Gouvernement du Canada | Government of Canada

Sondage de suivi sur la connaissance de la campagne Pensez cybersécurité

Rapport final de 2024

Préparé pour le Centre de la sécurité des télécommunications Canada

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

Pour plus d'information sur le présent rapport, veuillez communiquer avec le CST à l'adresse : media@cse-cst.gc.ca

This report is also available in English

Canada

Sondage de suivi sur la connaissance de la campagne Pensez cybersécurité Rapport final

Préparé par le Centre de la sécurité des télécommunications
Nom du fournisseur : Phoenix Strategic Perspectives Inc.
Avril 2024

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

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

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

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

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

Table des matières

Liste des diagrammes

Sommaire

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

Contexte et objectifs

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

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

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

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

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

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

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

Méthodologie

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

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

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

Principales constatations

Les pratiques de cybersécurité des Canadiens et des Canadiennes en ligne

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

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

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

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

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

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

La cybercriminalité et les menaces

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

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

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

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

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

Les communications et la campagne Pensez cybersécurité

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

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

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

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

Les entreprises et la cybersécurité

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

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

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

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

Les parents et la cybersécurité

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

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

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

Observations finales

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

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

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

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

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

Notes à l'intention du lecteur

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

Valeur du contrat

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

Déclaration de neutralité politique

En ma qualité de cadre supérieure de Phoenix Strategic Perspectives, je certifie par la présente que les produits livrés sont en tout point conformes aux exigences du gouvernement du Canada en matière de neutralité politique qui sont décrites dans la Politique de communication du

gouvernement du Canada et dans la Procédure de planification et d'attribution de marchés de services de recherche sur l'opinion publique. Plus particulièrement, les produits finaux ne comprennent pas de renseignements sur les intentions de vote aux élections, les préférences de partis politiques, les positions vis-à-vis de l'électorat ou l'évaluation de la performance d'un parti politique ou de son dirigeant.

Alethea Woods
Présidente
Phoenix Strategic Perspectives Inc.

Constatations du sondage

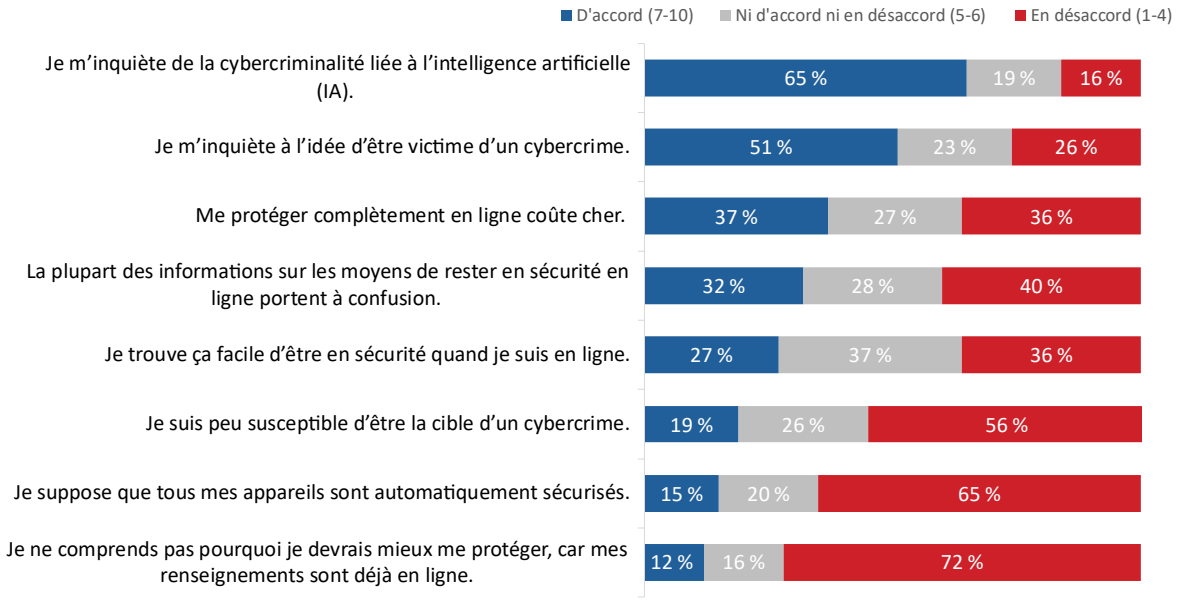
Points de vue et attitudes à l'égard de la cybersécurité

La majorité des Canadiens et des Canadiennes s'inquiètent de l'IA et de la cybercriminalité.

On a demandé aux répondants d'indiquer dans quelle mesure ils étaient d'accord ou en désaccord avec huit énoncés concernant des préoccupations en matière de cybersécurité. Pour ce faire, ils devaient utiliser une échelle de 10 points, où 1 signifiait « fortement en désaccord » et 10, « entièrement d'accord ». Les deux tiers (65 %) des Canadiens et des Canadiennes en ligne ont indiqué qu'ils s'inquiétaient de la cybercriminalité liée à l'intelligence artificielle (IA) (cotes de 7 à 10 sur l'échelle de 10 points) et la moitié (51 %) craignent d'être victimes d'un acte de cybercriminalité en général. En outre, beaucoup se considèrent comme une cible probable (56 % étaient en désaccord avec l'affirmation « *Je suis peu susceptible d'être la cible d'un cybercrime* »).

Lorsqu'il s'agit de se protéger en ligne, les Canadiens et Canadiennes avaient une opinion mitigée par rapport à ce qui suit : « me protéger complètement en ligne coûte cher » (37 % étaient d'accord, 27 % se disaient ni d'accord ni en désaccord et 36 % étaient en désaccord), « la plupart des informations sur les moyens de rester en sécurité en ligne portent à confusion » (32 % étaient d'accord, 28 % se disaient ni d'accord ni en désaccord et 40 % étaient en désaccord) et « je trouve facile d'être en sécurité quand je suis en ligne » (27 % étaient d'accord, 37 % se disaient ni d'accord ni en désaccord et 36 % étaient en désaccord). Un nombre relativement faible de personnes présument que leurs appareils sont automatiquement sécurisés (15 %) et ne voient pas l'intérêt d'essayer de protéger leurs renseignements, car ces derniers sont déjà en ligne (12 %).

Diagramme 1 : Attitudes à l'égard de la sécurité en ligne



QCS1a-k. À quel point êtes-vous d'accord avec les énoncés suivants sur la cybersécurité? Base de référence : n=2 222; tous les répondants.

Voici les différences dignes de mention entre les sous-groupes :

- À mesure que l'âge augmente, il en va de même pour les préoccupations concernant l'utilisation de l'IA à des fins de cybercriminalité, les préoccupations relatives au fait d'être victime d'un cybercrime et la perception selon laquelle les informations au sujet de la sécurité en ligne portent à confusion. Les personnes de 18 à 34 ans sont plus susceptibles que les gens plus âgés de penser qu'il est peu probable qu'ils soient la cible d'un cybercrime et de trouver facile d'être en sécurité quand ils sont en ligne.
- Des différences entre les genres sont ressorties. Les femmes sont plus susceptibles que les hommes d'être préoccupées par l'utilisation de l'IA aux fins de la cybercriminalité, de constater qu'il coûte cher de se protéger en ligne et d'être confuses par les informations au sujet de la sécurité en ligne. En revanche, les hommes ont plus tendance que les femmes à penser qu'il est facile d'être en sécurité en ligne.
- À mesure que le revenu du ménage augmente, la probabilité d'être d'accord avec le fait qu'il est coûteux de se protéger complètement en ligne diminue.
- Les résidents du Québec sont plus susceptibles que les habitants de l'Ontario de croire qu'ils seront la cible d'un cybercrime.
- Les personnes qui sont toujours branchées et qui estiment posséder un niveau avancé de connaissances en matière de sécurité en ligne sont plus susceptibles de trouver qu'il est facile d'être en sécurité en ligne. Elles sont également plus enclines à être en désaccord avec l'énoncé selon lequel la plupart des informations sur la sécurité en ligne portent à confusion. Les Canadiens et Canadiennes ayant un niveau avancé de connaissances en matière de sécurité en ligne sont plus susceptibles de *ne pas* craindre d'être victimes de la cybercriminalité. Les personnes qui possèdent un niveau de connaissances de base ont plus tendance à penser qu'il est coûteux de se protéger complètement en ligne. De plus, elles sont plus nombreuses à supposer que leurs appareils sont sécurisés, à penser qu'il est inutile d'essayer d'être en sécurité en ligne, à trouver que les informations sur la sécurité en ligne portent à confusion et à craindre de devenir victimes d'un cybercrime.

Relativement peu de personnes comptent sur les autres pour être en sécurité en ligne, mais beaucoup se tournent vers d'autres personnes pour obtenir des conseils en matière de cybersécurité.

Un peu plus d'une personne sur 10 (15 %) a indiqué qu'elle comptait sur d'autres personnes, comme sa famille ou ses collègues, pour assurer sa sécurité en ligne[1]. On a demandé aux gens d'indiquer dans quelle mesure ils étaient d'accord ou en désaccord, en utilisant une échelle de 10 points, avec l'énoncé « *Je compte sur d'autres personnes (p. ex., ma famille, mes collègues) pour assurer ma sécurité en ligne* ».

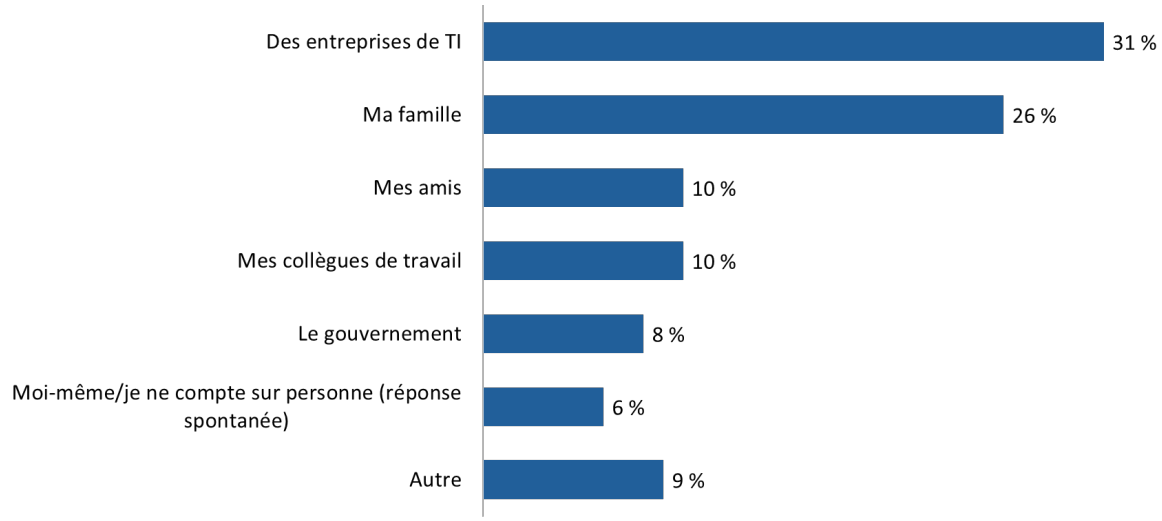
En ce qui concerne l'aide ou les conseils en matière de cybersécurité en général, un peu plus de la moitié des Canadiens et des Canadiennes en ligne comptent sur les entreprises de TI (31 %) ou leur famille (26 %). Deux personnes sur 10 comptent sur des amis (10 %) ou des collègues de travail

[1] QCS1m. À quel point êtes-vous d'accord avec les énoncés suivants sur la cybersécurité? Base de référence : n=2 222 ; tous les répondants.

(10 %), tandis que moins d'une personne sur 10 (8 %) se tourne vers le gouvernement, comme les sites Web du gouvernement. Six pour cent ont dit spontanément qu'ils géraient leur propre cybersécurité et qu'ils ne comptaient sur personne pour obtenir de l'aide ou des conseils.

Neuf pour cent des personnes sondées ont mentionné d'autres sources d'aide ou de conseils. Les types de réponses dans la catégorie « autre » comprenaient entre autres des experts en sécurité, des applications de sécurité, des médias sociaux (YouTube, Reddit), des émissions de radio et de télévision, des logiciels antivirus, Google, Internet (sans précisions supplémentaires) et diverses ressources en ligne.

Diagramme 2 : Source d'aide ou de conseils en matière de cybersécurité



QCS2. Sur qui comptez-vous le plus pour obtenir de l'aide ou des conseils en matière de cybersécurité? Base de référence : n=2 222; tous les répondants.

Les personnes âgées de 65 ans et plus sont plus susceptibles de déclarer qu'elles comptent le plus sur leur famille pour obtenir de l'aide ou des conseils en matière de cybersécurité, tandis que celles âgées de 18 à 34 ans ont plus tendance à compter sur des amis pour obtenir de tels conseils et se tournent moins vers des entreprises de TI.

Lorsqu'on examine les différences générationnelles, la génération Z est la plus susceptible de déclarer qu'elle compte sur ses amis, tandis que les milléniaux et la génération X sont plus enclins que la génération Z et les baby-boomers à se fier à leurs collègues de travail. La génération X et les baby-boomers ont plus tendance que les milléniaux et la génération Z à compter sur les entreprises de TI pour obtenir de l'aide ou des conseils en matière de cybersécurité.

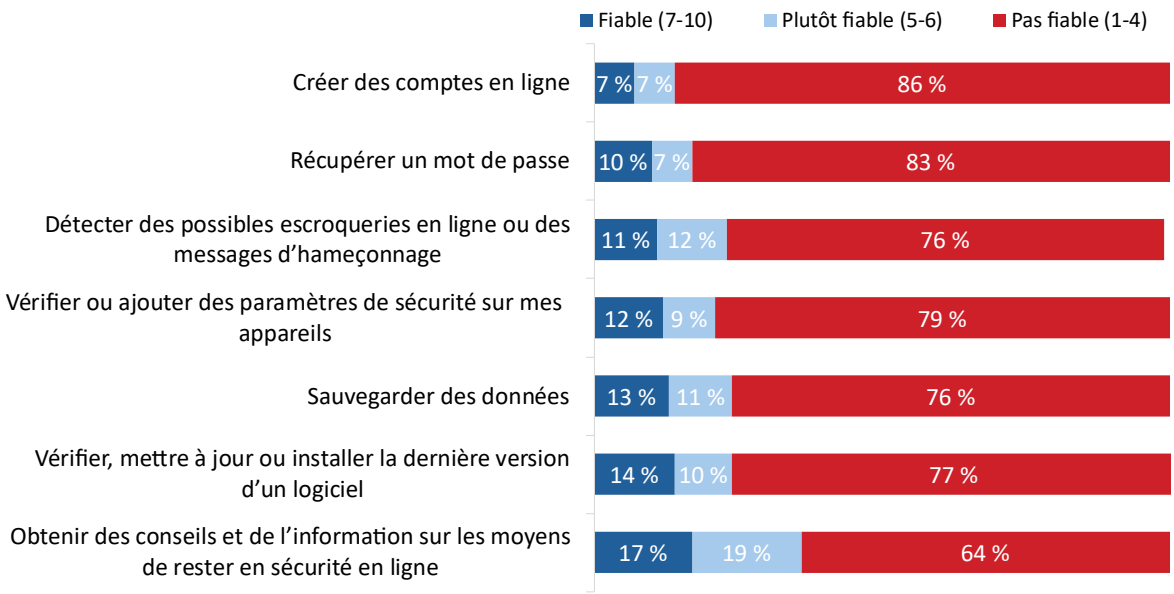
Les personnes possédant des connaissances de base en matière de sécurité en ligne sont plus susceptibles de compter sur leur famille.

Plus de la moitié des Canadiens et des Canadiennes en ligne ne dépendent pas d'autres personnes pour du soutien en matière de cybersécurité.

On a demandé aux répondants dans quelle mesure ils comptaient sur d'autres personnes pour obtenir de l'aide dans l'exécution de différentes tâches informatiques et de cybersécurité. Ils devaient pour ce faire utiliser une échelle de 10 points, où 1 signifiait « pas fiable du tout » et 10 « tout à fait fiable ». Plus de la moitié des Canadiens et des Canadiennes en ligne ont déclaré qu'ils ne comptaient pas sur d'autres personnes pour effectuer des tâches informatiques et de cybersécurité (cotes de 1 à 4 sur une échelle de 10 points). Les autres se fient au moins dans une certaine mesure à d'autres personnes (cotes de 5 à 10).

Pour ce qui est du soutien, 36 % des Canadiens et des Canadiennes se tournent au moins un peu vers d'autres personnes pour obtenir des conseils et des informations sur les moyens de rester en sécurité en ligne. Ils demandent également l'aide d'autres personnes pour vérifier, mettre à jour ou installer la dernière version d'un logiciel (24 %), pour sauvegarder leurs données (24 %), pour détecter de possibles escroqueries en ligne ou des messages d'hameçonnage (23 %), pour vérifier ou ajouter des paramètres de sécurité à leurs appareils (21 %), pour récupérer un mot de passe (17 %) et pour les aider à créer des comptes en ligne (14 %).

