 %) utilisent une authentification à facteurs multiples. Pour ce faire, ils ont le plus souvent recours à un code reçu par texto (87 %). Trois répondants sur cinq utilisent des mots de passe (62), un code reçu par courriel (66 %) ou des NIP (60 %). Près de la moitié utilisent des empreintes digitales (49 %) ou un code reçu par une application d'authentification (47 %). Trois personnes sur dix utilisent un code reçu par appel téléphonique (32 %) ou la reconnaissance faciale (32 %). Moins d'une personne sur cinq utilise des phrases passe (17 %) ou des périphériques jetons (14 %). Un moins grand nombre utilise la reconnaissance vocale (9 %), des cartes à puce (5 %) ou une clé USB (4 %).

L'utilisation de l'authentification à facteurs multiples a changé depuis 2020, les Canadiens utilisant davantage de codes reçus par texto, des applications d'authentification et la reconnaissance faciale, et ayant moins souvent recours aux empreintes digitales.

Tableau 2 : Authentification à facteurs multiples

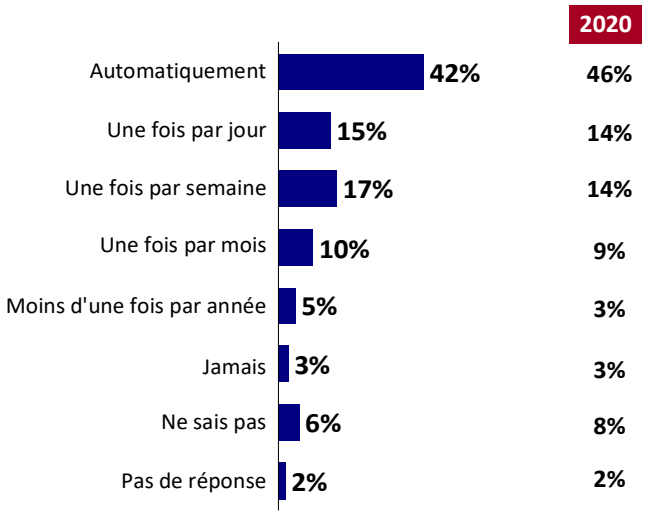
--	**Total 2022**	**Total 2020**
Q6. Utilisez-vous une authentification à facteurs multiples?	*n=2050*	*n=2710*
Oui	69 %	53 %
Non	17 %	31 %
Je ne sais pas	12 %	14 %
Pas de réponse	2 %	2 %
Q7. Lesquels des facteurs d'authentification suivants avez-vous utilisés?	*n=1423*	*n=1423*
Code reçu par texto	87 %	79 %
Code reçu par courriel	66 %	64 %
Mots de passe	62 %	65 %
NIP	60 %	63 %
Empreintes digitales	49 %	57 %
Code reçu par une application d'authentification	47 %	41 %
Code reçu par appel téléphonique	32 %	29 %
Reconnaissance faciale	32 %	23 %
Phrases passe	17 %	20 %
Périphériques jetons	14 %	14 %
Reconnaissance vocale	9 %	9 %
Cartes à puce	5 %	7 %
Clés USB	4 %	4 %

--	Total 2022	Total 2020
Autre	2 %	2 %
Je ne sais pas	0 %	1 %
Pas de réponse	0 %	1 %

- Les Canadiens âgés de 25 à 44 ans, ainsi que les hommes, les gens qui ont une formation universitaire et les gens dont le revenu est plus élevé, sont plus susceptibles d'utiliser l'authentification à facteurs multiples. À l'échelle régionale, les résidents de l'Alberta, de la Colombie-Britannique, des Territoires et de l'Ontario sont les plus susceptibles d'utiliser l'authentification, tandis que ceux du Québec sont moins enclins à le faire.
- Les jeunes Canadiens (moins de 35 ans) sont plus susceptibles d'utiliser un code reçu par courriel, par texto ou par une application d'authentification.
- Les hommes ont plus tendance que les femmes à utiliser un code reçu par une application d'authentification ou des périphériques jetons. Les femmes ont plus tendance que les hommes à avoir recours à la reconnaissance vocale.
- Les Canadiens ayant fait des études universitaires et dont le revenu est plus élevé sont plus susceptibles d'utiliser un code reçu par texto, une application d'authentification ou des périphériques jetons. Les personnes ayant un niveau d'études supérieur ont également plus tendance à dire qu'elles utilisent des phrases passe. Les parents, ainsi que les gens qui ont un revenu plus élevé, sont plus enclins à utiliser la reconnaissance faciale ou les empreintes digitales.

Pour près de la moitié des répondants (42 %), 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 (15 %), d'une semaine (17 %), d'un mois (10 %) ou d'un an (5 %). Une faible proportion (3 %) affirme ne jamais activer les mises à jour. Les résultats ne varient pas beaucoup par rapport à 2020.

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=2050; 2020 : n=2710

- Les répondants âgés de 35 ans ou plus ont plus tendance que les autres groupes d'âge à se fier aux mises à jour automatiques de leur système d'exploitation. Les jeunes Canadiens sont plus susceptibles de faire des mises à jour chaque semaine.
- Les résidents du Québec sont plus enclins à avoir recours aux mises à jour automatiques. Ceux de la Saskatchewan ont tendance à dire qu'ils effectuent des mises à jour quotidiennement.
- Les Canadiens ayant des études universitaires et un revenu plus élevé sont plus susceptibles d'effectuer des mises à jour hebdomadaires.

Neuf Canadiens sur dix (90 %) protègent le réseau sans fil de leur maison avec un mot de passe unique, bien que 29 pour cent utilise le mot de passe par défaut. Sept personnes sur dix (68 %) créent le mot de passe. Seulement 17 pour cent ont un réseau d'invités avec un mot de passe distinct. Les résultats obtenus ressemblent à ceux obtenus en 2020.

Tableau 3 : Protection du réseau sans fil

--	**Total 2022**	**Total 2020**	**Total 2018**
QB2B. Protégez-vous le réseau sans fil de votre maison avec un mot de passe unique?	*n=2050*	*n=2710*	*n=2072*
Oui	92 %	90 %	96 %
Non	3 %	4 %	3 %
Je n'ai pas un réseau sans fil à la maison	2 %	3 %	--
Je ne sais pas	1 %	2 %	1 %
Pas de réponse	1 %	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=1889*	*n=2430*	
Oui, mot de passe par défaut	25 %	29 %	
Non, je l'ai créé moi-même	72 %	68 %	
Je ne sais pas	2 %	2 %	
Pas de réponse	2 %	1 %	
Q10. Utilisez-vous un réseau pour invités avec un mot de passe distinct pour vos appareils intelligents et pour les visiteurs?	*n=2050*	*n=2710*	
Oui	17 %	17 %	
Non	78 %	77 %	
Je ne sais pas	3 %	4 %	
Pas de réponse	3 %	3 %	

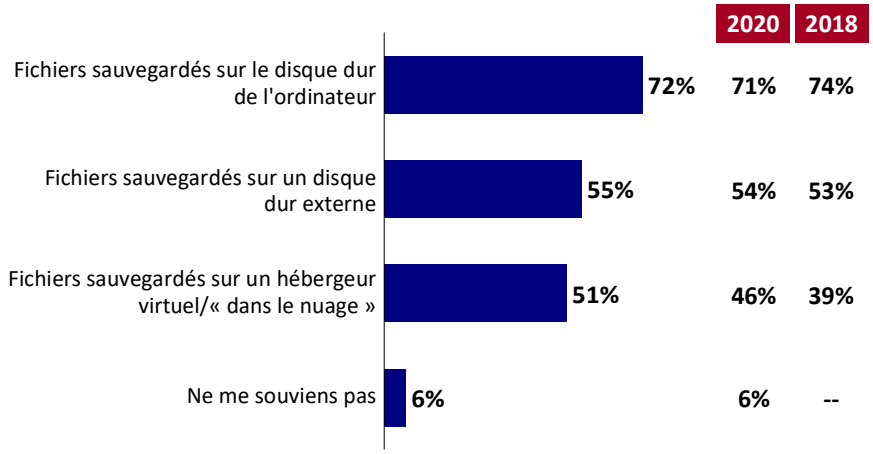
- Bien que presque tous les répondants protègent le réseau sans fil de leur maison, cette tendance est plus répandue chez les Canadiens âgés de moins de 45 ans, ainsi que chez les parents et les personnes ayant un niveau d'études supérieur et un revenu annuel supérieur. Les personnes âgées de 65 ans et plus sont plus susceptibles de dire qu'elles ne protègent pas le réseau sans fil de leur maison ou qu'elles n'ont pas de réseau sans fil.
- Le mot de passe par défaut est utilisé un peu plus souvent par les gens âgés de 55 à 64 ans que par les autres groupes d'âge. Cette pratique est aussi plus fréquente au Manitoba que

dans d'autres régions pour les gens qui ont un revenu plus bas, tout comme chez les femmes, comparativement aux hommes.

- Bien que relativement peu de gens utilisent un mot de passe distinct pour les invités, cette pratique est un peu plus courante chez les 35 à 54 ans et chez les parents.

Près de trois Canadiens sur quatre (72 %) sauvegardent leurs fichiers sur le disque dur de l'ordinateur. Plus de la moitié stockent leurs données sur un disque dur externe (55 %) ou ont recours à un serveur virtuel ou à un service infonuagique (51 %). Les résultats étaient très semblables en 2020 et en 2018, bien que la proportion de Canadiens ayant recours à un nuage informatique augmente de façon constante depuis 2018.

Graphique 10 : Stockage d'information

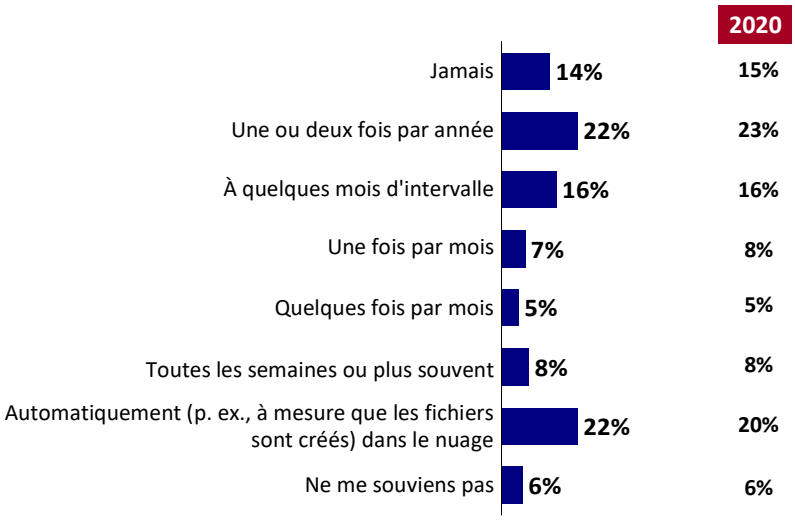


QD1B. En ce qui concerne le stockage de l'information à des fins personnelles, est-ce que vous sauvegardez vos données sur le disque dur de votre ordinateur, sur un disque dur externe (stockage supplémentaire/d'appoint) ou sur un hébergeur virtuel (c.-à-d. de l'informatique en nuage).
Base : n=2050; 2020 : n=2710; 2018 : n=2072

- Le niveau de scolarité, l'âge, le revenu et le genre constituent de fortes variables qui expliquent le recours à l'une ou l'autre des options de stockage de l'information signalées ci-dessus. Les Canadiens âgés de 44 ans ou moins sont plus susceptibles que leurs homologues plus âgés d'utiliser un service infonuagique, tout comme les parents d'enfants âgés de 6 à 12 ans. 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 susceptibles de mentionner toutes les options de stockage de données.

Une personne sur cinq (22 %) sauvegarde automatiquement ses données et ses fichiers personnels sur un nuage informatique à partir d'un ordinateur, d'un téléphone intelligent ou de tout autre appareil mobile. Une proportion semblable (22 %) sauvegarde manuellement ses fichiers une ou deux fois par année, alors que moins de répondants sauvegardent leurs fichiers quelques fois par année (16 %), une fois par mois (7 %), quelques fois par mois (16 %), ou une fois par semaine ou plus souvent (8 %). Certains Canadiens (15 %) ne sauvegardent jamais leurs fichiers. Ces résultats sont en harmonie avec ceux obtenus en 2020.

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



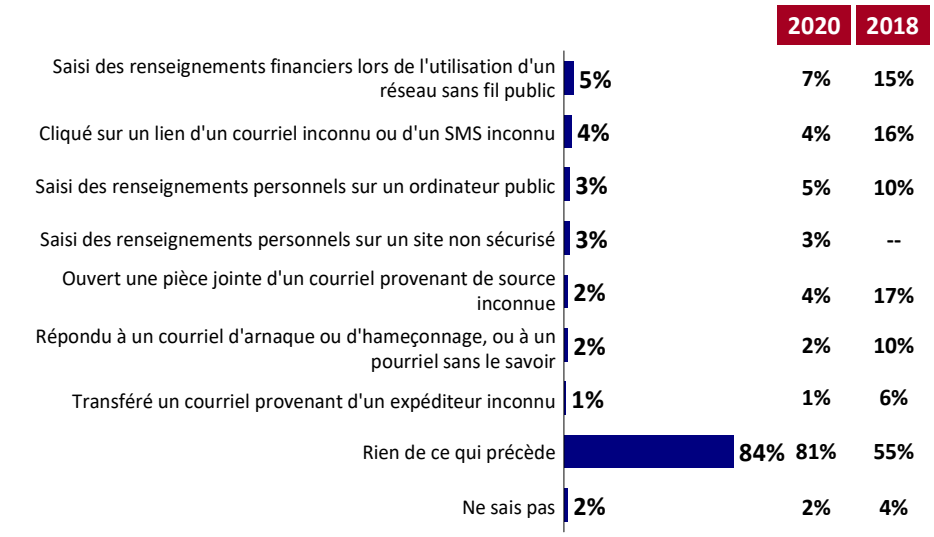
QB5X. À quelle fréquence sauvegardez-vous des données ou des fichiers personnels stockés sur votre ordinateur, sur votre téléphone intelligent ou sur un autre appareil mobile?
Base : n=2050; 2020 : n=2710; 2018 : n=1880

- Les Canadiens âgés de moins de 45 ans, ainsi que les parents et les gens dont le revenu annuel du ménage est d'au moins 80 000 dollars sont plus susceptibles de dire qu'ils sauvegardent automatiquement leurs fichiers sur un nuage informatique. Les personnes âgées de 65 ans et plus sont susceptibles de ne jamais sauvegarder leurs fichiers. Ceux qui n'ont fait que des études secondaires ou dont le niveau de scolarité est inférieur ont aussi plus tendance à dire qu'ils ne sauvegardent jamais leurs fichiers.

Au cours du dernier mois, huit Canadiens sur dix (84 %) déclarent ne pas s'être comportés d'une façon pouvant menacer leur cybersécurité. Moins d'un répondant sur dix a saisi des renseignements financiers lors de l'utilisation d'un réseau sans fil public (5 %), a cliqué sur le lien d'un courriel ou d'un SMS inconnu (4 %), a saisi des renseignements personnels sur un ordinateur public (3 %), a saisi des renseignements personnels sur un site non sécurisé (3 %), a ouvert une pièce jointe d'un courriel provenant de source inconnue (2 %), a répondu à un courriel d'arnaque ou d'hameçonnage, ou à un pourriel sans le savoir (2 %) ou a transféré un courriel provenant d'un expéditeur inconnu (1 %).

Les résultats ne varient pas beaucoup par rapport à 2020. Une question semblable était posée en 2018, même elle cherchait à savoir si cela s'était « déjà » produit, plutôt que de faire allusion au dernier mois. Bien que la question ne soit pas tout à fait comparable, elle donne une idée de la fréquence des comportements dans certains domaines (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'une source inconnue). L'utilisation d'un réseau sans fil public et de renseignements personnels sur un appareil public a encore lieu assez souvent, même sur une période d'un mois.

Graphique 12 : Types de risques pris



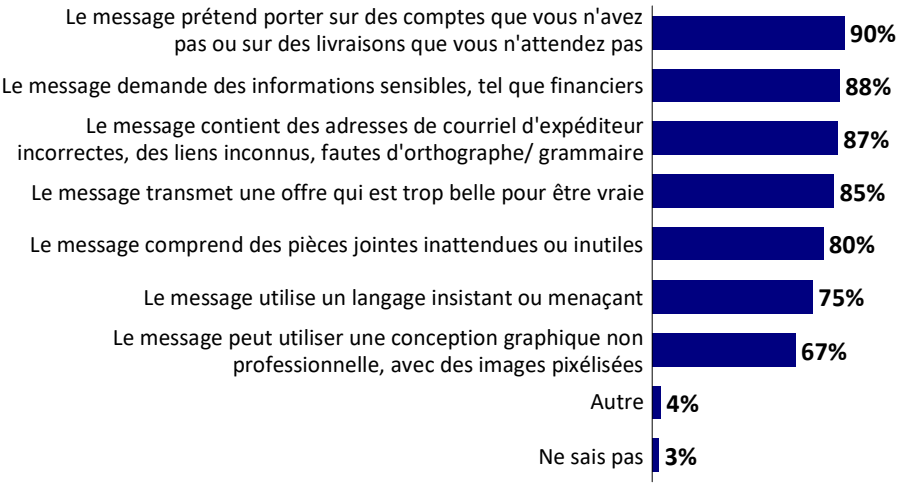
Question posée en 2018 : À votre connaissance, avez-vous déjà fait l'une de ces choses?

QB11. Au cours du dernier mois, avez-vous…?
Base : n=2050; 2020 : n=2710; 2018 : n=2072

- Les personnes âgées de moins de 25 ans sont plus susceptibles que les répondants des autres groupes d'âge d'avoir saisi des renseignements personnels sur un ordinateur public ou d'avoir saisi des renseignements financiers lors de l'utilisation d'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.

Les résultats du sondage donnent à penser que les gens reconnaissent généralement le plus souvent les signes d'un courriel d'hameçonnage, notamment les demandes suspectes (90 %), les demandes de renseignements financiers ou d'autres informations sensibles (88 %), les messages contenant des adresses de courriel incorrectes ou des liens inconnus (87 %), ou les offres qui sont trop belles pour être vraies (85 %). Huit personnes sur dix reconnaissent également que les messages comportant des pièces jointes suspectes ou l'utilisation d'un langage insistant ou menaçant (75 %) sont des signes de tentatives d'hameçonnage. L'utilisation d'une conception graphique non professionnelle constitue un autre signe relevé par deux répondants sur trois.

Graphique 13 : Signes d'hameçonnage



Q11b. D'après ce que vous savez, quels sont les signes d'une tentative d'hameçonnage?
Base : n=2135

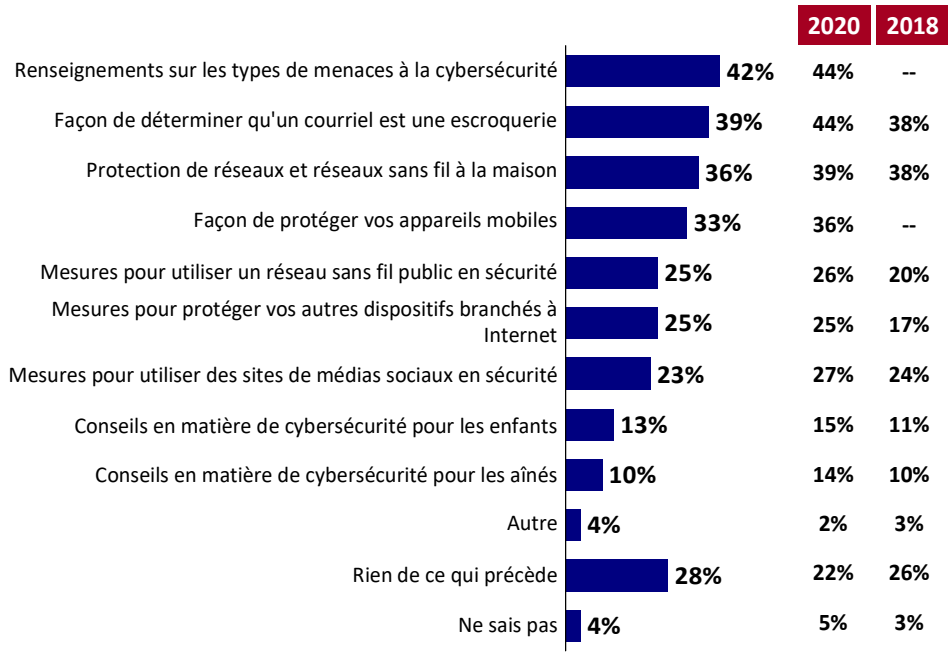
- Les personnes âgées de 25 à 45 ans sont généralement plus susceptibles de reconnaître les signes d'hameçonnage, alors que c'est moins souvent le cas chez les 65 ans ou plus. C'est également le cas des personnes n'ayant fait que des études secondaires par rapport à celles ayant fait des études postsecondaires, en particulier celles possédant un niveau d'éducation universitaire. Cette tendance se répète dans le modèle basé sur le revenu du ménage.