Diagramme 3 : Dépendance à l'égard d'autres personnes pour de l'aide en matière de cybersécurité



QCS3. Dans quelle mesure comptez-vous sur d'autres personnes (p. ex., des ami(e)s ou membres de famille) pour vous aider à faire ce qui suit? Base de référence : n=2 222; tous les répondants.

Les différences notables entre les sous-groupes sont les suivantes :

- Le Québec, suivi du Canada atlantique, semble se distinguer du reste du Canada. Plus précisément, les résidents du Québec sont plus susceptibles de dépendre d'autres personnes pour obtenir des conseils et de l'information sur les moyens de rester en sécurité en ligne, et avec les personnes du Canada atlantique, ils ont plus tendance à compter sur d'autres personnes pour vérifier ou ajouter des paramètres de sécurité à leurs appareils, pour vérifier,

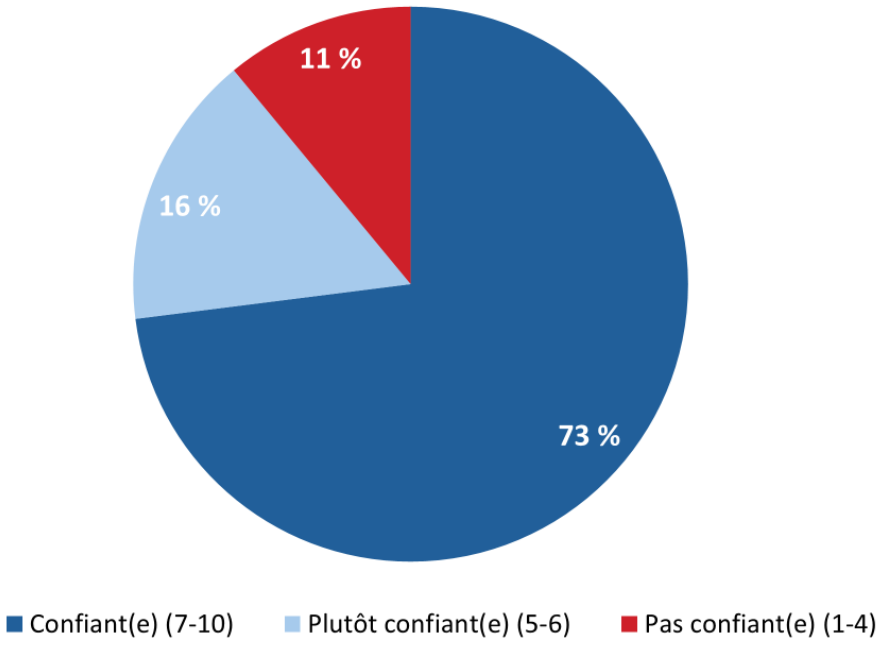
mettre à jour ou installer la version la plus récente d'un logiciel et pour récupérer un mot de passe.

- Plus l'âge augmente, plus s'accroît la probabilité de se fier à d'autres personnes pour l'exécution de toutes ces tâches de cybersécurité. La même tendance a généralement été observée chez les différentes générations : les baby-boomers et la génération silencieuse sont généralement plus susceptibles que la génération Z, la génération Y et la génération X de compter sur d'autres personnes pour obtenir du soutien dans ce domaine.
- De même, les femmes sont plus susceptibles que les hommes de déclarer compter sur d'autres personnes pour obtenir de l'aide à tous ces égards.
- En général, les personnes qui sont toujours branchées et celles qui possèdent un niveau avancé de connaissances en matière de sécurité en ligne sont plus susceptibles de *ne compter* sur personne pour effectuer ces tâches.

La plupart des Canadiens et des Canadiennes sont convaincus qu'ils peuvent identifier un message frauduleux.

Trois personnes en ligne sur quatre (73 %) ont confiance en leur capacité à identifier un message d'hameçonnage ou un lien malveillant. De plus, 16 % se sentent plutôt confiantes. En revanche, une personne sur 10 (11 %) n'est pas convaincue qu'elle serait en mesure d'identifier un message d'hameçonnage ou un lien malveillant.

Diagramme 4 : Niveau de confiance en sa capacité à identifier un message d'hameçonnage ou un lien malveillant



QCS5. À quel point avez-vous confiance en votre capacité à identifier un message d'hameçonnage ou un lien malveillant?
Base de référence : n=2 222; tous les répondants.

Les différences dignes de mention entre les sous-groupes sont les suivantes :

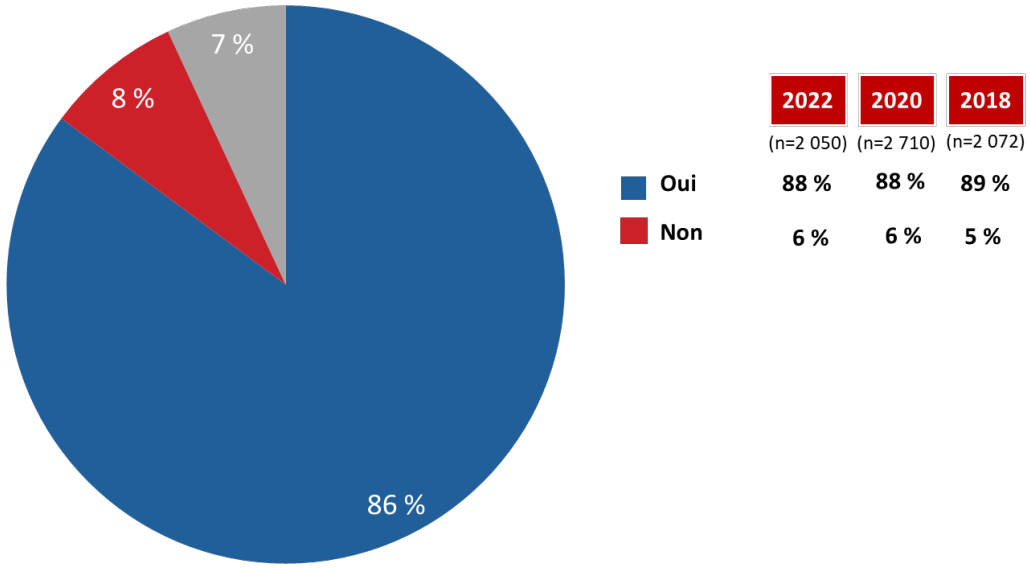
- Les répondants du Manitoba sont plus susceptibles d'avoir confiance en leur capacité à identifier un message d'hameçonnage ou un lien malveillant.
- Plus l'âge augmente, plus le niveau de confiance par rapport à l'identification de tels messages ou liens diminue. La génération Z, la génération Y et la génération X sont plus confiantes que les baby-boomers et la génération silencieuse.
- Plus d'hommes que de femmes ont déclaré être confiants qu'ils peuvent identifier un message d'hameçonnage ou un lien malveillant.
- La confiance dans la capacité d'une personne à repérer un message d'hameçonnage ou un lien malveillant augmente avec le revenu du ménage.
- Les personnes qui sont toujours branchées et celles qui possèdent un niveau avancé de connaissances en matière de sécurité en ligne sont plus susceptibles d'avoir confiance en leur capacité à identifier un message d'hameçonnage.

Les pratiques de cybersécurité des Canadiens et des Canadiennes en ligne

Plus de huit personnes sur 10 prennent des précautions pour protéger leur compte en ligne.

Plus de huit personnes en ligne sur 10 (86 %) ont déclaré prendre des précautions pour protéger leurs comptes en ligne, leurs comptes de médias sociaux, leurs appareils et leurs réseaux. Très peu (8 %) ne le font pas. La proportion de Canadiens et de Canadiennes en ligne qui prennent des précautions a très peu changé depuis la réalisation du sondage de référence en 2018.

Diagramme 5 : Mesures prises pour protéger ses comptes en ligne



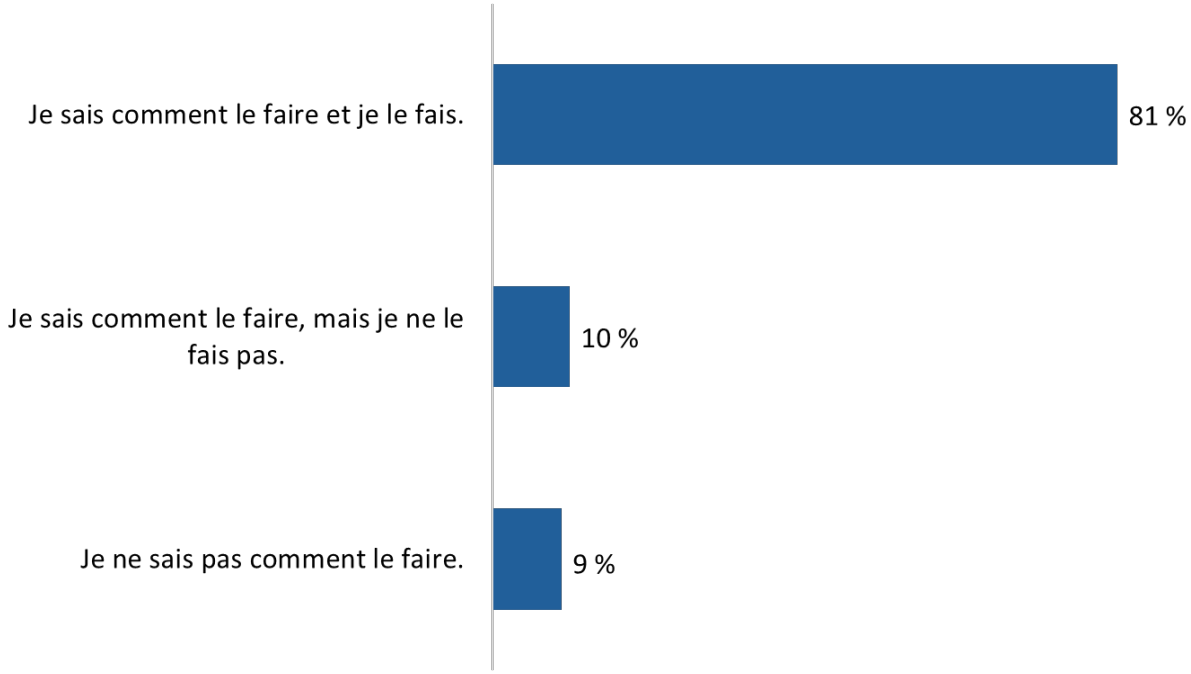
QBEH1. Prenez-vous des précautions pour protéger vos comptes en ligne, vos comptes de médias sociaux, vos appareils ou vos réseaux? Base de référence : n=2 222; tous les répondants.

La probabilité de prendre des précautions pour protéger ses comptes en ligne, ses comptes dans les médias sociaux, ses appareils et ses réseaux est plus élevée chez les résidents du Manitoba et de la Saskatchewan que chez les résidents du Québec et de l'Alberta; les personnes âgées de 45 ans et plus comparativement aux répondants entre 18 et 34 ans; les baby-boomers; les diplômés universitaires; et les personnes qui gagnent plus de 40 000 $ par année. Les parents sont moins enclins que les personnes en ligne qui n'ont pas d'enfants de moins de 18 ans à avoir pris des précautions pour protéger leurs comptes en ligne, leurs comptes dans les médias sociaux, leurs appareils ou leurs réseaux.

La plupart des Canadiens et des Canadiennes en ligne savent comment installer des mises à jour de logiciels et d'applications et le font.

En plus de prendre des précautions pour protéger leurs comptes en ligne, huit personnes sur 10 (81 %) savent comment installer les plus récentes mises à jour de logiciels et d'applications sur leurs appareils et déclarent le faire. De plus, 10 % savent comment installer les mises à jour, mais ne le font pas. Très peu (9 %) ont déclaré qu'ils ne savaient pas comment s'y prendre.

Diagramme 6 : Connaissances par rapport à l'installation des plus récentes mises à jour de logiciels et d'applications



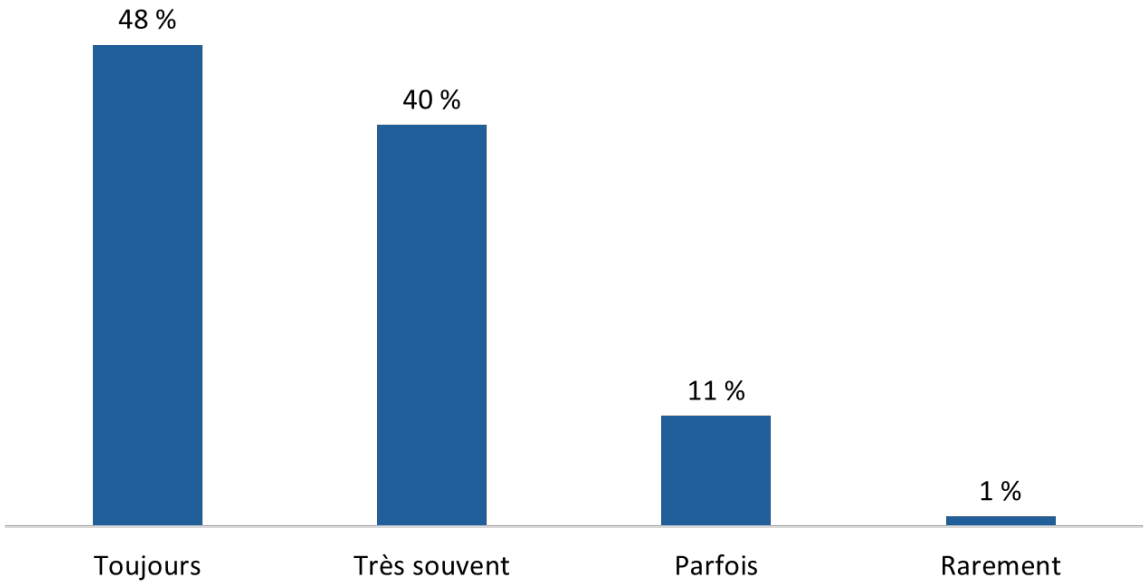
QBEH2. Savez-vous comment installer les plus récentes mises à jour de logiciels et d'applications pour tous vos appareils (p. ex., ordinateur et cellulaire)? Base de référence : n=2 222; tous les répondants.

Les groupes suivants de Canadiens et de Canadiennes en ligne sont *moins* susceptibles de savoir comment installer des mises à jour et de le faire : les personnes âgées de 65 ans et plus, les femmes, les membres de ménages dont le revenu annuel est inférieur à 40 000 $, les personnes qui ont fait des études secondaires ou collégiales, celles qui utilisent Internet quelques fois par semaine ou moins, et celles qui possèdent un niveau de connaissances de base en matière de sécurité en ligne. Les membres de la génération Z sont plus susceptibles de dire qu'ils savent comment installer les plus récentes mises à jour de logiciels et d'applications, mais ne le font pas réellement.

La grande majorité des Canadiens et des Canadiennes installent régulièrement les plus récentes mises à jour de logiciels ou d'applications.

Parmi les personnes qui savent comment installer les plus récentes mises à jour de logiciels et d'applications (n=1 813), la grande majorité (88 %) le fait régulièrement, y compris près de la moitié (48 %) qui le font « toujours » lorsqu'elles sont avisées que des mises à jour sont disponibles. Relativement peu de répondants (11 %) installent « parfois » des mises à jour sur leurs appareils, et presque personne (1 %) n'a déclaré le faire que « rarement ».

Diagramme 7 : Fréquence de l'installation des plus récentes mises à jour de logiciels et d'applications



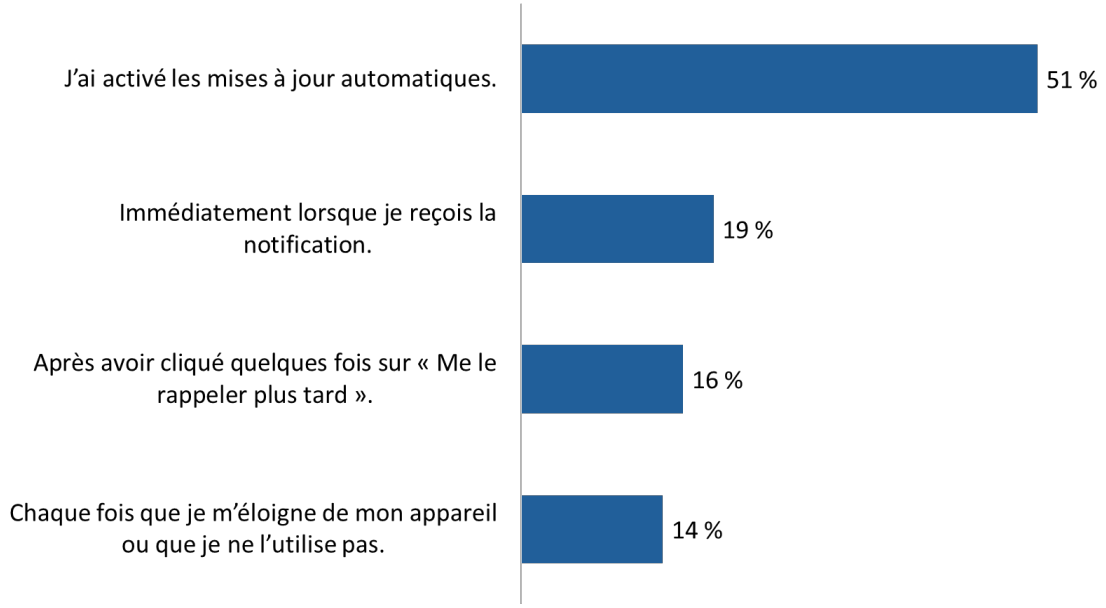
QBEH3. À quelle fréquence installez-vous les dernières mises à jour et versions des logiciels après avoir été avisé(e) qu'elles sont disponibles? Base de référence : n=1 813; répondants qui savent comment installer les plus récentes mises à jour de logiciels et d'applications.