D. INFORMATION

Deux Canadiens sur cinq recherchent des renseignements sur les types de cybermenaces (42 %) ou de l'information sur la façon de savoir si un courriel est une escroquerie (39 %). Environ le tiers des répondants recherche des renseignements sur la protection de réseaux sans fil à la maison (36 %) ou sur la façon de protéger des appareils mobiles (33 %). Une personne sur quatre cherche à obtenir des informations sur les mesures à prendre pour utiliser un réseau sans fil public en toute sécurité (25 %), pour protéger d'autres dispositifs branchés à Internet, comme des téléviseurs intelligents, des systèmes de sécurité à domicile, des moniteurs de conditionnement physique et des appareils à commande vocale (25 %), ou pour utiliser des sites de médias sociaux en toute sécurité (23 %). Environ une personne sur dix cherche à obtenir des conseils en matière de cybersécurité pour les enfants (13 %) ou pour les aînés (10 %). Une personne sur quatre (28 %) ne recherche jamais de renseignements sur la cybersécurité.

Les résultats sont semblables à ceux obtenus en 2020, une proportion légèrement inférieure de répondants ayant recherché des renseignements sur la façon de déterminer qu'un courriel est une escroquerie, et un plus grand nombre affirmant n'avoir pas recherché d'information. Bien qu'ils reflètent les réponses à une question quelque peu différente, les résultats de 2020 suggèrent que plusieurs recherches sont plus fréquentes qu'en 2018 (façon de reconnaître une fraude par courriel, d'utiliser en toute sécurité un réseau sans fil public ou de protéger d'autres appareils connectés à Internet).

Graphique 14 : 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=2050; 2020 : n=2710; 2018 : n=2072

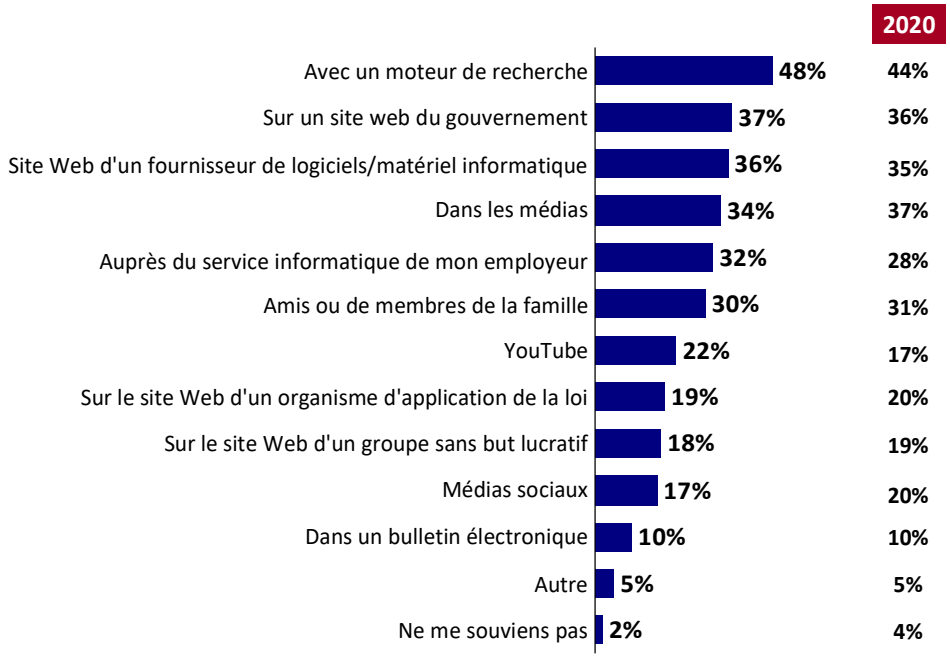
- Les jeunes Canadiens (moins de 35 ans) sont plus susceptibles de rechercher des renseignements sur les mesures à prendre pour utiliser un réseau sans fil public en toute sécurité. Les répondants âgés de 25 à 34 ans sont plus enclins à chercher à obtenir des renseignements sur les mesures à prendre pour utiliser des sites de médias sociaux en toute sécurité, pour protéger d'autres dispositifs branchés à Internet, pour protéger des appareils mobiles ou pour avoir des renseignements sur les types de menaces à la cybersécurité. Les Canadiens âgés de 65 ans ou plus ont plus tendance à rechercher des conseils en matière de cybersécurité pour les aînés. En comparaison, ceux âgés de 45 à 54 ans sont plus susceptibles de rechercher de l'information sur la protection de réseaux sans fil à la maison, alors que ceux âgés de 35 à 44 ans sont plus enclins à vouloir des conseils en matière de cybersécurité pour les enfants.
- Les parents sont plus susceptibles que les répondants qui n'ont pas d'enfants de moins de 18 ans à la maison de rechercher des conseils en matière de cybersécurité pour les enfants.
- Les hommes, ainsi que les répondants dont le niveau de scolarité ou le revenu du ménage sont plus élevés, sont plus enclins à rechercher de l'information dans la plupart des domaines que les femmes et que les gens dont le niveau de scolarité ou le revenu du ménage sont plus bas. Les Canadiens qui ont fait des études secondaires ou collégiales sont

plus susceptibles que ceux qui ont fait des études universitaires d'affirmer ne pas vouloir obtenir de renseignements.

- Les résidents de la Colombie-Britannique et des Territoires sont plus enclins que ceux des autres régions à rechercher des mesures pour utiliser un réseau sans fil public en toute sécurité.

Quarante-huit pour cent des Canadiens cherchent à obtenir de l'information sur la cybersécurité à l'aide d'un moteur de recherche. Environ trois personnes sur dix trouvent de l'information sur un site Web du gouvernement (37 %), sur le site Web d'un fournisseur de logiciels ou de matériel informatique (36 %), dans les médias, y compris sur le site Web d'un organisme de presse (34 %), dans le service des TI de leur employeur (32 %) ou par le biais d'amis et de membres de leur famille (30 %). Une personne sur cinq mentionne comme source YouTube (22 %), un site Web traitant d'application de la loi (19 %), un site Web d'un organisme sans but lucratif (19 %) ou un média social (17 %). Dix pour cent trouvent de l'information dans un bulletin. Les résultats ne varient pas beaucoup par rapport à 2020.

Graphique 15 : Sources d'information

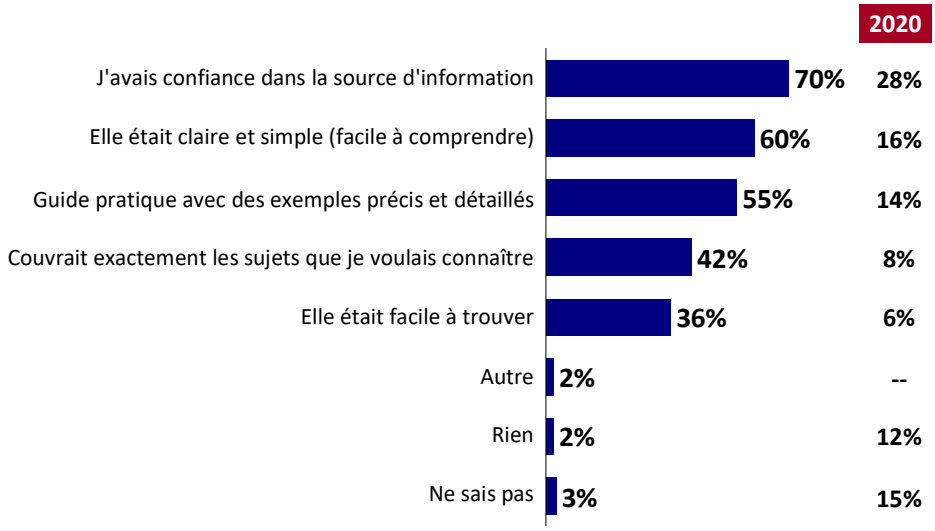


QIC5b. Où êtes-vous allé chercher cette information?
Base : n=1394); 2020 : n=1977 (toute personne recherchant de l'information sur l'un des sujets énumérés dans le tableau 13)

- Les personnes âgées de moins de 25 ans sont plus susceptibles que les répondants 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, ainsi que les répondants dont le niveau de scolarité et le niveau de revenu sont plus élevés, sont plus susceptibles que leurs homologues de dire qu'elles cherchent à obtenir de l'information auprès du service des TI de leur employeur. Les Canadiens plus âgés (55 ans et plus) sont plus susceptibles de rechercher de l'information auprès de leurs amis, de membres de leur famille ou d'un bulletin. Les personnes âgées 65 et plus ont plus tendance que les répondants plus jeunes à rechercher des renseignements sur le site Web d'un fournisseur ou d'un organisme de presse.
- 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 vendeur, du site Web d'un organisme sans but lucratif ou d'un bulletin électronique.
- Les résidents de l'Ontario, tout comme les Canadiens dont le revenu est plus bas, sont plus susceptibles que ceux des autres régions d'utiliser YouTube.