La probabilité d'installer « toujours » les plus récentes mises à jour de logiciels ou d'applications après avoir reçu une notification augmente généralement avec l'âge et le revenu annuel du ménage. Elle est plus élevée chez les personnes possédant un niveau avancé de connaissances en matière de sécurité en ligne. La génération Z est la moins susceptible de toujours installer des mises à jour. De plus, les parents ont moins tendance que les autres personnes à toujours installer des mises à jour lorsqu'ils reçoivent une notification.

Sept Canadiens et Canadiennes en ligne sur 10 installent les mises à jour immédiatement.

Parmi les personnes qui installent « souvent » des mises à jour de logiciels sur leurs appareils (n=1 800), sept sur 10 (70 %) installent ces mises à jour immédiatement. Plus précisément, 51 % ont activé les mises à jour automatiques et 19 % installent les mises à jour immédiatement après avoir reçu une notification. Parmi les autres, 16 % n'installent les mises à jour qu'après avoir cliqué sur « me rappeler plus tard » à quelques reprises et 14 % ne le font que lorsqu'elles sont loin de leur appareil ou ne l'utilisent pas.

Diagramme 8 : Installation typique des mises à jour de logiciels



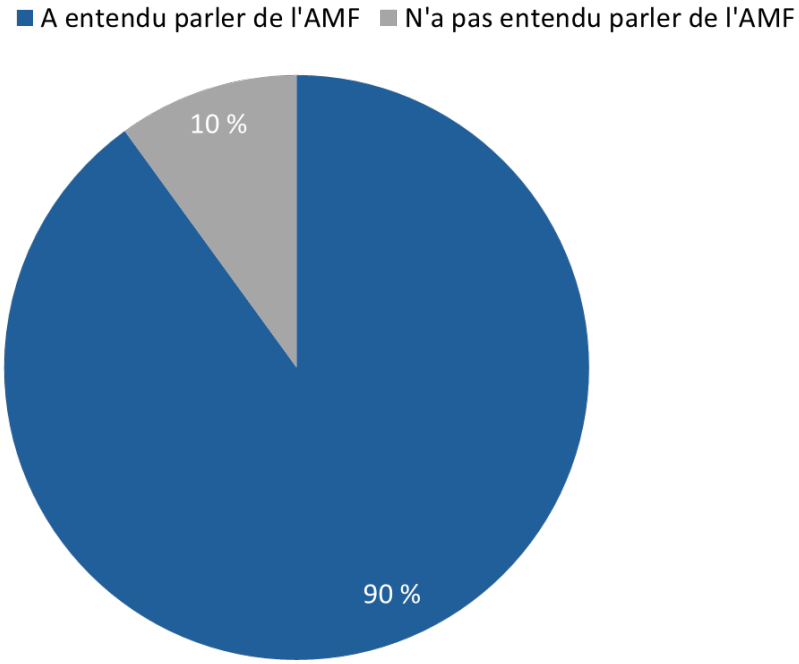
QBEH4. Quand installez-vous généralement les mises à jour sur vos appareils? Base de référence : n=1 800; répondants qui installent souvent les mises à jour.

Les différences de comportement fondées sur l'âge sont évidentes. Plus précisément, plus l'âge augmente, plus il est probable que les Canadiens et Canadiennes en ligne aient activé les mises à jour automatiques. En revanche, les personnes âgées de 18 à 34 ans sont plus susceptibles que celles de 35 ans et plus d'installer les mises à jour après avoir utilisé la fonction « me le rappeler plus tard » à quelques reprises ou chaque fois qu'elles s'éloignent de leur appareil ou qu'elles ne l'utilisent pas. Les membres de la génération Z ont plus tendance à dire qu'ils installent des mises à jour seulement après avoir cliqué sur « me rappeler plus tard » à quelques reprises.

Neuf Canadiens et Canadiennes en ligne sur 10 connaissent l'AMF et l'utilisent régulièrement.

Neuf personnes sur 10 (90 %) ont entendu parler de l'authentification multifactorielle (AMF), aussi connue sous le nom d'authentification à deux facteurs ou de vérification en deux étapes.

Diagramme 9 : Connaissance de l'AMF

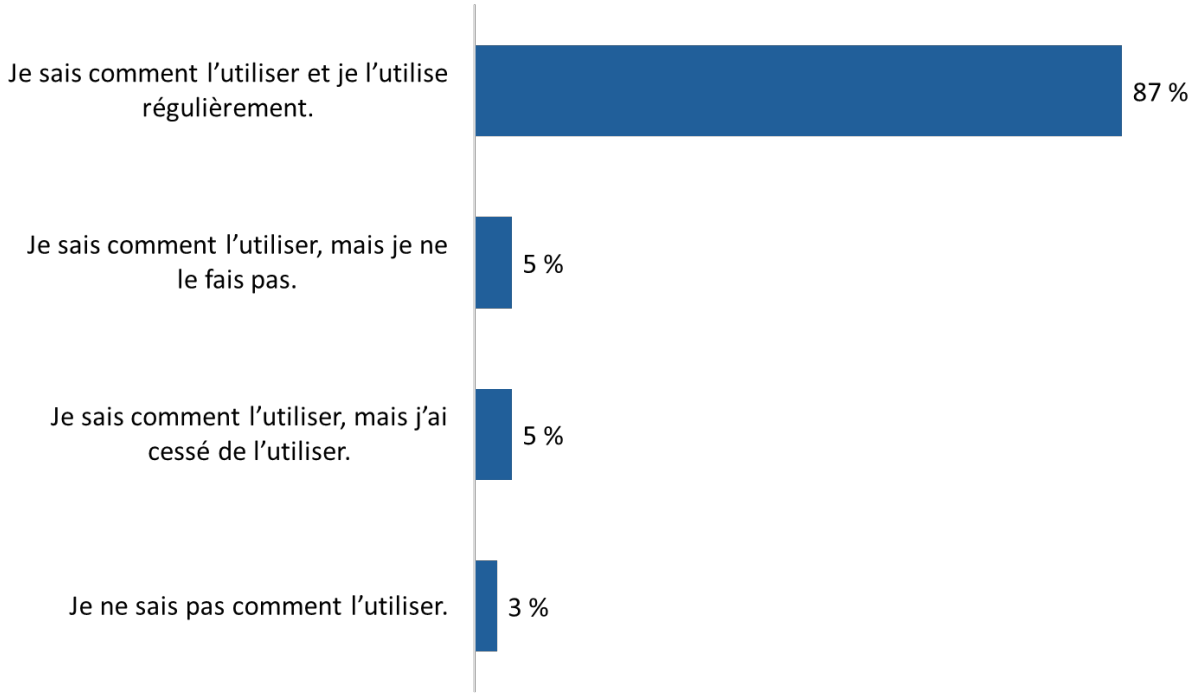


QBEH6. Avez-vous déjà entendu parler de l'authentification multifactorielle (AMF)? On l'appelle également l'authentification à deux facteurs ou la vérification en deux étapes. Base de référence : n=2 222; tous les répondants.

Les résidents du Québec sont plus susceptibles de déclarer n'avoir *jamais* entendu parler de l'AMF. Plus le niveau de scolarité et le revenu annuel du ménage sont élevés, plus les gens ont tendance à savoir ce que c'est. Il en va de même pour les jeunes Canadiens et Canadiennes et les parents. La probabilité de *ne pas* savoir ce qu'est l'AMF est plus élevée chez les personnes qui possèdent des connaissances de base en matière de sécurité en ligne.

Chez les personnes qui savent ce qu'est l'AMF (n=1 987), la plupart d'entre elles (87 %) savent comment l'utiliser et le font régulièrement. De plus, 10 % savent comment utiliser l'AMF, mais ne le font pas (5 %) ou ont cessé de le faire (5 %). Très peu (3 %) ont déclaré ne pas savoir comment utiliser l'AMF.

Diagramme 10 : Capacité à utiliser l'AMF



QBEH7. Vous avez indiqué avoir entendu parler de l'authentification multifactorielle (AMF). Savez-vous comment l'utiliser? Base de référence : n=1 987; répondants ayant entendu parler de l'AMF.

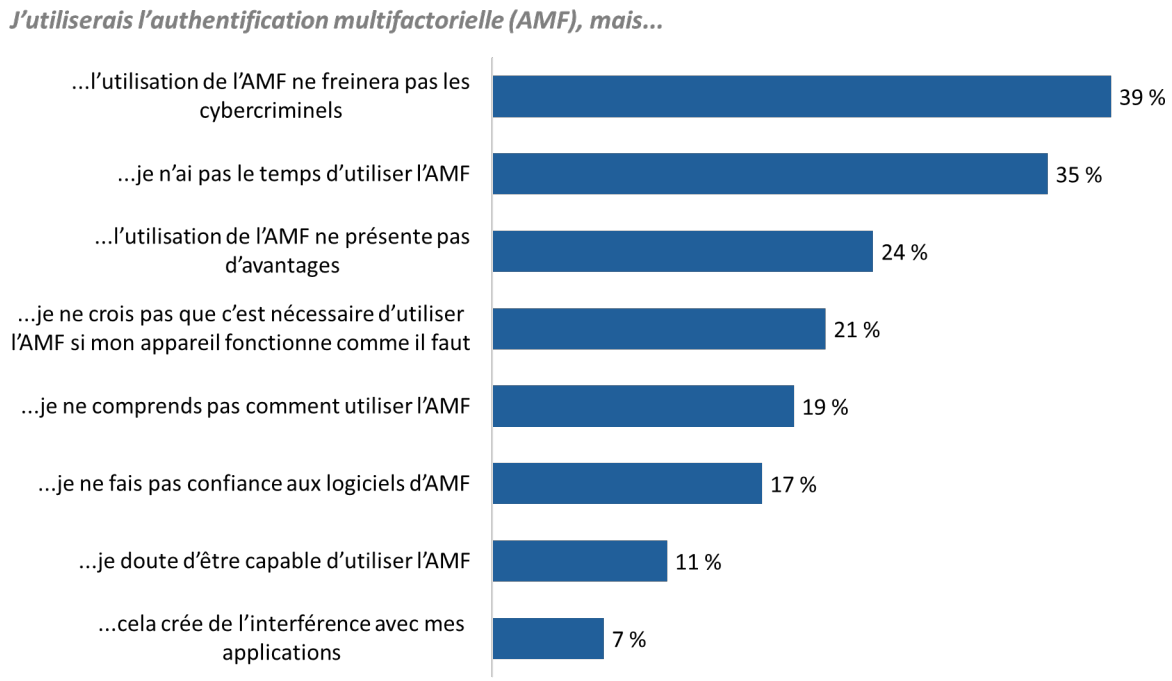
Les personnes âgées de 18 à 34 ans et de 35 à 44 ans sont plus susceptibles que celles de 65 ans et plus de savoir comment utiliser l'AMF et de s'en servir régulièrement. De plus, à mesure que le niveau de scolarité et le revenu du ménage augmentent, la probabilité de savoir comment utiliser l'AMF et de s'en servir régulièrement s'accroît également. Les Canadiens ayant un niveau avancé de connaissances en matière de sécurité en ligne sont plus susceptibles de savoir comment utiliser l'AMF et de le faire régulièrement.

L'inutilité et le manque de temps sont les principales raisons invoquées pour ne pas utiliser régulièrement l'AMF.

Les personnes qui n'utilisent pas régulièrement l'authentification multifactorielle (n=255) ne croient pas que cela freinera les cybercriminels (39 %) ou n'ont pas le temps de l'utiliser (35 %). Un quart (24 %) ne voient aucun avantage à utiliser l'authentification multifactorielle, tandis que deux personnes sur 10 considèrent qu'elle n'est pas nécessaire si leur appareil fonctionne (21 %) ou ne comprennent pas comment l'utiliser (19 %). En outre, 17 % ne font pas confiance aux logiciels d'authentification multifactorielle, 11 % n'ont aucune confiance en leur capacité à l'utiliser et 7 % pensent que de tels logiciels nuisent à leurs applications et craignent qu'ils ne « brisent » leur appareil.

On a demandé aux répondants d'indiquer dans quelle mesure ils étaient d'accord ou en désaccord avec divers énoncés sur l'AMF à l'aide d'une échelle de 10 points, où 1 signifie « fortement en désaccord » et 10, « fortement d'accord ». Le graphique ci-dessous présente le pourcentage de répondants qui étaient d'accord avec chaque énoncé (cotes de 7 à 10 sur l'échelle).

Diagramme 11 : Raisons de ne pas utiliser régulièrement l'AMF



QBEH9a-j. Veuillez indiquer à quel point vous êtes d'accord avec les énoncés suivants : « J'utiliserais l'authentification multifactorielle (AMF), mais… ». Base de référence : n=255; répondants qui n'utilisent pas régulièrement l'AMF.

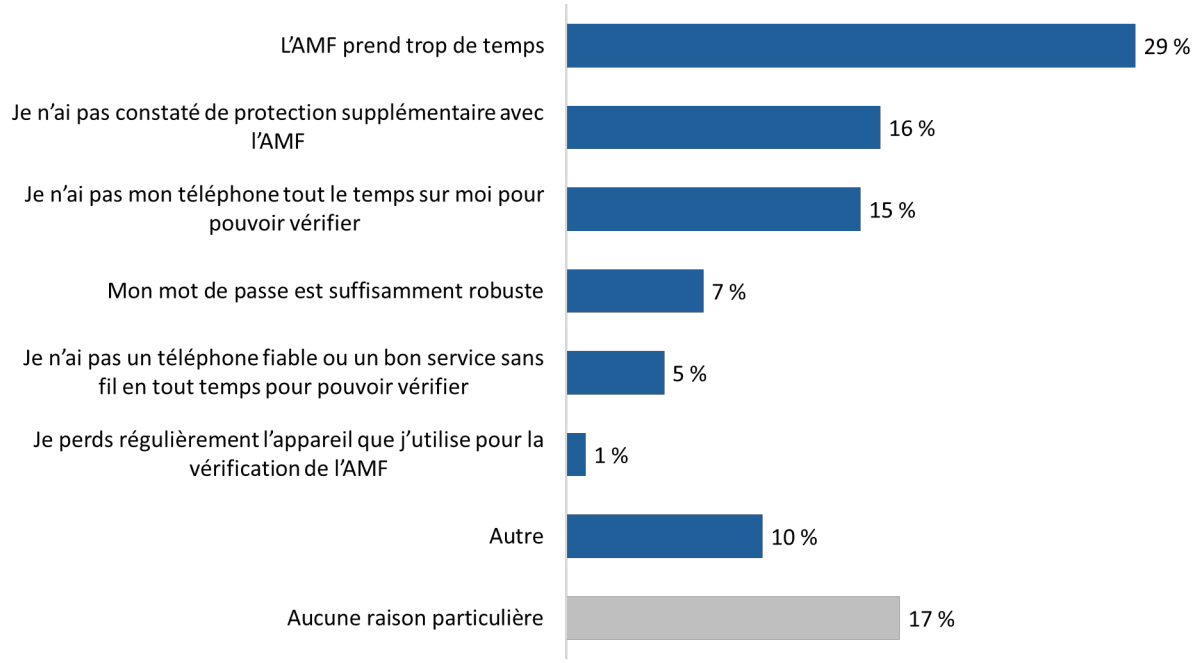
Diverses raisons ont été invoquées pour ne pas (ou ne plus) utiliser l'AMF.

Les personnes qui n'utilisent pas, ou n'utilisent plus, l'authentification multifactorielle (n=194) ont invoqué plusieurs raisons. La plus grande proportion de répondants (29 %) a indiqué que l'authentification multifactorielle prend trop de temps. Par ailleurs, 16 % ne pensent pas que l'authentification multifactorielle confère une protection supplémentaire, et 15 % n'ont pas leur téléphone avec eux en tout temps, ce qui est une exigence pour l'utilisation de l'authentification multifactorielle.

Parmi les raisons invoquées par de plus petites proportions de répondants, mentionnons la perception que leur mot de passe est suffisamment robuste (7 %), qu'ils n'ont pas de téléphone fiable ou de service sans fil fiable en tout temps (5 %) et qu'ils perdent régulièrement l'appareil configuré pour l'authentification multifactorielle (1 %).

Près de deux personnes sur 10 (17 %) n'ont aucune raison en particulier de ne pas utiliser (ou de ne plus utiliser) l'authentification multifactorielle.

Diagramme 12 : Raisons de ne pas utiliser l'AMF



QBEH8. Quelle est la principale raison pour laquelle vous n'utilisez pas (ou que vous avez cessé d'utiliser) l'authentification multifactorielle (AMF)? Base de référence : n=194; répondants qui savent comment utiliser l'AMF, mais qui choisissent de ne pas le faire.