Sept répondants sur dix (70 %) considèrent l'information comme utile parce qu'ils se fient à la source d'information. Plus de la moitié d'entre eux affirme que l'information est utile en raison de sa clarté et de sa simplicité (60 %) ou parce qu'elle offre un guide pratique avec des exemples précis et détaillés (55 %). Environ deux personnes sur cinq font confiance à l'information parce qu'elle couvre exactement les sujets de leur recherche (42 %) ou parce qu'elle est facile à trouver (36 %). Il était possible de choisir plusieurs réponses à cette question, alors que ce n'était pas le cas en 2020, ce qui rend les comparaisons difficiles. Toutefois, il convient de souligner que l'ordre d'importance de ces réponses est le même que celui obtenu en 2020.

Graphique 16 : Raisons pour lesquelles les renseignements sont utiles

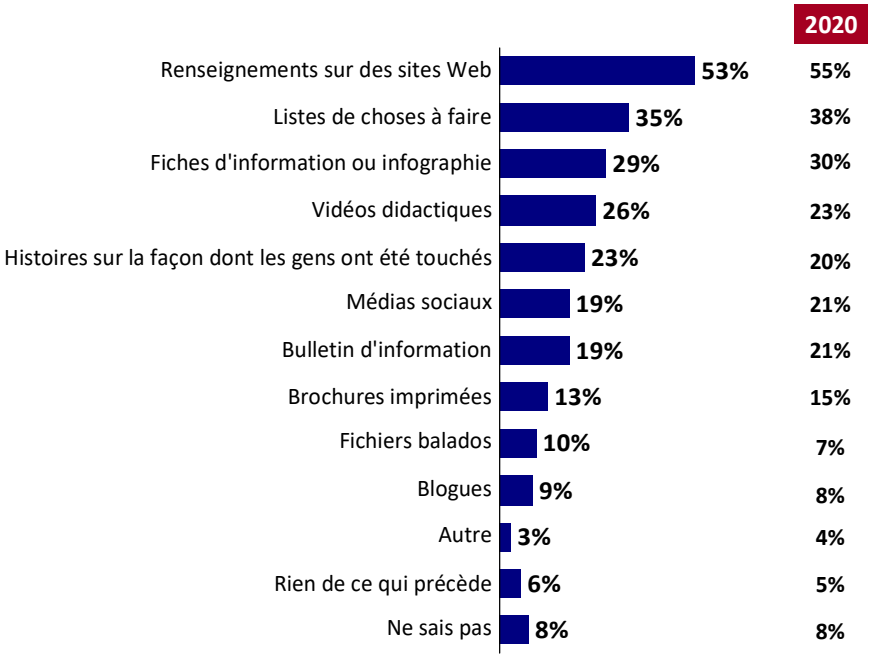


QIC8b. Quels aspects de cette information étaient utiles?
Base : n=1394; 2020 : n=1977 (toute personne recherchant de l'information sur l'un des sujets énumérés dans le tableau 13)

- Les Canadiens plus jeunes sont plus susceptibles que ceux âgés de 25 ans ou plus de dire que l'information était facile à trouver (ce groupe est plus enclin à recourir aux médias sociaux ou à YouTube).
- Les parents de jeunes enfants (6 à 12 ans) sont moins susceptibles de mentionner l'une ou l'autre des raisons.
- Les gens qui ont fait des études universitaires ou qui ont un revenu plus élevé sont plus susceptibles que les personnes ayant un niveau de scolarité inférieur et de moindres revenus de dire qu'ils se fient à la source d'information. Ceux dont le revenu est plus élevé sont également plus enclins à déclarer que l'information leur semblait utile parce qu'il s'agissait d'un guide pratique.

Plus de la moitié (53 %) des Canadiens préfèrent obtenir de l'information sur la protection contre les cybermenaces par le biais de sites Web. Trois personnes sur dix préfèrent des listes de choses à faire (35 %), ou encore des fiches d'information et des infographies (29 %). Un répondant sur quatre dit préférer des vidéos didactiques (26 %) ou des histoires sur la façon dont les gens ont été touchés (23 %). Un sur cinq mentionne des médias sociaux (19 %) ou des bulletins d'information, comme des abonnements par courriel (19 %). Un moins grand nombre mentionne des brochures imprimées (13 %), des balados (10 %) ou des blogues (9 %) comme un moyen privilégié pour obtenir de l'information. Les résultats ne varient pas beaucoup par rapport à 2020.

Graphique 17 : Type ou méthode d'information privilégiée



Q20. Comment préférez-vous obtenir de l'information pour vous protéger contre les cybermenaces?
Base : n=2050; 2020 : n=2651

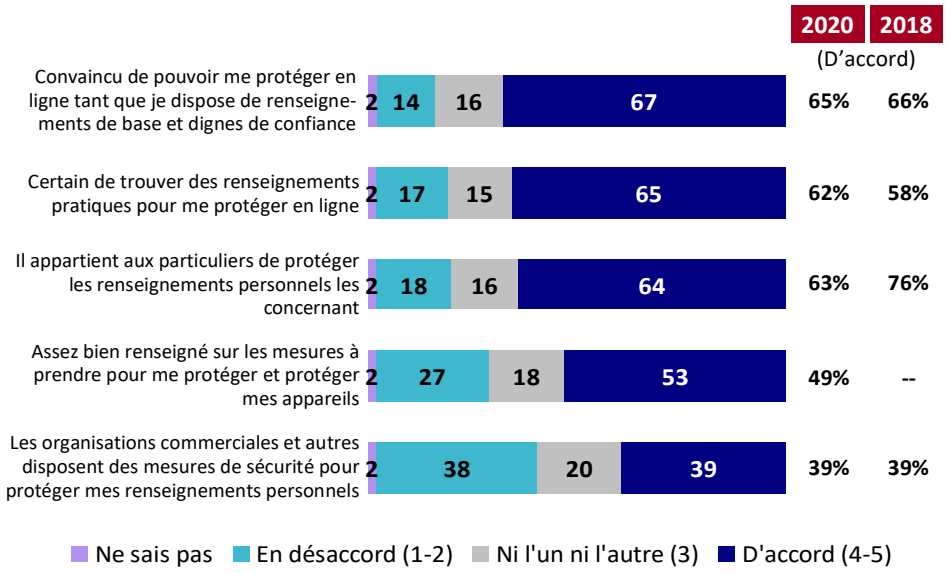
- Les Canadiens plus jeunes (moins de 25 ans) sont plus susceptibles que les répondants des autres groupes d'âge de préférer les vidéos didactiques ou les médias sociaux. Les Canadiens plus âgés (55 ans et plus) ont plus tendance que les plus jeunes à préférer les listes de choses à faire, les brochures imprimées ou les bulletins d'information.
- Les personnes âgées de 25 à 34 ans sont plus susceptibles de préférer les balados ou les blogues, alors que celles âgées de 35 à 44 ans ont plus tendance à mentionner des fiches d'information ou des infographies.

- Les résidents du Manitoba sont plus susceptibles de préférer les brochures imprimées, tandis que ceux du Québec mentionnent davantage les listes de choses à faire et les bulletins d'information.
- Les hommes sont plus susceptibles que les femmes de préférer obtenir des renseignements sur des sites Web et des blogues. Les femmes préfèrent les listes de choses à faire ou les fiches d'information.
- Les gens qui ont fait des études universitaires sont plus enclins à privilégier les sites Web, les listes de choses à faire ou les fiches d'information. Ceux de la catégorie de revenu la plus élevée (150 000 dollars et plus) sont plus susceptibles de préférer les fiches d'information ou les formations en milieu de travail. Les Canadiens à faible revenu ont plus tendance à préférer les brochures imprimées.

Les deux tiers des Canadiens (65 %) sont convaincus de pouvoir se protéger en ligne tant qu'ils disposent de renseignements de base et dignes de confiance sur les mesures à prendre. Une moindre proportion de répondants est certaine de trouver des renseignements pratiques pour se protéger en ligne (65 %) ou convient qu'il appartient aux individus de protéger les renseignements personnels les concernant (64 %). Cependant, seule la moitié (53 %) estime en savoir assez sur les mesures à prendre pour se protéger contre les cybermenaces. Deux personnes sur cinq (39 %) croient que les entreprises et d'autres organisations prennent des mesures de sécurité adéquates pour protéger leurs renseignements personnels.

Les résultats sont semblables à ceux obtenus en 2020. Toutefois, par rapport à 2018, plus de Canadiens sont convaincus de pouvoir trouver des renseignements pratiques (65 %, alors que cette proportion était de 58 % en 2018) et sont moins enclins à convenir qu'il appartient aux individus de protéger les renseignements personnels les concernant (64 % par rapport aux 76 % enregistrés en 2018).

Graphique 18 : Attitudes envers l'information

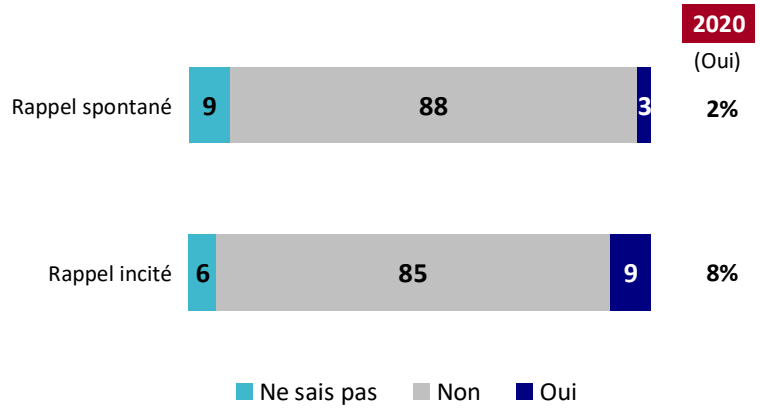


QA13, A11B, A118, Q120, A110. Veuillez indiquer dans quelle mesure vous êtes d'accord ou en désaccord avec les énoncés ci-dessous.
Base : n=2050; 2020 : n=2710; 2018 : n=2072

- Les Canadiens qui ont fait des études universitaires sont moins susceptibles de convenir qu'il est de la responsabilité des gens de protéger leurs renseignements personnels. Les répondants de la catégorie de revenu la plus élevée (150 000 dollars et plus) ont plus tendance à croire qu'ils sont assez bien renseignés sur les mesures à prendre pour se protéger et pour protéger leurs appareils, ou à être certains de pouvoir trouver des renseignements pratiques pour se protéger en ligne.
- Les Canadiens âgés de 18 à 54 ans sont plus susceptibles de convenir qu'ils ont assez d'information sur les mesures à prendre pour se protéger contre les cybermenaces, tandis que ceux âgés de 55 ans et plus ont plus tendance à ne pas être d'accord. Les jeunes Canadiens (moins de 35 ans) sont plus enclins à croire en leur capacité à se protéger en ligne tant qu'ils disposent d'informations de base et dignes de confiance ou à croire savoir où trouver des renseignements pratiques.
- Les hommes sont plus susceptibles que les femmes d'être certains de trouver des renseignements pratiques pour se protéger en ligne.

Très peu de répondants (3 %, une proportion semblable aux 2 % enregistrés en 2020) sont en mesure de nommer la 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 %) dit connaître la campagne Pensez cybersécurité du gouvernement du Canada une fois que celle-ci est nommée.

Graphique 19 : Connaissance de la campagne Pensez cybersécurité



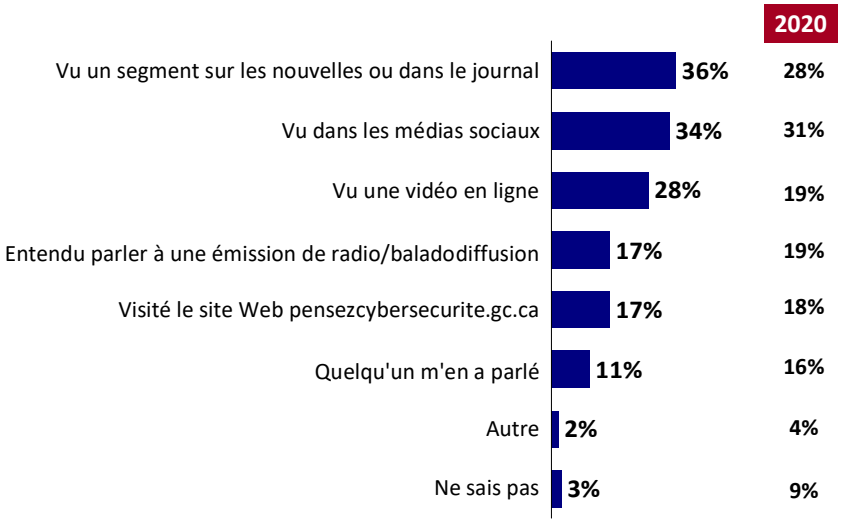
Q23. Une campagne de sensibilisation du gouvernement du Canada a été créée pour informer les Canadiens sur la cybersécurité et sur les mesures simples qu'ils peuvent prendre pour se protéger en ligne. Pouvez-vous nommer cette campagne?
Base : n=2050; 2020 : n=2683

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=2050; 2020 : n=2683

- Lorsqu'on nomme la campagne, les jeunes Canadiens (moins de 25 ans) sont plus susceptibles que ceux âgés de plus de 25 ans de dire qu'ils ont entendu parler de la campagne Pensez cybersécurité.

Parmi les personnes qui affirment connaître la campagne Pensez cybersécurité, 36 % ont vu quelque chose dans les journaux ou aux nouvelles et 34 % ont lu des informations sur la campagne dans les médias sociaux. Un peu plus d'un répondant sur quatre (28 %) a vu une vidéo en ligne. Moins d'une personne sur cinq en a entendu parler à une émission de radio ou dans un balado (17 %), sur le site Web pensezcybersécurité.ca (17 %) ou par le biais d'une connaissance (16 %). Une plus grande proportion de Canadiens qu'en 2020 qui connaissent la campagne déclare avoir vu quelque chose aux nouvelles ou dans les journaux, ou encore dans une vidéo en ligne, ou disent que quelqu'un leur en a parlé.

Graphique 20 : Raison pour la Connaissance de la campagne Pensez cybersécurité



QGOCADA. Où l'avez-vous vu, lu ou entendu?
Base : n=180; 2020 : n=210

E. EXPÉRIENCE D'ENTREPRISES

Plus d'un propriétaire ou gestionnaire d'entreprise sur trois (35 %) est responsable des TI au sein de leur société. Trois de ces répondants sur dix (30 %) confient cet aspect de l'exploitation de leur entreprise à une société spécialisée en TI. Un sur quatre (24 %) mentionne un employé de l'organisation qui se consacre aux TI et 15 % indiquent qu'un employé non spécialisé en est responsable. Six pour cent n'ont aucun responsable des TI.

Une grande proportion des propriétaires et gestionnaires indique confier cet aspect de l'exploitation de leur entreprise à une société spécialisée en TI (30 %), ce qui est supérieur aux résultats obtenus en 2020 (14 %) et en 2019 (19 %). Il y a également une augmentation apparente du nombre de propriétaires ou de gestionnaires d'entreprise qui mentionne que cette responsabilité est confiée à un autre employé (qui ne se consacre pas aux TI), ce qui constitue une hausse d'environ 10 % par rapport aux 4 % enregistrés en 2020 et aux 5 % obtenus en 2018.

Graphique 21 : Responsabilité pour les services des TI

QBUS4. Qui est responsable des TI de votre société?
Base : n=301; 2020 : n=356; 2018 : n=533

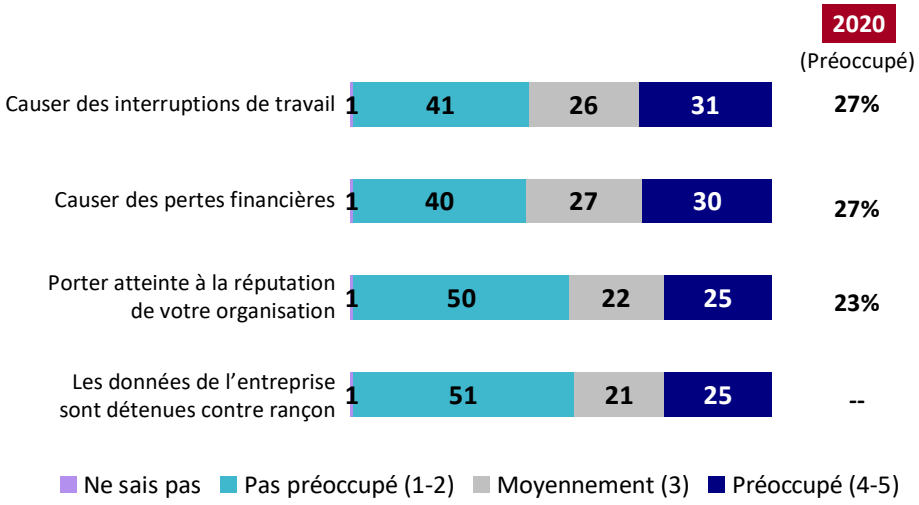
- Les petites entreprises de dix employés ou moins déclarent plus souvent s'occuper des TI que celles qui ont plus d'employés. Les représentants des plus grandes organisations (onze employés et plus) sont beaucoup plus susceptibles de confier cette responsabilité à un

autre employé de l'organisation ou d'externaliser la gestion à une entreprise spécialisée en TI.

- Les propriétaires et les gestionnaires d'entreprise plus âgés (65 ans et plus) sont plus susceptibles que les répondants plus jeunes d'affirmer être responsables des TI de leur entreprise.

Lorsqu'il est question des préoccupations liées aux activités quotidiennes, trois propriétaires ou gestionnaires d'entreprises sur dix craignent les interruptions de travail (31 %) ou les pertes financières (30 %) que peuvent entraîner les cybermenaces. Un répondant sur quatre s'inquiète d'une atteinte à la réputation de l'organisation (25 %) ou de la possibilité que des données de l'entreprise soient détenues contre une rançon. Le niveau de préoccupation par rapport à chacun des trois domaines abordés est légèrement plus élevé en 2022 qu'en 2020.

Graphique 22 : Niveau de préoccupation

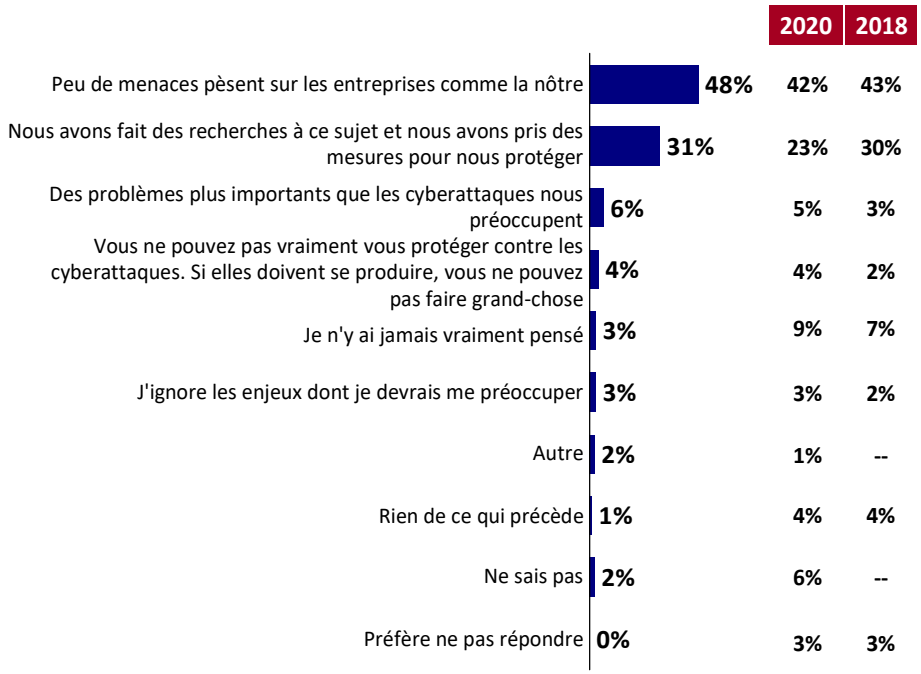


QBUS5A1-A3. En ce qui concerne les diverses préoccupations liées aux activités quotidiennes de votre organisation, à quel point êtes-vous préoccupé(e) par le fait qu'une cybermenace puisse…?
Base : n=301; 2020 : n=360

- Les petites entreprises de dix employés ou moins sont moins susceptibles d'être préoccupées par les interruptions de travail ou par la possibilité que des données soient détenues contre une rançon, alors que celles comptant plus de dix employés se disent préoccupées.
- Les résultats ne varient pas trop entre les différents groupes démographiques.