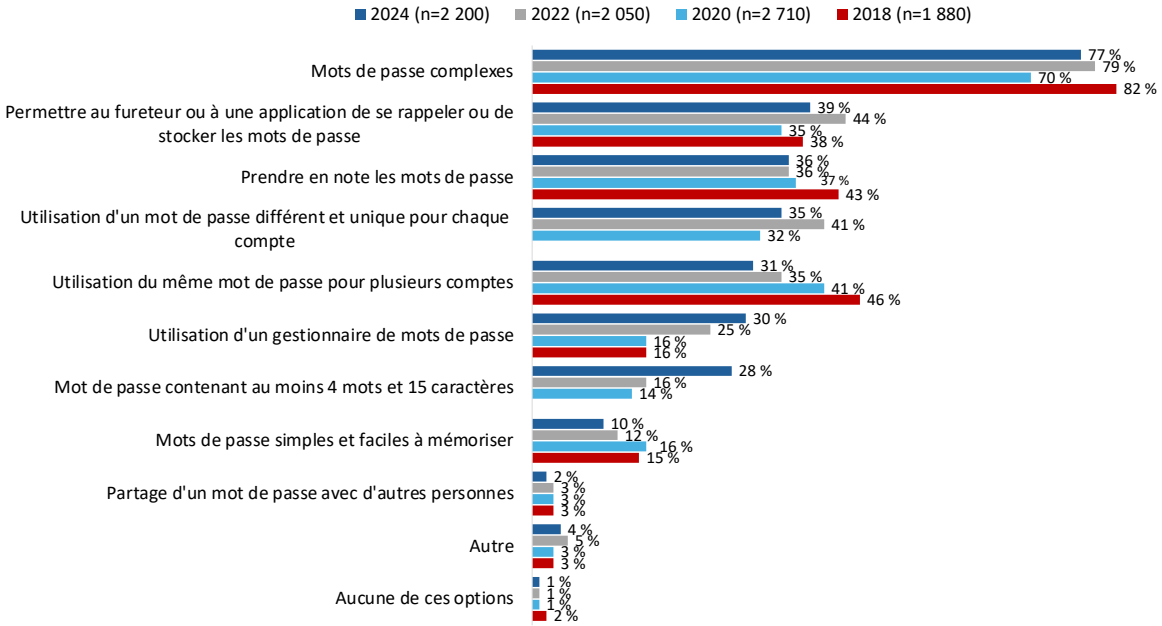
Les trois quarts des Canadiens et des Canadiennes optent pour des mots de passe complexes.

En ce qui concerne leurs mots de passe, un peu plus des trois quarts (76 %) des Canadiens et des Canadiennes choisissent des mots de passe complexes en utilisant une combinaison de lettres, de chiffres et de symboles. De plus, 35 % (contre 41 % en 2022) se servent d'un mot de passe différent et unique pour chaque compte, 30 % (contre 25 % en 2022) font appel à un gestionnaire de mots de passe et 27 % (contre 16 % en 2022) utilisent un mot de passe ayant entre quatre et 15 caractères.

D'autres répondants prennent des mesures qui *pourraient* mettre leur compte en danger : 39 % (contre 44 % en 2022) permettent aux navigateurs ou aux applications de « se souvenir » ou d'inscrire automatiquement leurs mots de passe, 36 % prennent en note leurs mots de passe, 31 % (contre 35 % en 2022) utilisent le même mot de passe pour plusieurs comptes, 10 % ont des mots de passe simples et faciles à retenir et 2 % divulguent leur mot de passe.

Si l'on compare d'une année à l'autre, la plus grande proportion de Canadiens et de Canadiennes en ligne continue d'opter pour des mots de passe complexes. De plus, cette année, un moins grand nombre de personnes en ligne permettent aux navigateurs ou aux applications de se souvenir de leurs mots de passe et utilisent le même mot de passe pour plusieurs comptes, tandis que beaucoup plus de gens se servent d'un mot de passe contenant entre 4 et 15 caractères.

Diagramme 13 : Mesures prises concernant les mots de passe



QBEH15. Lorsque vient le temps de choisir vos mots de passe, lesquelles des mesures suivantes prenez-vous? [Plusieurs réponses acceptées.] Base de référence : tous les répondants; n=2 200. Ne sait pas : 1 %.

Les différences fondées sur l'âge sont prononcées et suivent une tendance claire. Les personnes âgées de 18 à 44 ans sont plus susceptibles que les répondants plus âgés de permettre à leur navigateur ou à leur application de se souvenir ou de stocker leur mot de passe, de faire appel à un gestionnaire de mots de passe, de se servir du même mot de passe pour plusieurs comptes, d'utiliser un mot de passe contenant entre 4 et 15 caractères et d'opter pour des mots de passe complexes avec une combinaison de lettres, de chiffres et de symboles. Les personnes âgées de 65 ans et plus étaient *plus* susceptibles d'avoir pris en note leur mot de passe.

En ce qui concerne le genre, les hommes sont plus susceptibles que les femmes d'utiliser un gestionnaire de mots de passe et des mots de passe uniques, tandis que les femmes ont plus tendance à garder leurs mots de passe simples et faciles à retenir, à utiliser le même mot de passe pour plusieurs comptes, à prendre en note leurs mots de passe et à permettre aux navigateurs ou aux applications de stocker leurs mots de passe.

Voici d'autres différences notables entre les sous-groupes :

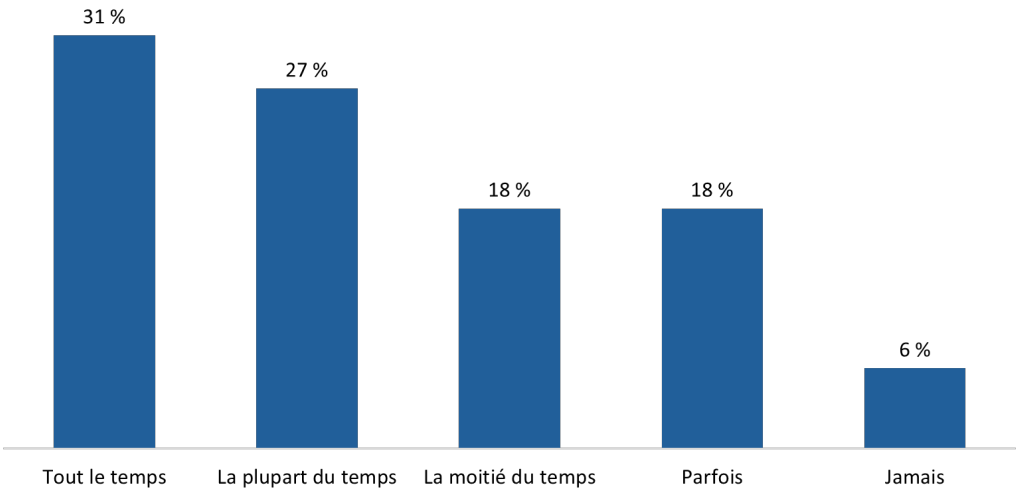
- La probabilité de faire appel à un gestionnaire de mots de passe augmente avec le revenu du ménage.
- Les diplômés universitaires sont plus susceptibles d'adopter des pratiques exemplaires pour assurer la sécurité des mots de passe : mots de passe complexes, mots de passe de 4 à 15 caractères, mots de passe uniques pour chaque compte et gestionnaires de mots de passe.
- Les parents sont plus enclins que les personnes sans enfants de moins de 18 ans à utiliser un mot de passe de 4 à 15 caractères, mais ils sont moins susceptibles que leurs homologues d'utiliser un mot de passe différent pour chaque compte.

- L'utilisation d'un gestionnaire de mots de passe est plus élevée en Ontario que dans le Canada atlantique et au Québec.

La moitié des Canadiens et des Canadiennes utilisent des mots de passe uniques la plupart du temps.

La moitié des personnes en ligne utilisent des mots de passe uniques pour leurs comptes en ligne importants « tout le temps » (31 %) ou « la plupart du temps » (27 %). De plus, un tiers le font « la moitié du temps » (18 %) ou une « parfois » (18 %). Très peu (6 %) ont déclaré ne pas utiliser de mots de passe uniques.

Diagramme 14 : Utilisation de mots de passe uniques



QBEH17. À quelle fréquence utilisez-vous des mots de passe uniques pour vos comptes en ligne importants? Base de référence : n=2 222; tous les répondants.

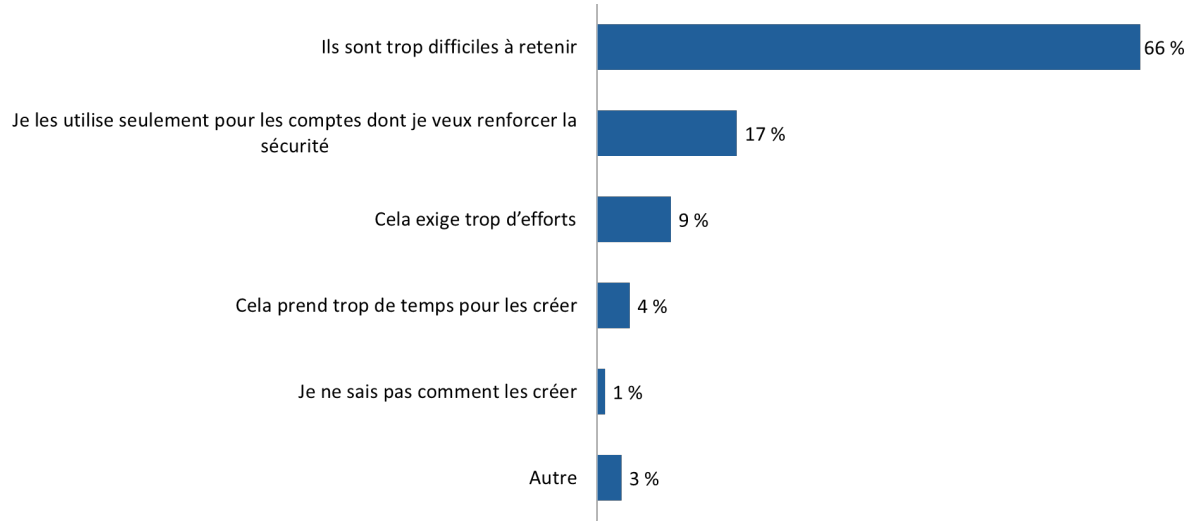
Les personnes âgées de 45 ans et plus sont plus susceptibles que les Canadiens et Canadiennes de 18 à 34 ans de dire qu'ils utilisent des mots de passe uniques « tout le temps » ou « la plupart du temps ». La génération Z est la génération la plus encline à utiliser des mots de passe uniques pour ses comptes importants « la moitié du temps ». Les hommes ont plus tendance que les femmes à utiliser des mots de passe uniques « tout le temps ». Les Canadiens détenant au plus un diplôme d'études secondaires sont plus susceptibles de dire qu'ils se servent de mots de passe uniques « parfois » pour leurs comptes en ligne importants. Les personnes qui possèdent un niveau avancé de connaissances en matière de sécurité en ligne sont plus enclines à utiliser des mots de passe uniques « tout le temps ».

La longueur des mots de passe varie, les deux tiers des répondants déclarant utiliser entre sept et huit caractères (20 %) ou entre 9 et 11 caractères (47 %). Parmi les autres personnes, un tiers optent pour des mots de passe plus longs (26 % utilisent des mots de passe de 12 à 15 caractères et 7 % choisissent des mots de passe de plus de 16 caractères). Pour se souvenir de plusieurs mots de passe, environ un quart d'entre eux les écrivent dans un bloc-notes (23 %) ou font appel à une application de gestion de mots de passe, telle que 1Password, LastPass ou iCloud Keychain (24 %). Une personne sur cinq (21 %) a déclaré se souvenir de son mot de passe sans le prendre en note.

Les Canadiens et les Canadiennes réutilisent les mots de passe principalement pour éviter de devoir s'en souvenir.

Les deux tiers (66 %) des personnes qui utilisent rarement, voire jamais, des mots de passe uniques pour leurs comptes en ligne (n=512) disent qu'elles ont de la difficulté à se souvenir de mots de passe différents. D'autres sont d'avis que cela exige trop d'efforts (9 %), que cela prend trop de temps (4 %) ou qu'elles ne savent pas comment les créer (1 %). Dix-sept pour cent n'utilisent des mots de passe uniques que pour des comptes particuliers où il est préférable d'accroître la sécurité.

Diagramme 15 : Raisons de ne pas utiliser des mots de passe uniques

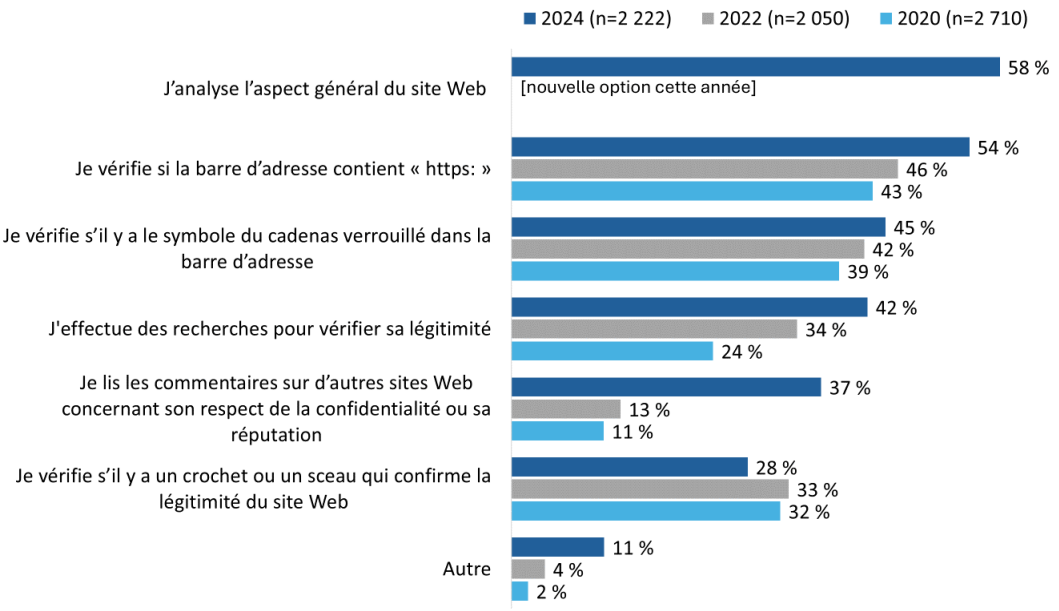


QBEH18. Vous avez indiqué que vous utilisez rarement des mots de passe uniques pour vos comptes en ligne ou que vous n'en utilisez jamais? Base de référence : n=512; répondants qui ne créent pas de mots de passe uniques.

Les Canadiens et Canadiennes en ligne misent sur plusieurs stratégies pour vérifier la légitimité d'un site Web.

Pour vérifier la légitimité d'un site Web, un peu plus de la moitié des Canadiens et Canadiennes en ligne analysent l'aspect général du site Web (58 %) ou vérifient si « https » figure dans la barre d'adresse (54 %, ce qui représente une hausse par rapport à 46 % en 2022). Environ quatre personnes sur 10 regardent si la barre d'adresse du site Web contient le symbole du cadenas verrouillé (45 % contre 42 % en 2022), mènent des recherches pour vérifier la légitimité du site Web (42 % contre 34 % en 2022) ou lisent des commentaires sur la protection des renseignements personnels ou la réputation du site Web (37 % contre 13 % en 2022). Un peu plus du quart vérifient s'il y a un crochet ou un sceau qui confirme la légitimité du site Web (28%, ce qui constitue une baisse par rapport à 33 % en 2022).

Diagramme 16 : Mesures pour vérifier la sécurité d'un site Web



QBEH12. Quelles mesures prenez-vous pour vérifier la légitimité d'un SITE WEB? [Plusieurs réponses acceptées.] Base de référence : tous les répondants.

Les Canadiens et Canadiennes de moins de 65 ans sont plus susceptibles que les personnes de 65 ans et plus d'avoir pris toutes les mesures énumérées pour vérifier la légitimité d'un site Web. Les différences entre les genres ne ressortent que pour deux mesures : les hommes ont plus tendance que les femmes à mener leurs propres recherches pour vérifier la légitimité d'une page Web et à vérifier la présence de l'élément « https ». Parmi les différences régionales notables, mentionnons les suivantes : les personnes du Québec sont *plus* susceptibles de s'assurer de la présence du symbole du cadenas et plus enclines que celles du Canada atlantique et de la Colombie-Britannique à vérifier si « https » figure dans la barre d'adresse. Les personnes qui possèdent un niveau avancé de connaissances en matière de sécurité en ligne et celles qui sont toujours branchées à Internet ont plus tendance à prendre toutes ces mesures pour vérifier la légitimité d'un site Web.