Parmi les répondants qui ne sont pas préoccupés, près de la moitié (48 %) dit avoir l'impression que peu de menaces pèsent sur les entreprises comme la leur (ce qui est en harmonie avec les résultats obtenus en 2020 et en 2018). Une personne sur trois (33 %) affirme avoir effectué des recherches et avoir pris des mesures pour protéger son entreprise. Une moindre proportion soutient que des problèmes plus importants que les cyberattaques les préoccupent (6 %), croit ne pas pouvoir faire grand-chose contre les cyberattaques (4 %), dit n'avoir jamais vraiment pensé à la cybersécurité (3 %) ou ignore les enjeux dont elle devrait se préoccuper (3 %).

Graphique 23 : Raison du manque de préoccupation



QBUS5B. Pourquoi donc?
Base : n=188; 2020 : n=203; 2018 : n=533

- Les personnes représentant des petites entreprises de dix employés ou moins déclarent plus souvent ne pas se préoccuper des possibles répercussions, car elles considèrent que peu de menaces pèsent sur elles.
- La même tendance se dégage des gens qui ont fait des études universitaires.

Environ deux propriétaires ou gestionnaires d'entreprise sur cinq indiquent que leur entreprise exige une protection par mot de passe sur tous les dispositifs (69 %), garde les logiciels de sécurité à jour sur tous les dispositifs (63 %) ou utilise un mot de passe ou un système d'authentification d'utilisateur pour l'accès sans fil et à distance (60 %). Plus de la moitié (58 %) prend des mesures pour effectuer des copies de sécurité sur tous les dispositifs, alors qu'un peu moins de la moitié (49 %) installe des logiciels de filtrage antipourriel pour se protéger contre les cybermenaces. Environ un répondant sur trois utilise un logiciel de cryptage (34 %) ou adopte une politique de cybersécurité pour les employés (32 %). Environ un sur quatre suit des protocoles de suppression d'information lorsque des employés quittent l'organisation (28 %), n'utilise pas un compte administrateur pour accéder au Web (24 %) ou offre une formation sur les pratiques exemplaires de cybersécurité pour les employés (24 %). Toutes les mesures évaluées sont en hausse par rapport à 2020, mais demeurent inférieures aux résultats obtenus en 2018.

Graphique 24 : 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?

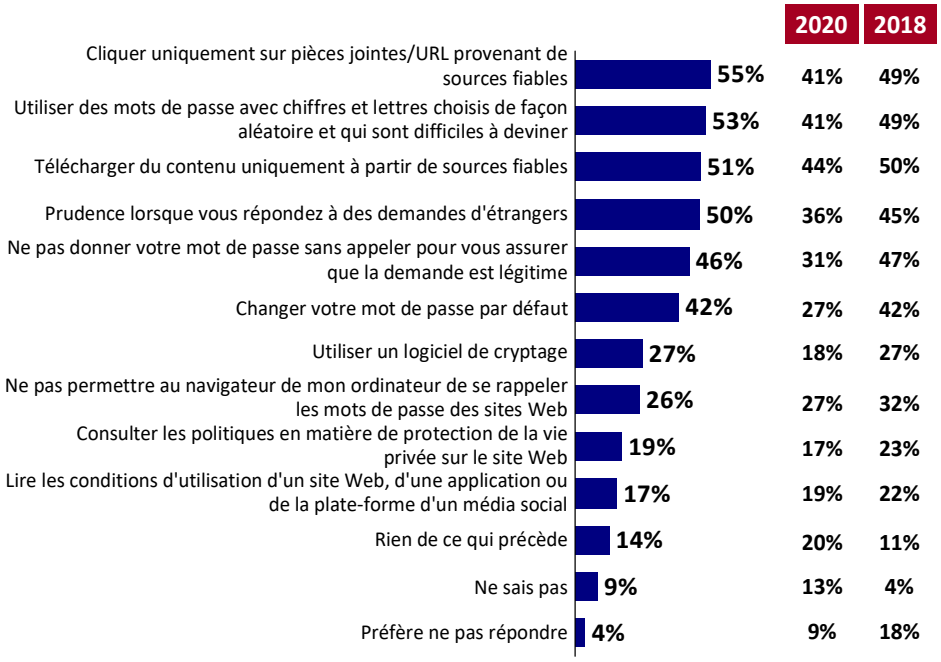
Base : n=301; 2020 : n=360; 2018 : n=533

- Les répondants qui ont recours à une société spécialisée en TI sont plus susceptibles de s'assurer d'utiliser des logiciels de filtrage antipourriel à jour et d'avoir recours à un mot de passe ou à un système d'authentification d'utilisateur pour l'accès sans fil et à distance. Ceux qui utilisent des employés à l'interne pour les TI sont plus susceptibles d'adopter une politique de cybersécurité pour les employés, d'utiliser un logiciel de cryptage, de suivre des protocoles de suppression d'information lorsque des employés quittent l'organisation et de fournir une formation sur les pratiques exemplaires de cybersécurité aux employés. Ceux qui sont personnellement responsables des TI mentionnent plus souvent le fait d'effectuer régulièrement des copies de sécurité de tous les dispositifs.
- Les grandes entreprises de plus de dix employés ont plus tendance à mentionner plusieurs de ces mesures de sécurité (p. ex., exiger une protection par un mot de passe sur tous les dispositifs, utiliser un mot de passe pour l'accès sans fil, adopter une politique de cybersécurité, offrir une formation sur la cybersécurité et utiliser un logiciel de cryptage).
- Les entreprises dont les revenus sont plus élevés sont plus susceptibles de dire qu'elles offrent une formation sur les pratiques exemplaires de cybersécurité ou qu'elles adoptent une politique de cybersécurité.

Environ deux propriétaires ou gestionnaires d'entreprise sur cinq indiquent que les employés sont invités à cliquer uniquement sur les pièces jointes ou les URL provenant de sources fiables (55 %), à utiliser des mots de passe contenant des chiffres et des lettres choisis de façon aléatoire qui sont difficiles à deviner (53 %), à télécharger du contenu uniquement à partir de sources fiables (51 %) ou à faire preuve de prudence lorsqu'ils répondent à des demandes d'étrangers (50 %). Environ deux de ces répondants sur cinq demandent à leurs employés de ne pas donner leur mot de passe sans appeler pour vérifier que la demande est légitime (46 %) ou de changer leur mot de passe par défaut (42 %). Un propriétaire ou gestionnaire d'entreprise sur quatre 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 (26 %). Moins d'un de ces répondants sur dix demande aux employés de consulter les politiques en matière de protection de la vie privée des sites Web (19 %) ou de lire les conditions d'utilisation des sites Web, des applications ou des plateformes des médias sociaux (17 %). Un peu plus d'une personne sur dix (14 %) ne fournit aucune directive à ses employés pour protéger l'entreprise contre les cybermenaces.

La plupart des directives évaluées dans le présent sondage sont mentionnées plus souvent qu'en 2020, les quatre premières présentant aussi une hausse par rapport à 2018.

Graphique 25 : 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=301; 2020 : n=360; 2018 : n=533

- Les entreprises comptant plus de dix employés sont plus susceptibles de demander aux employés de cliquer uniquement sur les pièces jointes ou les URL provenant de sources fiables et de faire preuve de prudence lorsqu'ils répondent à des demandes d'étrangers. Cette dernière directive est fournie plus souvent lorsque l'entreprise a un employé interne spécialisé en TI. Les employés qui s'occupent personnellement des TI ont plus tendance à demander aux autres employés d'utiliser des règles de mot de passe appropriées et de télécharger du contenu uniquement à partir de sources fiables.

La moitié des propriétaires ou des gestionnaires d'entreprise affirment que leur entreprise tirerait profit de directives pour réagir à une cyberattaque (50 %) et d'une liste de types de menaces qui existent et de signaux à rechercher (49 %). Environ deux personnes sur cinq estiment qu'elles tireraient parti de mesures pour protéger les appareils mobiles dans un environnement public (44 %), de pratiques sur la façon pour les employés de gérer les mots de passe (44 %), de pratiques exemplaires sur la sécurité dans un environnement de nuage informatique (43 %), de directives sur l'utilisation de dispositifs personnels au travail (42 %), de ressources sur la façon de crypter des ordinateurs, portables et dispositifs de stockage (41 %),

de ressources pour le type de logiciel ou matériel permettant de sécuriser des réseaux (41 %) ou de directives pour mettre en place des règles relatives à la politique d'utilisation sécuritaire des courriels (40 %). Environ la même proportion affirme qu'elle profiterait de pratiques exemplaires pour l'utilisation de dispositifs de stockage (39 %) ou de pratiques exemplaires pour une politique claire d'utilisation d'Internet (38 %). Environ un répondant sur trois pense pouvoir protéger son entreprise en ayant recours à des conseils pour communiquer aux employés l'importance de suivre des politiques de cybersécurité (35 %) ou des informations sur les mesures pour gérer les renseignements liés au travail que possèdent les employés qui quittent l'organisation (33 %). Un répondant sur quatre mentionne le besoin de directives sur la façon d'établir une politique solide en matière d'utilisation de médias sociaux (28 %).

Tableau 4 : Renseignements utiles pour les petites et moyennes entreprises

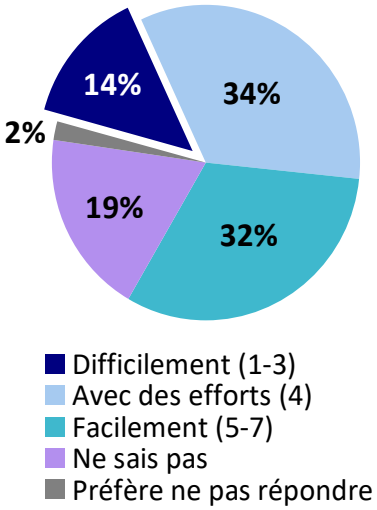
--	**Total 2022**	**Total 2020**	**Total 2018**
QBUS3. De quels types de renseignements parmi les suivants croyez-vous que votre organisation tirerait profit pour se protéger contre les cybermenaces?	*n=301*	*n=360*	*n=533*
Directives pour réagir à une cyberattaque	50 %	40 %	46 %
Liste de types de menaces qui existe et signaux à rechercher	49 %	41 %	47 %
Mesures pour protéger les appareils mobiles dans un environnement public	44 %	39 %	40 %
Meilleures pratiques sur la façon pour les employés de gérer les mots de passe	44 %	29 %	37 %
Pratiques exemplaires sécuritaires en informatique en nuage (avec la définition)	43 %	36 %	35 %
Directives sur l'utilisation de dispositifs personnels au travail	42 %	31 %	40 %
Ressources sur la façon de crypter des ordinateurs, portables et dispositifs de stockage	41 %	34 %	37 %
Conseils et ressources pour le type de logiciel ou matériel permettant de sécuriser des réseaux	41 %	29 %	36 %
Directives pour mettre en place des règles relatives à la politique d'utilisation sécuritaire des courriels	40 %	28 %	39 %
Meilleures pratiques pour l'utilisation de dispositifs de stockage (p. ex., clés USB)	39 %	34 %	40 %
Meilleures pratiques pour une politique claire d'utilisation d'Internet	38 %	27 %	37 %
Conseils pour communiquer aux employés l'importance de suivre de politiques de cybersécurité	35 %	25 %	32 %

--	Total 2022	Total 2020	Total 2018
Mesures pour gérer les renseignements liés au travail que possèdent les employés qui quittent l'organisation	33 %	22 %	33 %
Directives sur la façon d'établir une politique solide en matière de médias sociaux	28 %	26 %	37 %
Autre	4 %	3 %	4 %
Aucune de ces réponses	5 %	9 %	8 %
Je ne sais pas	11 %	13 %	12 %
Je préfère ne pas répondre	4 %	7 %	7 %

- Parmi les répondants qui s'occupent personnellement des TI, la demande pour chacun de ces types d'information est plus élevée que chez les autres répondants, ce qui donne à penser que la demande pour ce type d'information est possiblement de 10 à 15 points de pourcentage plus élevé que ce qui est indiqué.
- Dans les petites entreprises de dix employés ou moins, la demande est comparativement plus élevée pour les conseils sur le type de logiciel ou de matériel permettant de sécuriser les réseaux.
- En comparaison avec les petites entreprises, la demande est plus forte dans les entreprises comptant plus de dix employés en ce qui a trait aux directives pour réagir à une cyberattaque, aux directives sur l'utilisation de dispositifs personnels au travail, aux pratiques exemplaires sur la façon pour les employés de gérer les mots de passe, et aux conseils pour communiquer aux employés l'importance de suivre des politiques de cybersécurité.

Près de la moitié des propriétaires ou gestionnaires d'entreprise croient qu'il faudrait un certain effort pour se remettre de l'attaque d'un rançongiciel (34 %) ou qu'il serait difficile de s'en remettre (14 %). Environ un répondant sur trois (32 %) est d'avis qu'il serait facile de s'en remettre. Une personne sur cinq (19 %) n'est pas sure ou préfère ne pas répondre (2 %).

Graphique 26 : Se remettre d'une attaque d'un rançongiciel

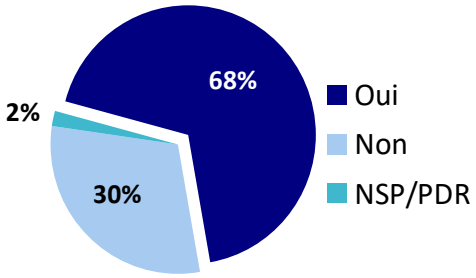


BUSBA42. Dans quelle mesure votre entreprise serait-elle en mesure de se remettre d'une attaque d'un rançongiciel?
Base : n=301

- Les représentants d'entreprises de dix employés ou moins sont plus susceptibles que leurs homologues des plus grandes entreprises de dire qu'il serait facile de se remettre d'une cyberattaque. Cette tendance est également avérée pour les répondants dont le niveau de scolarité est plus élevé.

Deux propriétaires ou gestionnaires d'entreprise sur trois indiquent avoir des employés qui travaillent à la maison au moins à temps partiel.

Graphique 27 : Employés travaillant à domicile



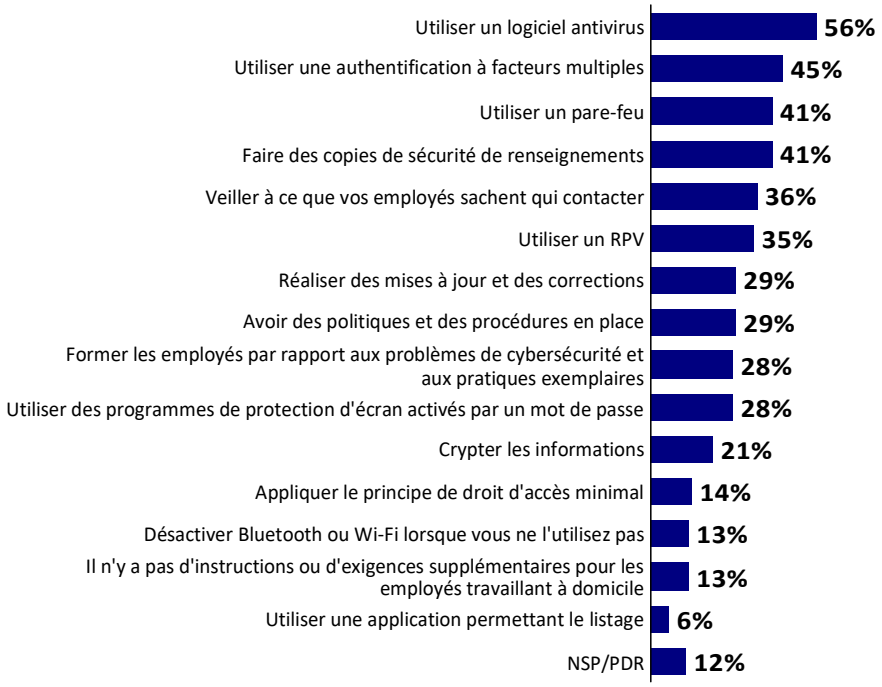
QBUS2B. Votre entreprise a-t-elle des employés qui travaillent à domicile, même à temps partiel?
Base : n=301

- Les entreprises comptant plus de dix employés ont plus souvent des employés travaillant à la maison à temps partiel.
- Les gens qui ont un niveau de scolarité plus élevé ont plus tendance à avoir des employés qui travaillent à la maison, ainsi que les parents d'enfants âgés de 6 à 12 ans ou de 13 à 15 ans.

Plus de la moitié (56 %) des propriétaires ou gestionnaires d'entreprise disent exiger l'utilisation d'un logiciel antivirus pour les employés qui travaillent à domicile afin de protéger l'entreprise contre les cybermenaces. Environ deux de ces répondants sur cinq affirment exiger l'utilisation d'une authentification à facteurs multiples (45 %), d'un pare-feu (41 %) ou de copies de sécurité (41 %). Plus d'un propriétaire ou gestionnaire d'entreprise sur trois déclare s'assurer que les employés savent avec qui communiquer (36 %) ou comment utiliser un RPV. Plus de deux de ces répondants sur dix exigent que les employés réalisent des mises à jour et des corrections (29 %), mettent en place des politiques et procédures (29 %), forment les employés par rapport aux problèmes de cybersécurité et aux pratiques exemplaires (28 %), utilisent des programmes de protection d'écran activés par un mot de passe (28 %) ou cryptent des informations (21 %). Parmi les autres instructions ou exigences figurent l'application du principe de droit d'accès minimal (14 %), la désactivation de Bluetooth ou du réseau sans fil lorsqu'ils ne sont pas utilisés (13 %) ou l'utilisation d'une application permettant le listage (6 %). Plus d'un propriétaire ou

gestionnaire d'entreprise sur dix n'a pas d'instruction ou d'exigences supplémentaires pour les employés travaillant à domicile (13 %) ou n'est pas sûr (12 %).

Graphique 28 : Protection des employés à domicile contre les cybermenaces



QBUS2C. Quelles instructions ou exigences supplémentaires fournissez-vous aux employés qui travaillent à domicile pour protéger l'entreprise contre les cybermenaces?
Base : n=209

- Les petites organisations, ainsi que celles dont le répondant est responsable des TI, sont plus susceptibles que les autres de dire qu'elles demandent aux employés d'effectuer des copies de sécurité de leurs informations.
- Les personnes représentant de plus grandes entreprises sont plus susceptibles que celles travaillant pour de petites entreprises de demander aux employés d'utiliser un RPV, de s'assurer que les employés savent qui contacter s'ils éprouvent un problème de TI, de mettre en place des politiques et des procédures, et de former les employés par rapport aux problèmes de cybersécurité et aux pratiques exemplaires. Ces pratiques sont particulièrement courantes si l'entreprise a un employé spécialisé en TI.

ANNEXES

A. DÉTAILS MÉTHODOLOGIQUES

L'échantillon se compose de 2 050 entretiens réalisés avec des Canadiens âgés de 18 ans ou plus qui utilisent régulièrement Internet, y compris plus de 553 entrevues avec des parents de jeunes âgés de 16 à 24 ans, et 301 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 12 295 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 17 pour cent[3]. L'échantillon du sondage final, en vertu duquel 2 050 sondages ont été achevés, présente un niveau de précision de +/- 2,2 pour cent pour l'échantillon dans son ensemble et de +/- 3 à

[3] Dans l'échantillon de 12 295 cas, 58 invitations n'ont pu être remises au destinataire (échantillon valide de 12 237 cas) et 31 cas ont été rejetés, car hors de portée.

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).