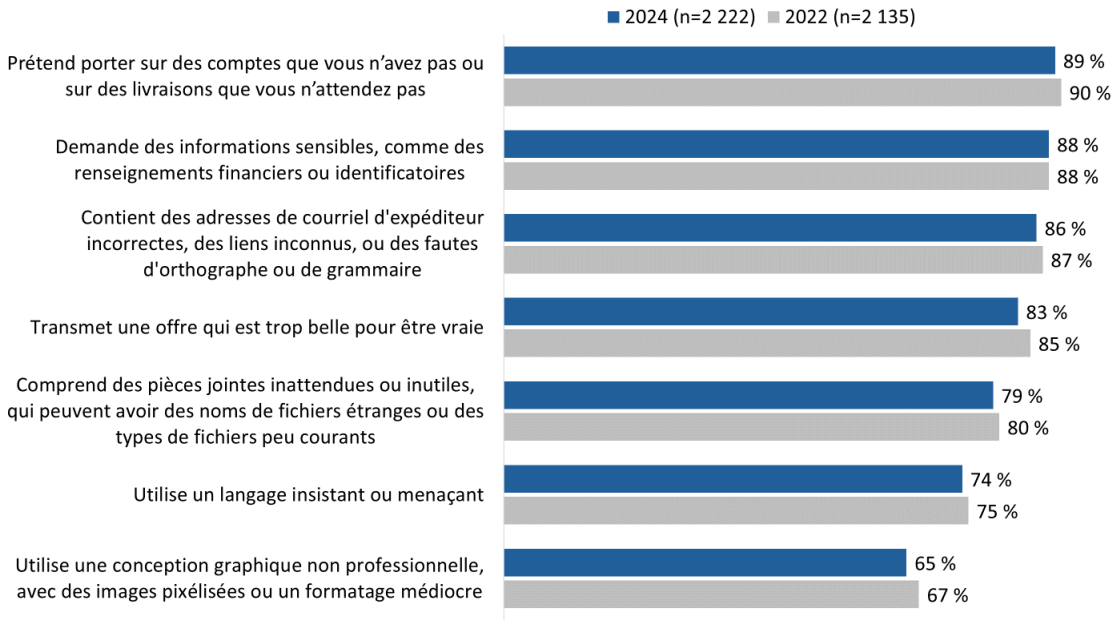
Si l'on établit des comparaisons d'une année à l'autre, on observe en général qu'un plus grand nombre de Canadiens et de Canadiennes en ligne déclarent adopter certaines mesures pour vérifier la légitimité des sites Web. Plus précisément, la proportion des personnes qui mènent leurs propres recherches est passée de 24 % en 2020 à 34 % en 2022 et à 42 % en 2024. La recherche de commentaires sur d'autres sites Web pour confirmer la réputation a considérablement augmenté, passant de 11 % et 13 % en 2020 et 2022 à 37 % en 2024. La recherche du symbole du cadenas a connu de légères augmentations d'une année à l'autre, passant de 39 % en 2020 à 42 % en 2022 et à 45 % en 2024. Il en va de même pour la proportion de personnes qui vérifient la présence de l'élément « https » (de 43 % en 2020, à 46 % en 2022 et à 54 % en 2024).

La plupart des Canadiens et des Canadiennes en ligne reconnaissent généralement les signes des tentatives d'hameçonnage.

La grande majorité des Canadiens et des Canadiennes en ligne reconnaissent les signes de tentatives d'hameçonnage, y compris les allégations au sujet de comptes qu'ils n'ont pas ou les livraisons inattendues (89 %), les demandes de renseignements sensibles (88 %) et les messages contenant des adresses de courriel incorrectes, des liens inconnus ou des fautes d'orthographe ou de grammaire (86 %). Un nombre presque aussi important de ces personnes reconnaissent que les messages contenant des offres trop belles pour être vraies (83 %) et des pièces jointes inattendues ou inutiles (79 %) sont également des signes de tentatives d'hameçonnage. Les trois quarts (74 %) reconnaissent que l'emploi d'un langage insistant ou menaçant est révélateur d'une tentative d'hameçonnage, tandis que les deux tiers (65 %) trouvent que les messages dont la conception graphique manque de professionnalisme sont une indication d'hameçonnage.

Les résultats du sondage sont pratiquement identiques à ceux de 2022.

Diagramme 17 : Signes d'une tentative d'hameçonnage



QBEH13. D'après ce que vous savez, quels sont les signes d'une tentative d'hameçonnage? [Plusieurs réponses acceptées.] Base de référence : tous les répondants. Ne sait pas : 2 %.

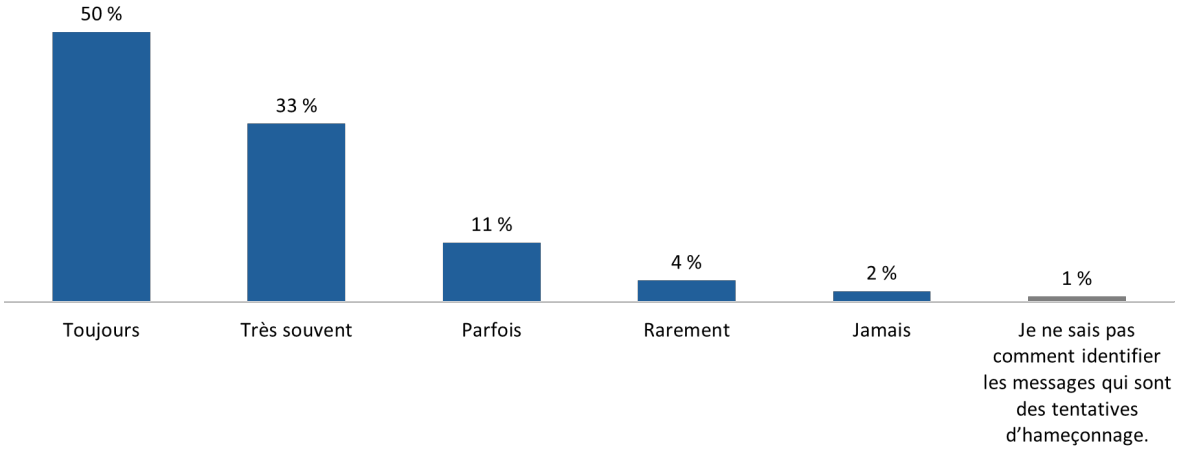
Les Canadiens et Canadiennes en ligne de moins de 45 ans sont plus susceptibles que les personnes plus âgées de désigner tous ces éléments comme des signes potentiels de tentatives d'hameçonnage. À mesure que le niveau de scolarité augmente, la probabilité de les identifier comme tels s'accroît également. De plus, lorsque le revenu du ménage diminue, il en va de même pour la probabilité d'identifier de tels messages comme des signes de tentative d'hameçonnage. Les personnes déclarant gagner moins de 40 000 $ par année ont plus de difficulté à cerner de telles tentatives. Les parents sont plus susceptibles que les personnes sans enfants de signaler que les offres trop belles pour être vraies, les pièces jointes inattendues et la conception graphique non professionnelle représentent des signes d'hameçonnage. Les personnes qui possèdent un niveau

avancé de connaissances en matière de sécurité en ligne et celles qui sont toujours branchées à Internet sont plus susceptibles d'être conscientes de bon nombre de ces signes d'hameçonnage.

La plupart des Canadiens et Canadiennes en ligne vérifient fréquemment les messages pour y détecter des signes d'hameçonnage.

La plupart des Canadiens et Canadiennes en ligne vérifient « toujours » (50 %) ou « très souvent » (33 %) les messages, y compris les courriels, les textes ou les médias sociaux, pour repérer des signes de tentative d'hameçonnage avant de cliquer sur des liens ou de répondre aux messages. De plus, 11 % effectuent parfois une vérification, tandis que très peu (6 %) examinent les messages « rarement » ou « jamais » dans ce but.

Diagramme 18 : Fréquence de la vérification des messages pour détecter les tentatives d'hameçonnage



QBEH14. À quelle fréquence vérifiez-vous les messages (p. ex., courriels, textos ou médias sociaux) pour détecter des tentatives d'hameçonnage avant de cliquer sur un lien ou de répondre au message? Base de référence : tous les répondants; n=2 222.

Les groupes suivants sont plus susceptibles de vérifier « toujours » les messages pour détecter les signes de tentatives d'hameçonnage : les résidents de l'Ontario comparativement au Canada atlantique et au Québec; les hommes; les milléniaux; les personnes dont le revenu annuel du ménage totalise entre 100 000 $ et un peu moins de 150 000 $ comparativement aux personnes dont le revenu annuel est inférieur à 100 000 $; et les diplômés des universités et des collèges. Les personnes qui possèdent un niveau avancé de connaissances en matière de sécurité en ligne et les personnes toujours branchées à Internet sont également plus susceptibles de toujours vérifier les messages pour y détecter des signes de tentatives d'hameçonnage.

La cybercriminalité et les menaces

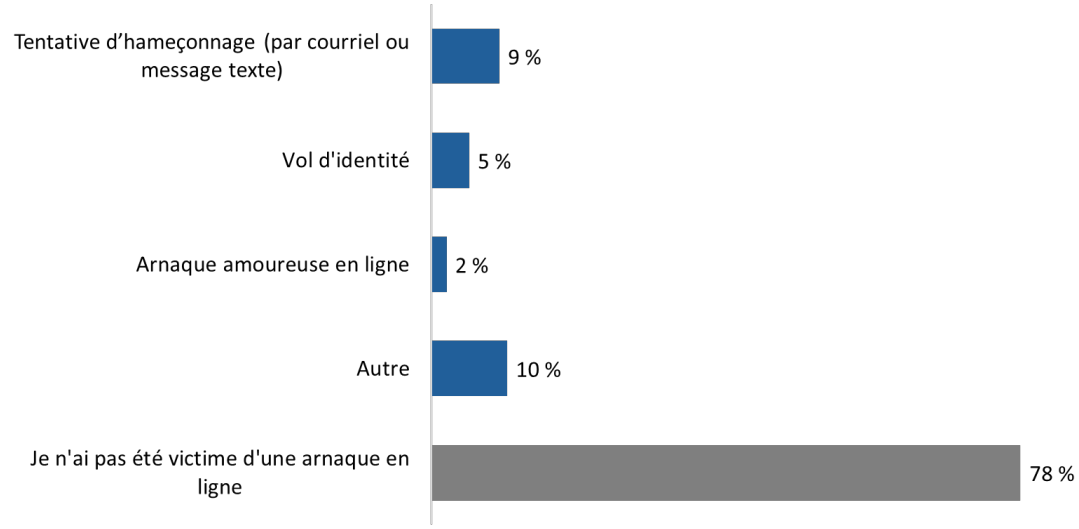
La plupart des Canadiens et Canadiennes n'ont jamais été victimes d'arnaques en ligne.

Plus des trois quarts (78 %) des répondants n'ont jamais été victimes d'une arnaque en ligne qui leur a fait perdre de l'argent ou des données. Un nombre de personnes relativement faible n'a pas eu cette chance : 9 % ont déclaré avoir été victimes d'hameçonnage, 5 %, d'un vol d'identité et 2 %, d'une arnaque amoureuse en ligne.

Les descriptions suivantes ont été fournies aux répondants :

- « Hameçonnage » : Les cybercriminels trompent les gens pour qu'ils fournissent des informations ou installent des logiciels malveillants afin de leur voler de l'argent ou des données. Cela se fait souvent via de faux courriels qui semblent provenir d'expéditeurs de confiance, qui encouragent les gens à cliquer sur des liens malveillants vers de faux sites Web ou à ouvrir des pièces jointes malveillantes.
- « Arnaque amoureuse en ligne » : Les fraudeurs adoptent une fausse identité en ligne dans le but de créer l'illusion d'une relation amoureuse ou intime avec la victime pour la manipuler ou la voler. Souvent, les demandes du fraudeur font grandement appel aux émotions, qui dit avoir besoin d'argent pour recevoir des soins médicaux d'urgence ou s'il est à l'étranger, afin de payer les frais de transport à débourser pour venir visiter la victime.
- « Vol d'identité » : Le vol d'identité se produit lorsqu'un fraudeur a accès à suffisamment de renseignements sur l'identité d'une personne (p. ex., son nom, sa date de naissance, son adresse actuelle et ses anciennes adresses) pour recevoir des biens ou des services de façon frauduleuse, comme ouvrir un compte bancaire ou obtenir une carte de crédit ou un prêt.

Diagramme 19 : Fréquence des arnaques en ligne



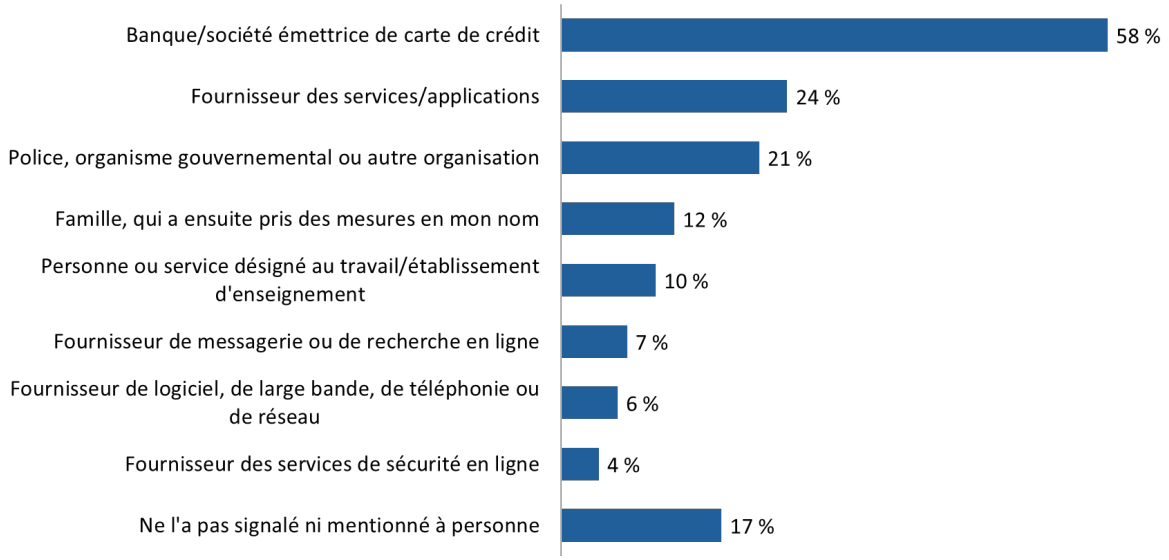
QCCE1. Avez-vous subi personnellement une perte d'argent ou de données à cause d'activités nuisibles en ligne? [Plusieurs réponses acceptées.] Base de référence : n=2 222; tous les répondants.

La probabilité d'être victime d'une escroquerie en ligne, qu'il s'agisse d'hameçonnage, d'une arnaque amoureuse en ligne ou d'un vol d'identité, est plus élevée chez les ménages dont le revenu annuel est inférieur à 40 000 $ que chez les ménages ayant un revenu annuel de plus de 100 000 $.

La plupart des victimes d'une arnaque en ligne l'ont signalée ou mentionnée à quelqu'un.

Plus de huit personnes sur 10 (83 %) ayant été victimes d'une arnaque en ligne (n = 193) l'ont signalée ou mentionnée à quelqu'un. La majorité (58 %) a communiqué avec la banque ou la société émettrice de carte de crédit. En outre, 24 % en ont parlé au fournisseur de services ou d'applications par l'entremise desquels ils ont perdu de l'argent ou des données, et 21 % l'ont signalée à la police ou à un autre organisme gouvernemental pertinent. Douze pour cent l'ont dit à leur famille, qui a ensuite pris des mesures en leur nom. Le diagramme 20 présente toute la gamme des mesures.

Diagramme 20 : Signalement des tentatives d'hameçonnage



QCCE2. Vous avez mentionné avoir subi une perte d'argent ou de données à cause d'une tentative d'hameçonnage. L'avez-vous signalé à quelqu'un? [Plusieurs réponses acceptées.] Base de référence : n=193; répondants ayant été victimes d'hameçonnage.

Les personnes ayant été victimes d'une escroquerie par hameçonnage et qui l'ont déclarée (n=161)[2] l'ont fait pour deux raisons principales : pour éviter que cela leur arrive de nouveau ou que d'autres personnes deviennent des victimes (47 %) ou pour récupérer leur argent (41 %).

Les personnes n'ayant pas signalé l'arnaque par hameçonnage (n=32)[3] ont fait mention notamment des raisons suivantes : elles ne savaient pas à qui le signaler ou comment le faire, elles avaient l'impression qu'il serait inutile de le signaler parce qu'aucune mesure ne serait prise, elles éprouvaient de la honte et elles étaient d'avis que le montant de la perte n'était pas assez important.

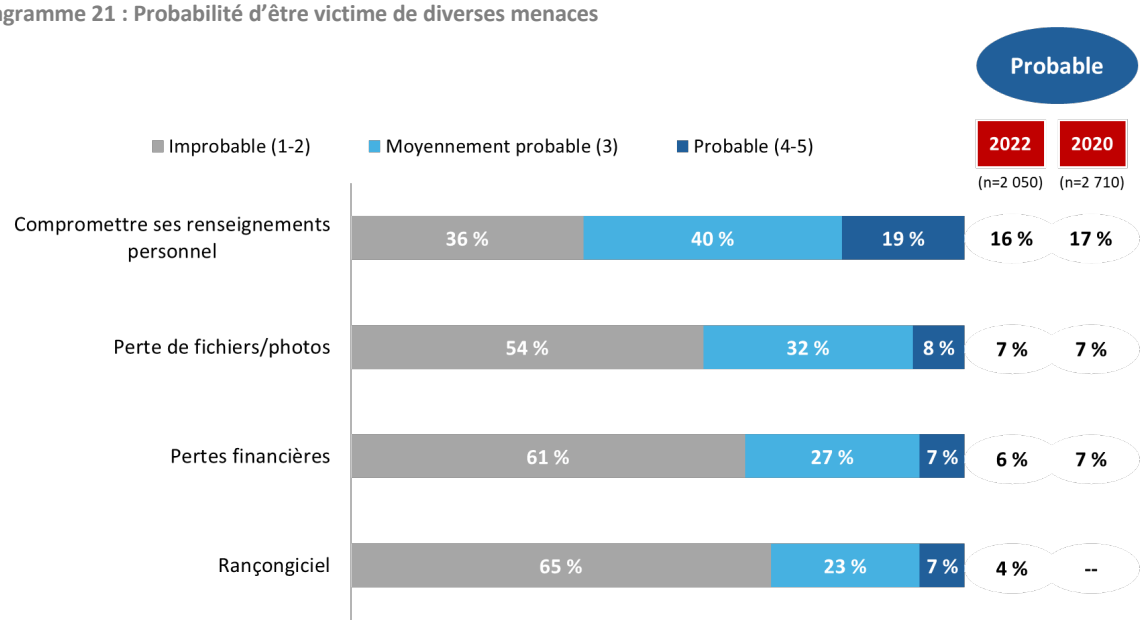
[2] QCCE3. Quelle est la principale raison pour laquelle vous avez signalé une tentative d'hameçonnage? Si vous avez subi une perte d'argent ou de données plus d'une fois, veuillez penser à la plus récente fois où cela s'est produit. Base de référence : répondants ayant signalé une tentative d'hameçonnage.

[3] QCCE4. Quelle est la principale raison pour laquelle vous n'avez pas signalé la tentative d'hameçonnage?

Le quart des Canadiens et des Canadiennes en ligne estiment probable qu'ils soient touchés par une cybermenace.

En hausse par rapport à 8 % en 2022, 24 % des Canadiens en ligne estiment probable qu'ils soient touchés par au moins l'une des quatre cybermenaces au cours de la prochaine année. Deux personnes sur 10 (19 %, soit une hausse par rapport à 16 % en 2022) estiment probable qu'ils soient touchés par une cybermenace pouvant compromettre leurs renseignements personnels. Conformément aux résultats des années précédentes, un nombre relativement faible de répondants croient qu'ils seront confrontés à une menace entraînant la perte de fichiers ou de photos (8 %), des pertes financières (7 %) ou la conservation de leurs données jusqu'au versement d'une rançon (4 %).

Diagramme 21 : Probabilité d'être victime de diverses menaces



QCT1a-d. 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 de référence : n=2 222; tous les répondants. Ne sait pas : 5 % à 6 %.

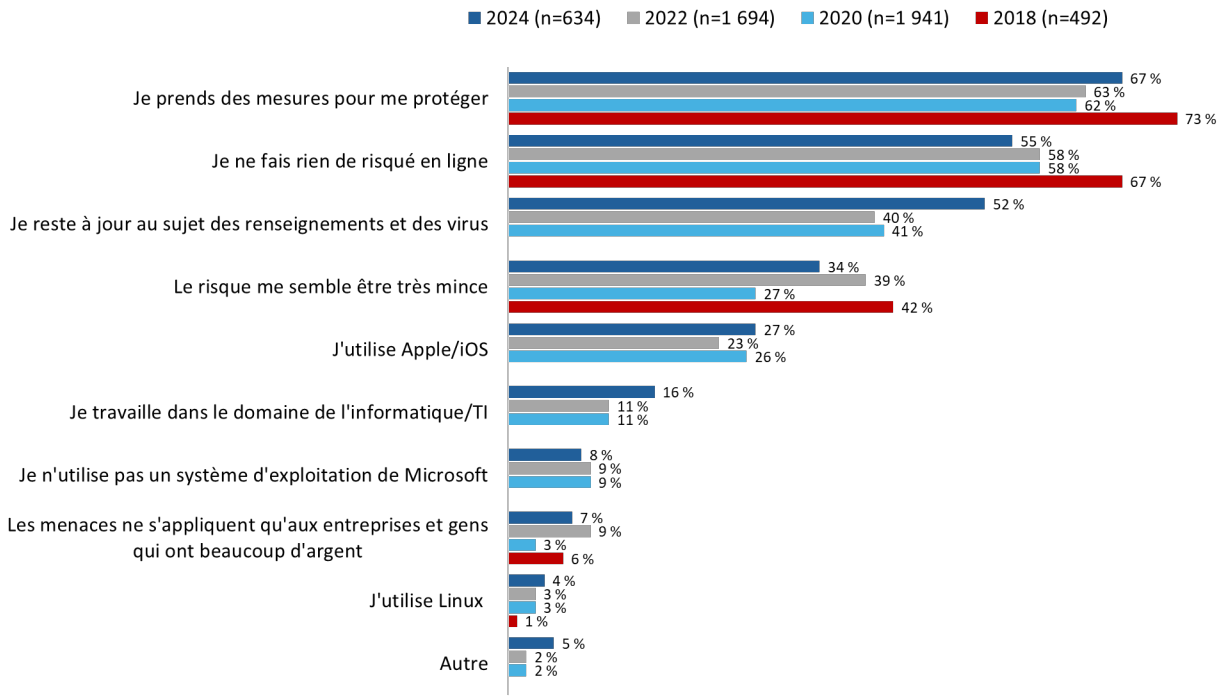
Plus l'âge diminue, plus s'accroît la probabilité de penser qu'on ne sera *pas* touché par l'un de ces quatre types de cybermenaces. La génération Z et la génération Y sont plus susceptibles que les autres générations de penser qu'elles ne seront pas touchées par l'une de ces cybermenaces. Il en va de même pour les personnes ayant un niveau avancé de connaissances en matière de sécurité en ligne.

Les personnes qui pensent qu'il est peu probable qu'elles soient touchées par une cybermenace ont attribué cela aux mesures qu'elles prennent ou à leur comportement en ligne.

La majorité des personnes qui pensent qu'il est peu probable qu'elles soient touchées par une cybermenace (n=634) ont déclaré qu'elles prennent des mesures pour se protéger en ligne (67 %, soit une hausse par rapport à 63 % en 2024), évitent les comportements risqués en ligne (55 %, ce qui représente une baisse par rapport à 58 % en 2022) ou se tiennent à l'affût des dernières nouvelles et des virus (52 %, soit une hausse par rapport à 40 % en 2022). Un tiers des répondants (34 %, soit une baisse par rapport à 39 % en 2022) se sentent peu susceptibles d'être touchés parce

que les risques sont tout simplement très faibles, tandis qu'un peu plus du quart (27 %, une hausse par rapport à 23 % en 2022) pensent qu'ils courent moins de risques parce qu'ils utilisent le système d'exploitation d'Apple qui n'est pas aussi vulnérable face aux virus. Le diagramme 22 présente toute la gamme des raisons.

Diagramme 22 : Raisons invoquées pour la faible probabilité d'être victime d'une cybermenace



QCT2. Pourquoi ne croyez-vous pas qu'il est probable que vous soyez victime d'une cybermenace? [Plusieurs réponses acceptées.] Base de référence : répondants croyant qu'il est peu probable qu'ils soient victimes d'une cybermenace. Ne sait pas : 1 % à 2 %.

Les répondants plus jeunes (c.-à-d. les personnes âgées de 44 ans et moins), les hommes, ainsi que les diplômés de collèges et d'universités sont plus susceptibles de prendre des mesures pour se protéger. Les personnes âgées de 44 ans et moins ont également plus tendance à dire qu'elles ne font rien de risqué en ligne et que les risques d'être touchées par une cybermenace sont tout simplement faibles.

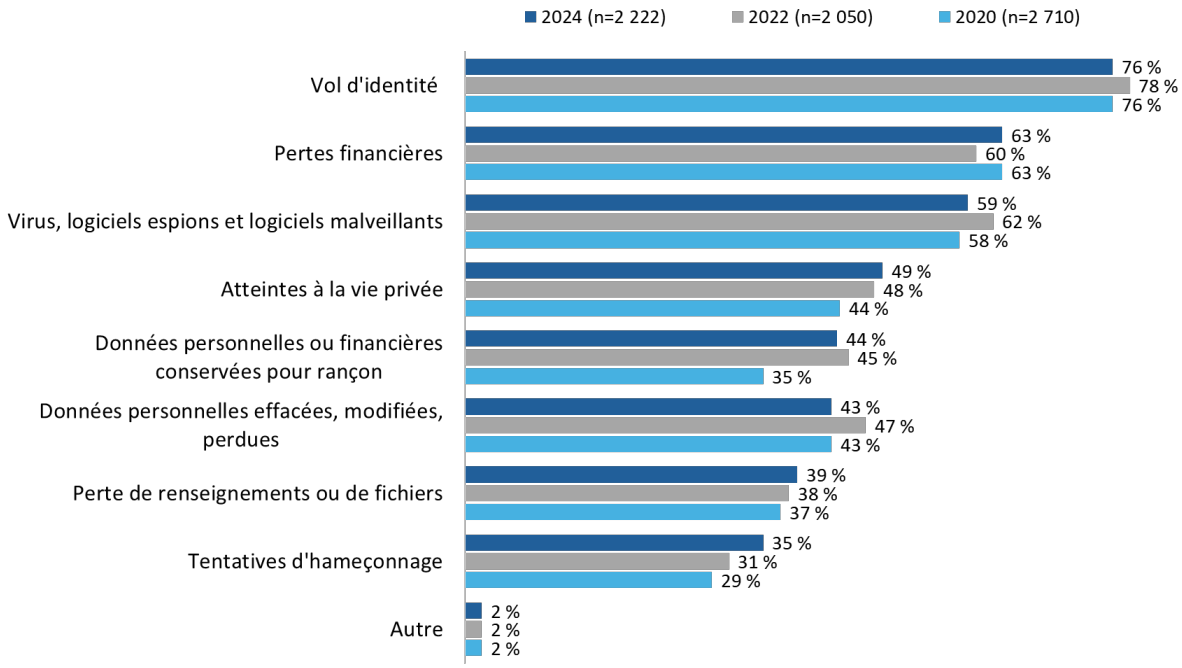
Le vol d'identité, les pertes financières et les logiciels malveillants sont en tête de liste des menaces qui préoccupent les Canadiens et les Canadiennes.

À l'instar des années précédentes, les trois quarts (76 %) des personnes en ligne sont préoccupées par le vol d'identité. De plus, environ six personnes sur 10 s'inquiètent des pertes financières (63 %) ainsi que des virus, des logiciels espions et des logiciels malveillants (59 %). La moitié (49 %) des répondants craignent les atteintes à leur vie privée, 44 % les attaques par rançongiciel, 43 % la perte de données personnelles et 39 % la perte d'informations ou de fichiers. Un peu plus du tiers (35 %) sont préoccupés par les tentatives d'hameçonnage lorsqu'ils pensent aux cybermenaces.

Au fil du temps, la proportion de Canadiens et de Canadiennes en ligne préoccupés par les tentatives d'hameçonnage a augmenté, passant de 29 % en 2020 à 35 % en 2024. Après une légère

augmentation en 2022 (jusqu'à 47 %), la proportion de gens s'inquiétant de la perte de données personnelles a diminué à 43 %. Toutes les autres préoccupations n'ont pas augmenté ou diminué de plus de 3 % entre 2022 et 2024.

Diagramme 23 : Nature de la préoccupation



QCT3. Quels types de cybermenaces vous préoccupent le plus? Base de référence : tous les répondants. Ne sait pas : 2 %.

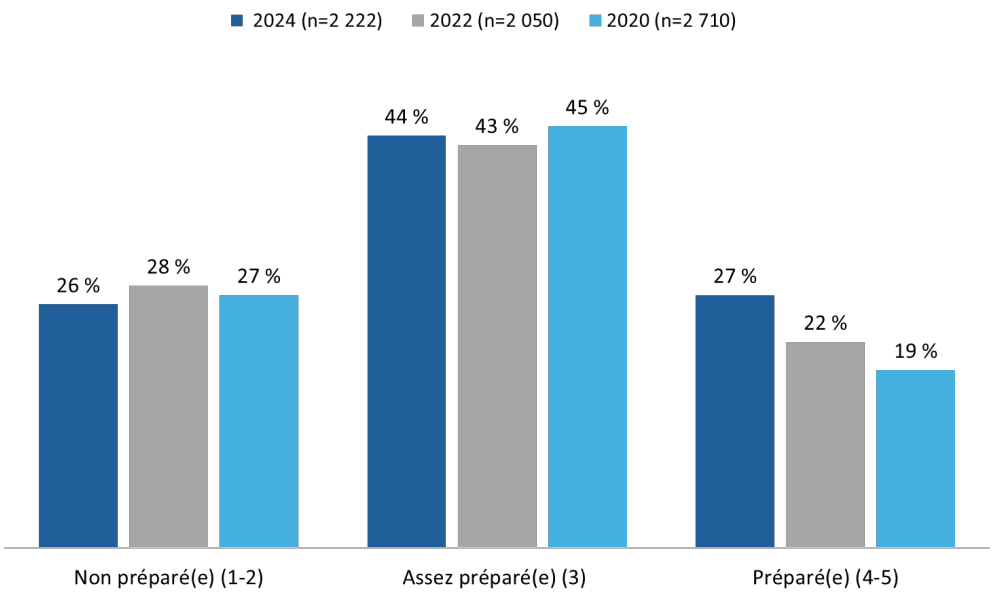
Les différences notables entre les sous-groupes sont les suivantes :

- Les répondants âgés de 45 ans et plus sont plus susceptibles d'être préoccupés par les arnaques par hameçonnage, les virus, les logiciels espions ou les logiciels malveillants, ainsi que le vol d'identité, tandis que les personnes entre 18 et 34 ans craignent davantage les atteintes à leur vie privée.
- La génération Z est susceptible d'être préoccupée par les arnarques par hameçonnage et le vol d'identité, et tout comme les milléniaux, qui sont plus enclins à se soucier des atteintes à la vie privée. Les milléniaux, la génération X et la génération silencieuse ont davantage de préoccupations par rapport aux pertes financières que la génération Z.
- Les personnes au sein de ménages dont le revenu annuel est supérieur à 150 000 $ ont plus tendance à se préoccuper des tentatives d'hameçonnage, tandis que les membres des ménages ayant un revenu annuel inférieur à 40 000 $ sont moins susceptibles d'être préoccupés par le vol d'identité.
- Les préoccupations concernant le vol d'identité et les attaques par rançongiciel augmentent avec les niveaux de scolarité. Les résidents du Québec sont plus susceptibles d'être préoccupés par le vol d'identité.
- Les Canadiens et Canadiennes toujours branchés à Internet ont plus tendance que les utilisateurs qui sont en ligne moins souvent à être préoccupés par la possibilité que leurs données personnelles ou financières soient conservées pour rançon.

Sept personnes sur 10 sont au moins préparées dans une certaine mesure à faire face aux cybermenaces.

La majorité des Canadiens et des Canadiennes en ligne ont déclaré être assez (44 %) ou bien (27 %) préparés à faire face aux cybermenaces. Le quart (26 %) ne se sentent pas préparés. Au fil du temps, la proportion de personnes qui estiment être bien préparées a augmenté, passant de 19 % en 2020 à 22 % en 2022 et à 27 % en 2024.

Diagramme 24 : État de préparation à l'égard des cybermenaces



QCT4. À quel point êtes-vous bien préparé(e) pour faire face aux cybermenaces? Base de référence : tous les répondants. Ne sait pas : 4 %.

Les résidents du Québec sont plus susceptibles que les gens du reste du Canada à s'estimer non préparés à faire face aux cybermenaces. Il en est de même pour les personnes qui gagnent moins de 40 000 $ par année, les femmes, les personnes de 65 ans et plus et les Canadiens et Canadiennes en ligne ayant fait des études secondaires.