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

Le sondage, qui s'est déroulé entre le 21 janvier et le 14 février 2022, faisait appel à un questionnaire bilingue de 15 minutes 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 5 : Tableau démographique

Tableau 5a : Province/Territoire (non pondérés)

-	**Total**
n=	*2050*
Colombie-Britannique et Yukon	13 %
Alberta et Territoires-du-Nord-Ouest	12 %
Saskatchewan et Manitoba	10 %
Ontario	36 %
Québec et Nunavut	21 %
Atlantique	9 %

Tableau 5b : Genre (non pondéré)

-	**Total**
n=	*2050*
Homme	48 %
Femme	50 %
Préfère s'auto-identifier	2 %
Préfère ne pas répondre	1 %

Tableau 5c : Âge (non pondéré)

-	**Total**
n=	*2050*
18-24	4 %
25-34	18 %
35-44	21 %
45-54	19 %
55-64	17 %
65 et +	21 %

Tableau 5d : Enfants du ménage âgés de moins de 18 ans

--	**Total**
n=	*2050*
Oui	25 %
Non	74 %
Préfère ne pas répondre	0 %

Tableau 5e : Âge des enfants à la maison

-	**Total**
n=	*553*
Moins de 6 ans	39 %
6 à 12	47 %
13 à 15	31 %
16 ans ou plus	34 %
Préfère ne pas répondre	1 %

Tableau 5f : Niveau de scolarité atteint

-	**Total**
n=	*2050*
École secondaire ou moins	13 %
Un peu d'études postsecondaires	12 %
Certificat ou diplôme d'un établissement collégial ou d'une école de métiers	25 %
Diplôme d'études de premier cycle	27 %
Diplôme d'études supérieures ou professionnel	22 %
Préfère ne pas répondre	1 %

Tableau 5h : Revenu annuel du ménage

-	**Total**
n=	*2050*
Moins de 20 000 $	4 %
Entre 20 000 $ et 39 999 $	10 %
Entre 40 000 $ et 59 999 $	12 %
Entre 60 000 $ et 79 999 $	12 %
Entre 80 000 $ et 99 999 $	11 %
Entre 100 000 $ et 149 999 $	20 %
150 000 $ ou plus.	17 %
Ne sais pas/Pas de réponse	13 %

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 %, comparativement à 35 % dans la population). Comme décrit précédemment, chaque échantillon a été pondéré en fonction de l'âge, du sexe et de la région.

B. QUESTIONNAIRE

WINTRO

Online

Merci pour votre participation à ce sondage. Ekos Research Associates, une société canadienne de recherche sur l'opinion publique, réalise le sondage au nom du gouvernement du Canada sur des questions relatives à la sécurité en ligne. If you prefer to answer the survey in English, please click on English. **Votre participation est facultative et vos réponses demeureront confidentielles et anonymes.** Il faut environ 15 minutes pour répondre au sondage, qui est géré par les Associés de recherche EKOS en conformité avec à la *Loi sur la protection des renseignements personnels*. Pour consulter notre politique de confidentialité, cliquez ici. Cette recherche est enregistrée auprès du service de vérification des recherches du Conseil de recherche et d'intelligence marketing canadien. Veuillez cliquer ici si vous souhaitez vérifier son authenticité (code du projet 20220121-EK115). Si vous avez besoin d'assistance technique, veuillez communiquer avec nous à online@ekos.com.

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
Je préfère ne pas répondre	99

QEMP

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	97
Je ne sais pas	98
Pas de réponse	99

QEMPA

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	98
Pas de réponse	99

QEMPB [1,2]

Full/part-time employed, D2; Fewer than 100 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
Je préfère ne pas répondre	99

QCHILDA [1,6]

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
Je préfère ne pas répondre	99

D4

Quelle est votre année de naissance?

Année :	1
Je préfère ne pas répondre	9999

QAGEA

Avez-vous au moins 18 ans?

Oui	1
Non	2
Pas de réponse	99

QAGEY

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

Pas de réponse	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

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 réponse (veuillez préciser)	77
Rien de ce qui précède	98
Je ne sais pas	99

Q6

MFA

Utilisez-vous <hover="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">une authentification à facteurs multiples>?

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 réponse (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 sais 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 sais 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 ou d'un SMS 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

B11B [1,10]

D'après ce que vous savez, quels sont les signes d'une tentative d'hameçonnage?

Veuillez choisir toutes les réponses pertinentes

Le message utilise un langage insistant ou menaçant	1
Le message demande des informations sensibles, comme des renseignements financiers ou identificatoires	2
Le message transmet une offre qui est trop belle pour être vraie	3
Le message prétend porter sur des comptes que vous n'avez pas ou sur des livraisons que vous n'attendez pas	4

Le message contient des adresses de courriel d'expéditeur incorrectes, des liens inconnus, ou des fautes d'orthographe ou de grammaire	5
Le message comprend des pièces jointes inattendues ou inutiles, qui peuvent avoir des noms de fichiers étranges ou des types de fichiers peu courants	6
Le message peut utiliser une conception graphique non professionnelle, avec des images pixélisées ou un formatage médiocre	7
Autre (veuillez préciser)	77
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

Utilise uniquement des sites Web que je connais bien	1
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
Affiche le symbole du verrou de sécurité	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

Q11D

Au cours de la prochaine année, avez-vous l'impression que vous serez victime d'une cybermenace où vos données seront conservées en vue d'obtenir une rançon?

1 Pas du tout probable	1
2	2
3 Moyennement probable	3
4	4
5 Extrêmement probable	5
Je ne sais pas	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 ou financières conservées pour rançon	6
Perte de renseignements ou de fichiers	7
Données personnelles effacées, modifiées, perdues	8
Autre réponse (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 réponse (veuillez 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
Hameçonnage	6
Rançongiciel	7
Rien de ce qui précède	97
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
Déconnecter tous les périphériques connectés à votre réseau	11
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 réponse (veuillez 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 réponse (veuillez préciser)	77
Rien de ce qui précède	97
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 réponse (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 sais pas	99

IC8B [1,8]

1-9,77, IC5A

Quels aspects de cette information étaient utiles?

Veuillez choisir toutes les réponses pertinentes

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 réponse (veuillez préciser)	77
Rien	97
Je ne sais pas	99

QEMPE

À quelle fréquence travaillez-vous à domicile?

Temps partiel	1
Temps plein	2
Au besoin	3
Jamais	4
Je ne sais pas	8
Pas de réponse	9

QEMPF

Votre employeur vous a-t-il donné des instructions ou des exigences précises pour protéger l'entreprise contre les cybermenaces?

Oui	1
Non	2
Je ne sais pas	8
Pas de réponse	9

QEMPFB [1,10]

Si c'est le cas, quel type d'instructions ou d'exigences avez-vous reçu de votre employeur?

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
Formation pour les employés sur les pratiques exemplaires en matière de cybersécurité	9
Adoption d'une politique de cybersécurité pour les employés	10
Rien de ce qui précède	97
Je ne sais pas	98
Je préfère ne pas répondre	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

IC6 [1,15]

À qui feriez-vous confiance pour vous donner la meilleure **information technologique fiable et à jour** sur les menaces en ligne et les mesures à prendre pour vous protéger?

Sélectionner toute réponse pertinente

Des amis ou membres de la famille	1
Un fournisseur de services internet	2
Une compagnie de logiciels de sécurité	3
Des institutions financières	4
Le site Web d'un fournisseur (p. ex. un magasin en ligne que vous fréquentez, etc.)	5
Une organisation sans but lucratif qui se consacre à la sécurité électronique	6
Le gouvernement	7
Un organisme d'application de la loi	8
Autre réponse (veuillez préciser)	77
Je ne sais pas	98
Pas de réponse	99

BUS1 [1,20]

FT/PT (D2) and responsible (EMPB) OR S-E (D2) AND Size <100 (QEMP / QEMPA)

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
Formation pour les employés sur les pratiques exemplaires en matière de cybersécurité	9
Adoption d'une politique de cybersécurité pour les employés	10
Rien de ce qui précède	97
Je ne sais pas	98
Je préfère ne pas répondre	99

BUS2 [1,20]

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

QBUS2B

Votre entreprise a-t-elle des employés qui travaillent à domicile, même à temps partiel?

Oui	1
Non	2
Je ne sais pas	98
Je préfère ne pas répondre	99

QBUS2C [1,20]

Quelles instructions ou exigences supplémentaires fournissez-vous aux employés qui travaillent à domicile pour protéger l'entreprise contre les cybermenaces?

Veuillez choisir toutes les réponses pertinentes

Utiliser un RPV	1
Utiliser un pare-feu	2
Utiliser un logiciel antivirus	3
Utiliser une application permettant le listage	4
Avoir des politiques et des procédures en place	5
Veiller à ce que vos employés sachent qui contacter	6
Former les employés par rapport aux problèmes de cybersécurité et aux pratiques exemplaires	7
Utiliser une authentification à facteurs multiples	8
Utiliser des programmes de protection d'écran activés par un mot de passe	9
Réaliser des mises à jour et des corrections	10
Désactiver Bluetooth ou Wi-Fi lorsque vous ne l'utilisez pas	11
Faire des copies de sécurité de renseignements	12
Crypter les informations	13
Appliquer le principe de droit d'accès minimal	14
Il n'y a pas d'instructions ou d'exigences supplémentaires pour les employés travaillant à domicile	97
Je ne sais pas	98
Pas de réponse	99

BUS3 [1,20]

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 réponse (veuillez préciser)	77
Rien de ce qui précède	97
Je ne sais pas	98
Je préfère ne pas répondre	99

BUS4 [1,20]

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 réponse (veuillez préciser)	77
Rien de ce qui précède	97
Je ne sais pas	98
Je préfère ne pas répondre	99

BUS5A1

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

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

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

BUS5A4

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...

conserver des données de votre entreprise en vue d'obtenir une rançon?

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 réponse (veuillez préciser)	77
Rien de ce qui précède	97
Je ne sais pas	98
Je préfère ne pas répondre	99

BUSBA42

Dans quelle mesure votre entreprise serait-elle en mesure de se remettre d'une attaque d'un rançongiciel?

1 Très difficilement	1
2	2
3	3
4 Difficilement mais assez bien	4
5	5
6	6
7 Facilement, avec des conséquences limitées	7
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 réponse (veuillez 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

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

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

<[THNKSP2 = 1 and QCHILDA = 4,5]Nous vous avons envoyé une invitation à transmettre à votre fils ou votre fille de 16 à 24 ans pour participer à cette étude. Si vous avez plus qu'un(e) fils ou fille de 16 à 24 ans à la maison, veuillez le transmettre à l'adolescent(e) qui a fêté son anniversaire de naissance le plus récemment.> 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.