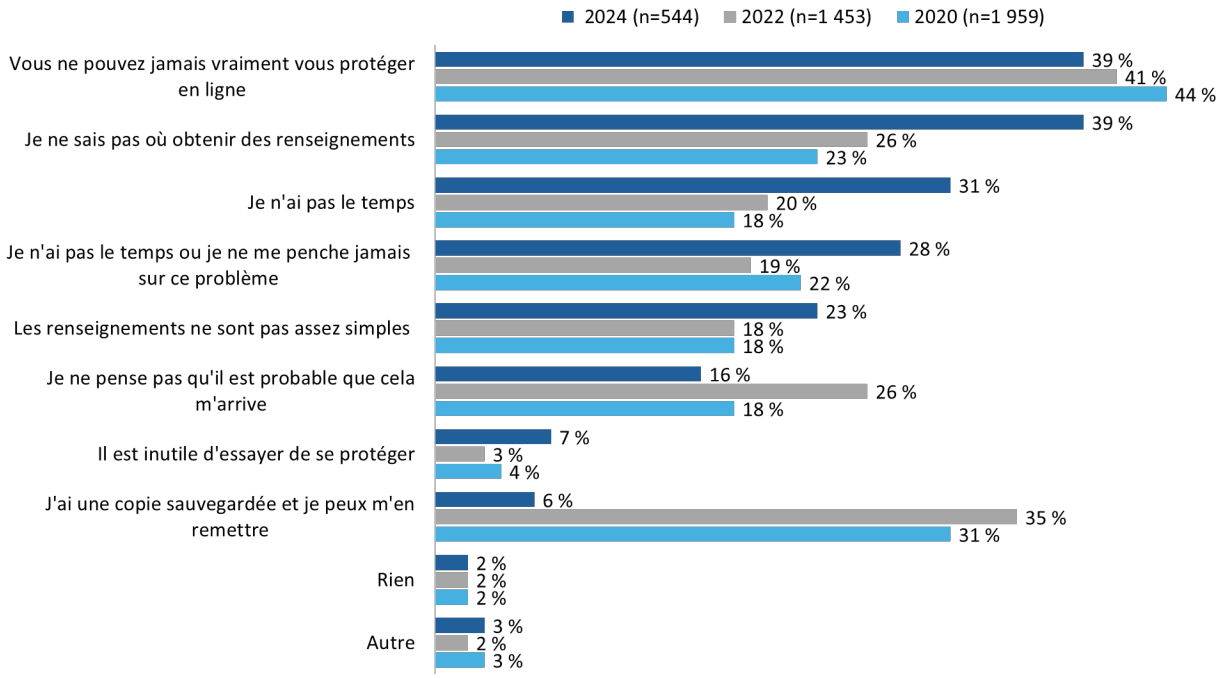
Les raisons expliquant l'absence de préparation pour faire face à une cybermenace varient.

Les personnes qui ne s'estiment pas prêtes à faire face à une cybermenace (n=544) sont plus susceptibles d'invoquer les deux raisons suivantes : la perception qu'on ne peut jamais se protéger en ligne (39 %) et le fait de ne pas savoir où obtenir de l'information (39 %, ce qui représente une hausse par rapport à 26 % en 2022). En outre, environ trois personnes sur 10 ont mentionné un manque de temps (31 %, soit une hausse par rapport à 20 % en 2022) et des connaissances insuffisantes concernant les différents types de menaces (28 %, une hausse comparativement à 19 % en 2022). Près du quart ont déclaré que l'information n'était pas simple (23 %, soit une hausse par rapport à 18 % en 2022). La liste complète des raisons invoquées par les répondants se trouve dans le diagramme 25.

En regroupant les raisons invoquées pour justifier l'absence de préparation, deux thèmes sont ressortis : la futilité (il n'est pas possible de se protéger en ligne) et le manque de connaissances (ne pas savoir où obtenir cette information, ne pas connaître les différentes menaces et ne pas avoir d'information simple à sa disposition).

Au fil du temps, les raisons liées au manque de connaissances ont augmenté de façon constante depuis le sondage de référence en 2020.

Diagramme 25 : Raisons invoquées pour justifier l'absence de préparation afin de faire face aux cybermenaces



QCT5. Pourquoi n'étiez-vous pas bien préparé(e) pour faire face aux cybermenaces? [Plusieurs réponses acceptées.] Base de référence : répondants qui ne sont pas préparés pour faire face aux cybermenaces.

Les répondants âgés de 65 ans et plus sont plus susceptibles que les jeunes Canadiens et Canadiennes en ligne d'attribuer leur manque de préparation à des ressources ou des connaissances insuffisantes. Plus précisément, ils ne se sentent pas préparés parce qu'ils ne savent pas où obtenir ce type d'information ni quelles sont les différentes menaces. Ils trouvent également que l'information à leur disposition n'est pas simple. Les parents sont plus enclins que les personnes sans enfants de moins de 18 ans à dire qu'ils ne sont pas préparés parce qu'ils n'ont pas le temps de prendre des mesures pour se protéger.

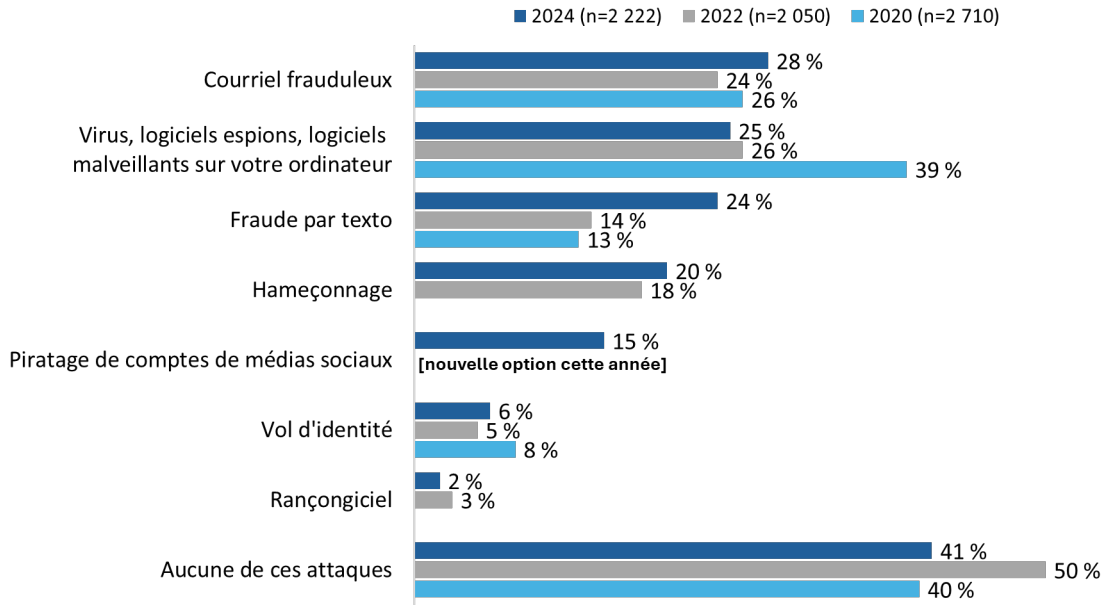
Quatre Canadiens et Canadiennes en ligne sur 10 n'ont jamais été victimes d'une cyberattaque.

Quarante et un pour cent des Canadiens et Canadiennes en ligne ont déclaré qu'ils n'avaient jamais été victimes d'une cyberattaque (il s'agit d'une baisse par rapport à 50 % en 2022). Les victimes d'une cyberattaque ont le plus souvent été touchées par un courriel frauduleux (28 % contre 24 % en 2022), une attaque par un logiciel malveillant sur leur ordinateur (25 %) ou une fraude par texto (24 %, soit une hausse par rapport à 14 % en 2022). Deux personnes sur 10 (20 %) ont été victimes

d'hameçonnage et 15 % ont subi un piratage de compte sur les médias sociaux. Un nombre relativement faible de répondants ont été victimes d'un vol d'identité (6 %) ou d'une attaque par rançongiciel (2 %).

Au fil du temps, la fréquence des courriels frauduleux et des fraudes par texto a augmenté. Pour ce qui est des fraudes par texto, on observe une augmentation considérable. La proportion de Canadiens et de Canadiennes en ligne ayant été victimes d'une attaque par un virus, un logiciel espion ou un logiciel malveillant sur leur ordinateur continue d'être inférieure à celle du sondage de référence, alors que 39 % des répondants déclaraient avoir été victimes d'une telle attaque.

Diagramme 26 : Victime de cyberattaques



QCT6. Avez-vous déjà été victime de l'une des cyberattaques suivantes? Base de référence : tous les répondants. Ne sait pas : 5 %.

Les résidents du Québec sont plus susceptibles que les personnes vivant ailleurs au pays d'avoir été victimes d'un courriel frauduleux. La probabilité d'être victime d'une telle arnaque et d'hameçonnage est plus élevée chez les personnes âgées de 65 ans et plus. Les femmes sont plus nombreuses que les hommes à avoir été victimes d'un courriel frauduleux ou d'une fraude par texto et d'un piratage de compte sur les médias sociaux. Les hommes sont plus susceptibles d'avoir été victimes d'une attaque au moyen d'un virus, d'un logiciel espion ou d'un logiciel malveillant et d'un vol d'identité. Les Canadiens et Canadiennes ayant un niveau avancé de connaissances en matière de sécurité en ligne avaient plus tendance à n'avoir jamais été victimes d'une cyberattaque.

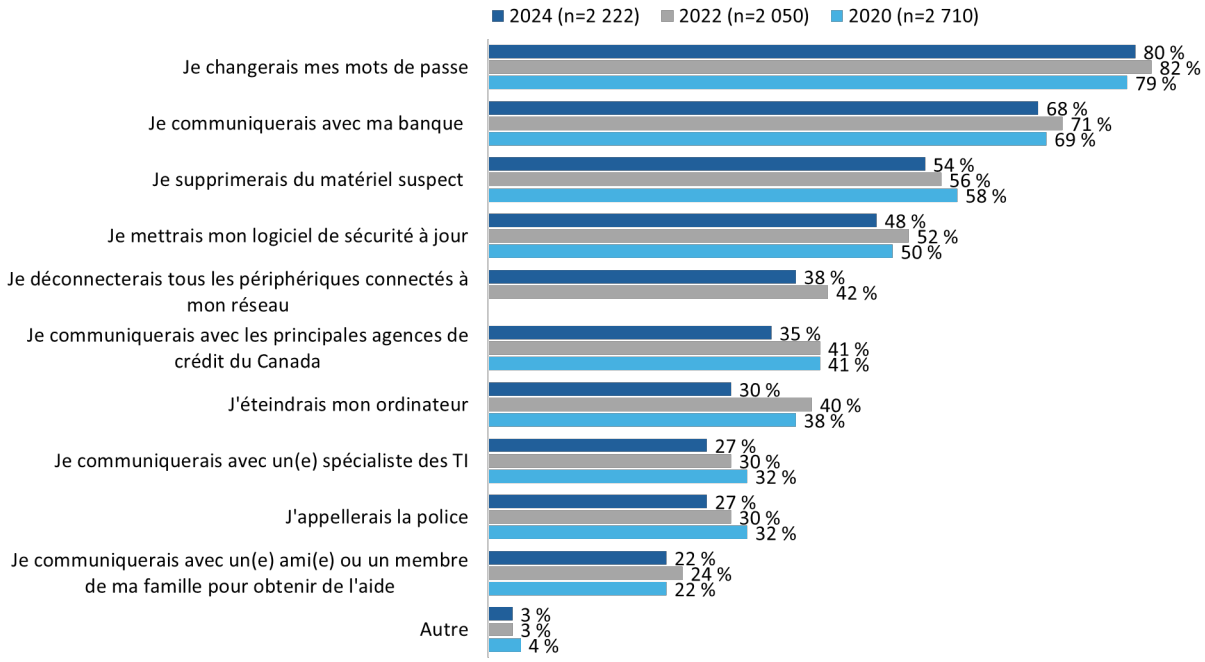
Changer de mot de passe, communiquer avec la banque et supprimer le matériel suspect sont les principales mesures prises en cas de cyberattaque.

Si les répondants savaient ou soupçonnaient qu'ils ont été victimes d'une cyberattaque, la majorité d'entre eux changeraient leurs mots de passe (80 %), communiqueraient avec leur banque (68 %) et supprimeraient le matériel suspect (54 %). Près de la moitié (48 %) mettraient à jour leur logiciel de sécurité, 38 % déconnecteraient tous les périphériques de leur réseau, 35 % communiqueraient avec les principales agences de crédit du Canada et 30 % éteindraient leur ordinateur. Un peu plus

du quart d'entre eux communiqueraient avec un spécialiste en TI (27 %) ou appelleraient la police (27 %) pour se protéger. Deux personnes sur 10 (22 %) communiqueraient avec un ami ou un membre de la famille pour obtenir de l'aide si elles croyaient avoir été victimes d'une cyberattaque.

Au fil du temps, on observe peu de changements par rapport à plusieurs mesures qui seraient prises par les Canadiens et Canadiennes en ligne pour se protéger. Parmi les exceptions notables cette année, mentionnons la fermeture de l'ordinateur; un nombre beaucoup plus faible de personnes ont indiqué qu'ils prendraient cette mesure (30 % comparativement à 40 % en 2022). On constate également une légère diminution pour ce qui est de la communication avec les principales agences de crédit du Canada (35 % cette année comparativement à 41 % en 2020 et 2022). De plus, cette année, la proportion de Canadiens et de Canadiennes en ligne qui communiqueraient avec un spécialiste en TI ou qui appelleraient la police a continué de diminuer.

Diagramme 27 : Mesures prises pour se protéger après avoir été victime d'une cyberattaque



QCT7. Si vous saviez ou pensiez avoir été victime d'une cyberattaque, quelles mesures prendriez-vous pour vous protéger? [Plusieurs réponses acceptées.] Base de référence : tous les répondants. Ne sait pas : 2 %.

Voici les différences dignes de mention entre les sous-groupes :

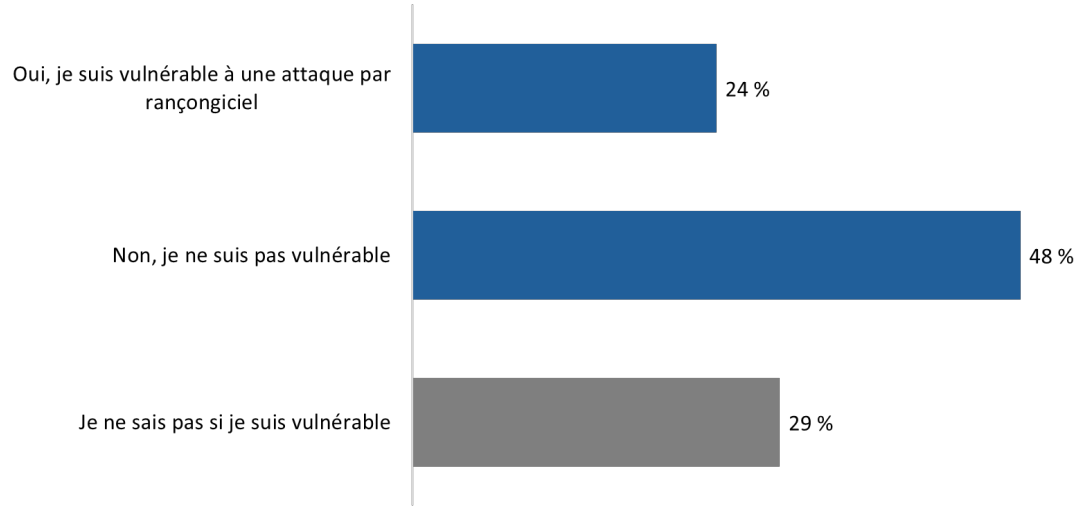
- Les résidents du Québec sont plus susceptibles que les personnes vivant ailleurs au pays de communiquer avec les principales agences de crédit du Canada. En revanche, comparativement aux Ontariens, les personnes vivant au Québec ont moins tendance à vouloir éteindre leur ordinateur, à déconnecter tous les périphériques, à supprimer le matériel suspect, à mettre à jour leur logiciel de sécurité, à changer leurs mots de passe et à communiquer avec leur banque.
- Les Canadiens et Canadiennes en ligne âgés de 65 ans et plus sont plus enclins que les jeunes à éteindre leur ordinateur et à supprimer le matériel suspect, et ils sont moins susceptibles de changer leur mot de passe.
- Les femmes ont plus tendance que les hommes à se tourner vers un tiers pour obtenir de l'aide, en particulier les agences de crédit, un spécialiste en TI ou un ami ou un membre de la famille.

- Les personnes ayant fait des études secondaires sont moins susceptibles que leurs homologues titulaires d'un diplôme d'études collégiales ou universitaires de mettre à jour leur logiciel de sécurité, de changer leurs mots de passe, de communiquer avec leur banque et de contacter un spécialiste informatique.

Un quart des répondants pensent qu'ils sont vulnérables à une attaque par rançongiciel.

Le quart (24 %) des Canadiens et des Canadiennes en ligne pensent qu'ils sont vulnérables à une attaque par rançongiciel, tandis que près de la moitié (48 %) se sentent vulnérables. Les autres (29 %) ne savent pas s'ils sont vulnérables à une telle attaque.

Diagramme 28 : Vulnérabilité à l'égard des attaques par rançongiciel



QCT8. Croyez-vous être vulnérable à une attaque par rançongiciel? Base de référence : n=2 222; tous les répondants.

Les groupes suivants sont plus susceptibles de penser qu'ils sont vulnérables à une attaque par rançongiciel : les résidents de la Saskatchewan, les hommes, les membres de ménages dont le revenu annuel s'élève à plus de 100 000 $ et les propriétaires d'entreprise. Les Canadiens et Canadiennes ayant un niveau avancé de connaissances en matière de sécurité en ligne sont plus susceptibles que les gens moins bien informés de croire qu'ils ne sont *pas* vulnérables à une attaque par rançongiciel.

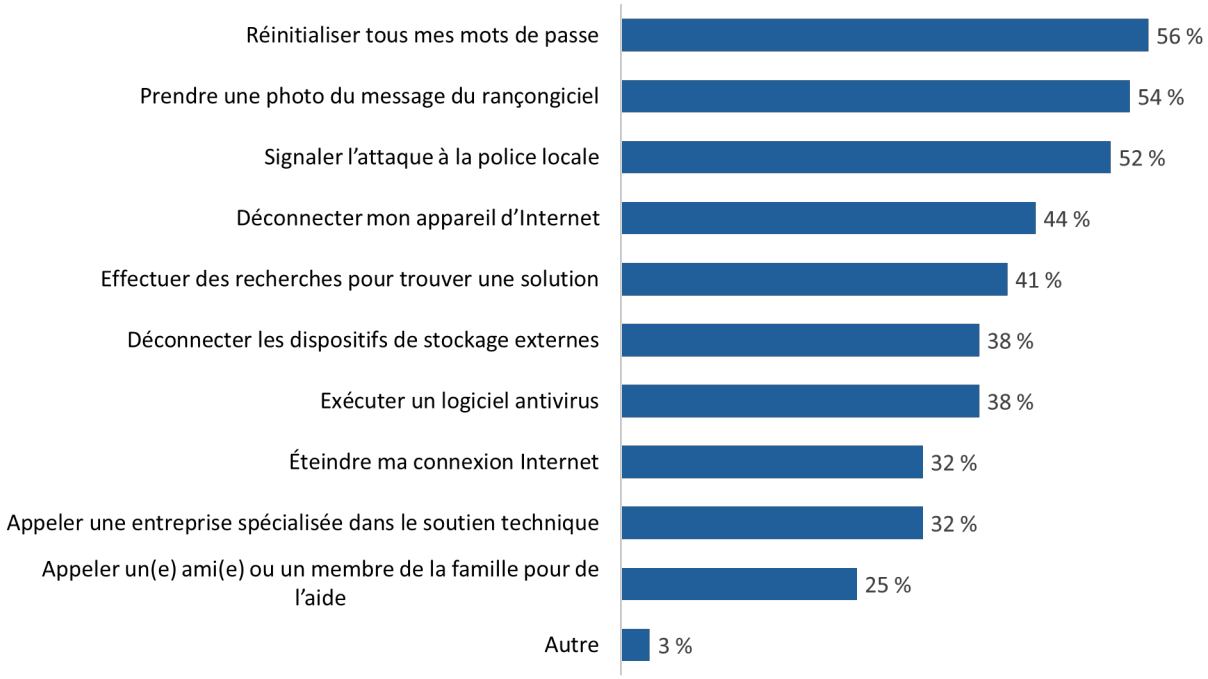
En ce qui concerne l'âge, les personnes de 35 à 64 ans ont plus tendance que les jeunes Canadiens et Canadiennes à penser qu'elles sont vulnérables à une attaque par rançongiciel, tandis que les personnes âgées de 65 ans et plus sont plus susceptibles de *ne pas* savoir si elles sont vulnérables à une telle attaque.

En cas d'attaque par rançongiciel, la majorité des Canadiens et des Canadiennes en ligne réinitialiseraient leur mot de passe, prendraient une photo du message et signaleraient l'attaque à la police locale.

La majorité des Canadiens et des Canadiennes en ligne réinitialiseraient leur mot de passe (56 %), prendraient une photo du message du rançongiciel (54 %) et le signaleraient à la police locale (52 %) s'ils étaient victimes d'une attaque par rançongiciel. De plus, 44 % déconnecteraient leur appareil d'Internet et 41 % effectueraient des recherches pour trouver une solution. Trente-huit pour cent

des répondants déconnecteraient leurs dispositifs de stockage externes et procéderaient à l'exécution d'un logiciel antivirus. Environ un tiers d'entre eux éteindraient leur connexion Internet (32 %) et appelleraient une entreprise spécialisée dans le soutien technique (32 %). Le quart (25 %) se tourneraient vers un ami ou un membre de la famille pour de l'aide.

Diagramme 29 : Mesures prises après avoir été victime d'une attaque par rançongiciel



QCT9. Si vous étiez victime d'une attaque par rançongiciel, que feriez-vous? [Plusieurs réponses acceptées.] Base de référence : n=2 222; tous les répondants. Ne sait pas : 7 %.

Les personnes âgées de 45 ans et plus sont plus susceptibles que les jeunes Canadiens et Canadiennes de dire qu'elles signaleraient l'attaque à la police locale, qu'elles déconnecteraient leur appareil d'Internet et qu'elles appelleraient une entreprise spécialisée en technologies de l'information. Les personnes en ligne âgées de 18 à 34 ans et celles de 65 ans et plus ont plus tendance que les répondants de 35 à 64 ans à dire qu'elles se tourneraient vers un ami ou un membre de leur famille pour obtenir de l'aide. La probabilité d'effectuer elles-mêmes des recherches pour trouver une solution est plus élevée chez les personnes âgées de 18 à 34 ans.

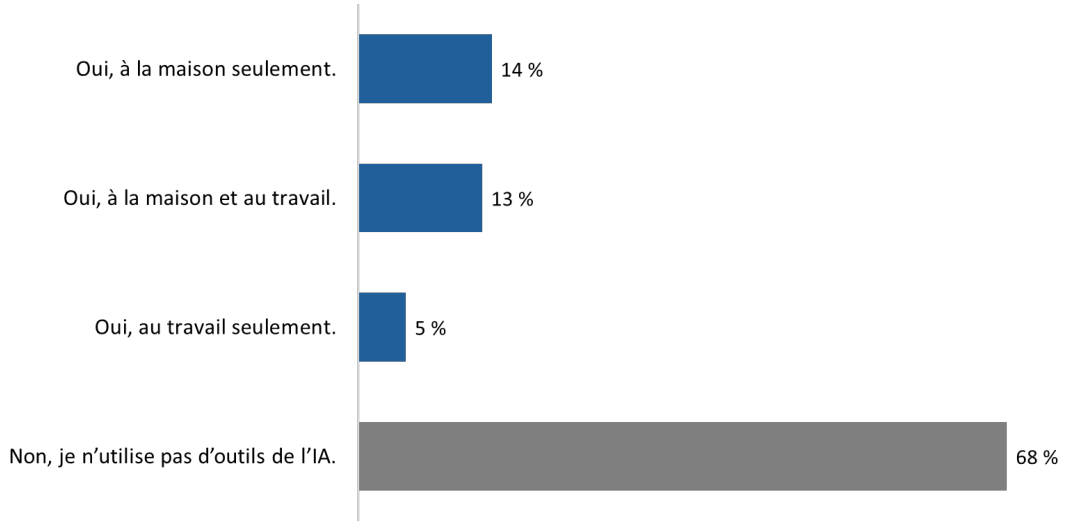
Alors que les hommes sont plus susceptibles que les femmes de mener leurs propres recherches, les femmes sont plus enclines à prendre une photo du message, à signaler l'incident à la police et à demander de l'aide à un ami ou à un membre de la famille (35 % par rapport à 18 %) ou à une entreprise spécialisée dans le soutien technique (38 % contre 31 %).

Points de vue sur l'intelligence artificielle

Le tiers des Canadiens et des Canadiennes en ligne utilisent des outils d'IA.

Le tiers (32 %) des personnes en ligne utilisent des outils d'intelligence artificielle (IA), comme ChatGPT, CoPilot, DALL-E, à la maison ou au travail. Quatorze pour cent se servent des outils d'IA à la maison seulement et 5 % les utilisent uniquement au travail. Les autres (13 %) y ont recours au travail et à la maison. En revanche, les deux tiers (68 %) ne se tournent vers aucun outil d'IA.

Diagramme 30 : Utilisation de l'IA



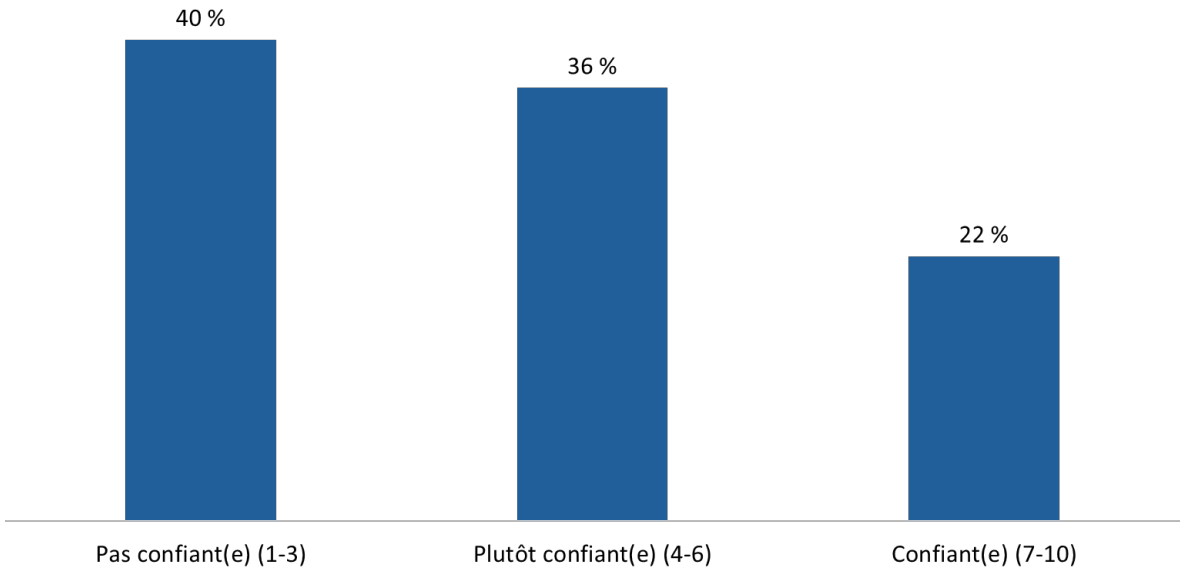
QAI1: Utilisez-vous des outils de l'intelligence artificielle (IA)* à la maison ou au travail? Base de référence : n=2 222; tous les répondants.

L'utilisation des outils d'IA diminue à mesure que l'âge augmente, et l'utilisation à domicile des outils d'IA est plus élevée chez les répondants de 18 à 34 ans. Les personnes de moins de 45 ans sont plus nombreuses que les membres des autres groupes à se servir des outils d'IA au travail et à la maison. La génération Z est plus susceptible d'utiliser des outils d'IA à la maison, tandis que les baby-boomers et la génération silencieuse ont plus tendance à ne pas recourir à des outils d'IA. Les personnes dont le revenu du ménage est supérieur à 150 000 $ sont plus enclines à utiliser l'IA au travail et à la maison que celles dont le revenu du ménage s'élève à moins de 80 000 $.

Les deux tiers des répondants ont confiance du moins dans une certaine mesure en leur capacité à reconnaître du contenu généré par l'IA.

Vingt-deux pour cent des Canadiens et des Canadiennes en ligne ont déclaré avoir confiance en leur capacité de reconnaître du contenu généré par l'IA, comme des messages, des photos, des vidéos ou des hypertrucages. De plus, 36 % se disent assez confiants. Les autres (40 %) n'ont pas confiance en leur capacité d'identifier du contenu généré par l'IA.

Diagramme 31 : Reconnaissance du contenu généré par l'IA



QAI3. Dans quelle mesure avez-vous confiance en votre capacité de reconnaître du contenu généré par l'IA (p. ex., messages, photos, vidéos, hypertrucages)? Base de référence : n=2 222; tous les répondants. Ne sait pas : 3 %.

Les jeunes et les hommes en ligne sont plus susceptibles d'avoir confiance en leur capacité de reconnaître du contenu généré par l'IA. C'est la même chose pour les personnes qui possèdent un niveau avancé de connaissances en matière de sécurité en ligne. Le niveau de confiance est plus élevé au sein des membres de la génération Z, suivis des milléniaux et de la génération X.

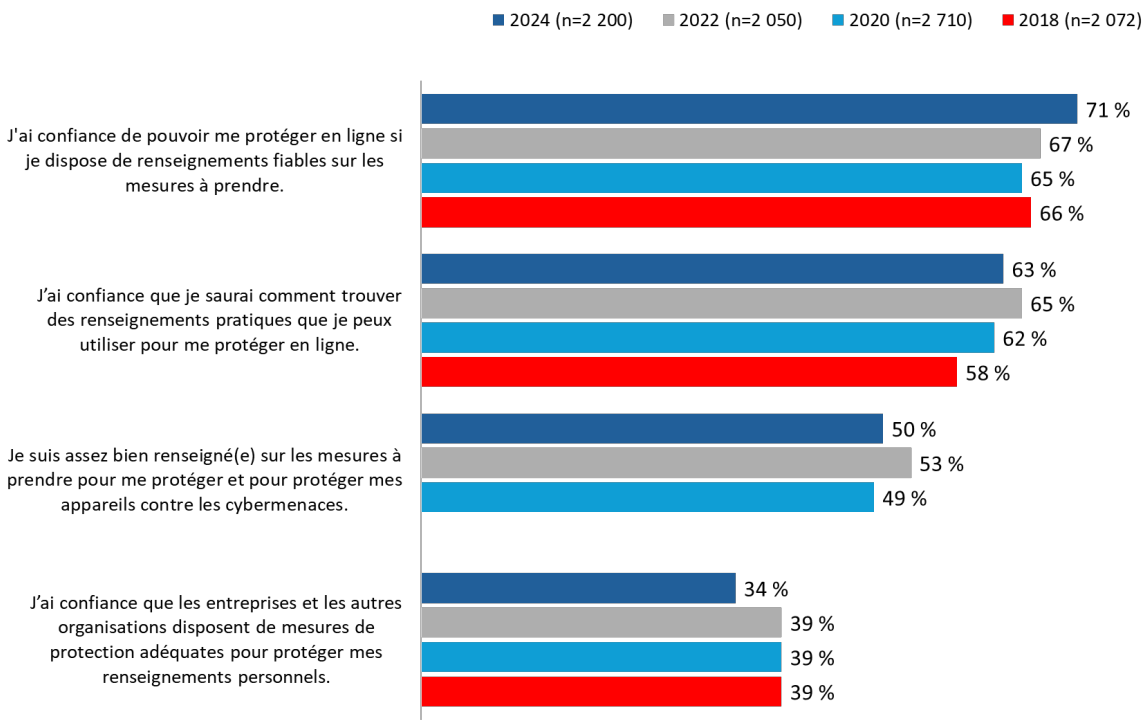
Les communications et la campagne Pensez cybersécurité

De nombreux Canadiens et Canadiennes sont convaincus qu'ils peuvent se protéger en ligne; un nombre beaucoup plus faible de répondants sont convaincus que les entreprises disposent de mesures de protection adéquates pour protéger leurs renseignements personnels.

Sept Canadiens et Canadiennes en ligne sur 10 (71 %, soit une hausse par rapport à 67 % en 2022) sont convaincus qu'ils peuvent se protéger en ligne s'ils disposent de renseignements fiables sur les mesures à prendre. Près des deux tiers (63 %, une baisse comparativement à 65 % en 2022) estiment qu'ils savent comment trouver des renseignements pratiques pour se protéger en ligne et exactement la moitié (50 %, soit une baisse par rapport à 53 % en 2022) croient détenir suffisamment d'informations sur la façon de prendre des mesures pour se protéger contre les cybermenaces. Ils sont moins nombreux (34 %, ce qui représente une baisse par rapport à 39 % en

2022) à être d'avis que les entreprises et les autres organisations disposent de mesures de protection adéquates pour protéger leurs renseignements personnels. Les résultats de cette année sont similaires à ceux de 2022; les différences d'une année à l'autre ne dépassent pas 5 %.

Diagramme 32 : Renseignements sur la protection contre les cybermenaces



QINFO1. Veuillez indiquer dans quelle mesure vous êtes d'accord ou en désaccord avec les énoncés ci-dessous. Base de référence : n=2 222; tous les répondants. Ne sait pas : 2 %.

Les Canadiens et Canadiennes de moins de 45 ans ont plus tendance à croire qu'ils disposent de suffisamment d'informations pour prendre des mesures assurant leur protection en ligne. Les personnes de moins de 45 ans sont également plus susceptibles d'être convaincues qu'elles peuvent se protéger en ligne si elles disposent de renseignements fiables et qu'elles peuvent trouver des renseignements pratiques à cette fin.

Les hommes ont plus tendance que les femmes à croire qu'ils disposent de suffisamment d'information sur les mesures pouvant les protéger contre les cybermenaces et à être confiants qu'ils peuvent trouver des renseignements pratiques pour se protéger en ligne. Les femmes sont plus susceptibles de croire que les entreprises et les autres organisations ont mis en place des mesures de sécurité adéquates pour protéger les renseignements personnels.

Les personnes dont le ménage touche un revenu annuel plus élevé (150 000 $ et plus) sont plus enclines à croire qu'elles ont suffisamment d'informations pour se protéger et protéger leurs appareils. Elles ont en outre confiance qu'elles peuvent se protéger en ligne si elles disposent de renseignements fiables et qu'elles peuvent trouver des informations pratiques pour assurer leur protection en ligne.

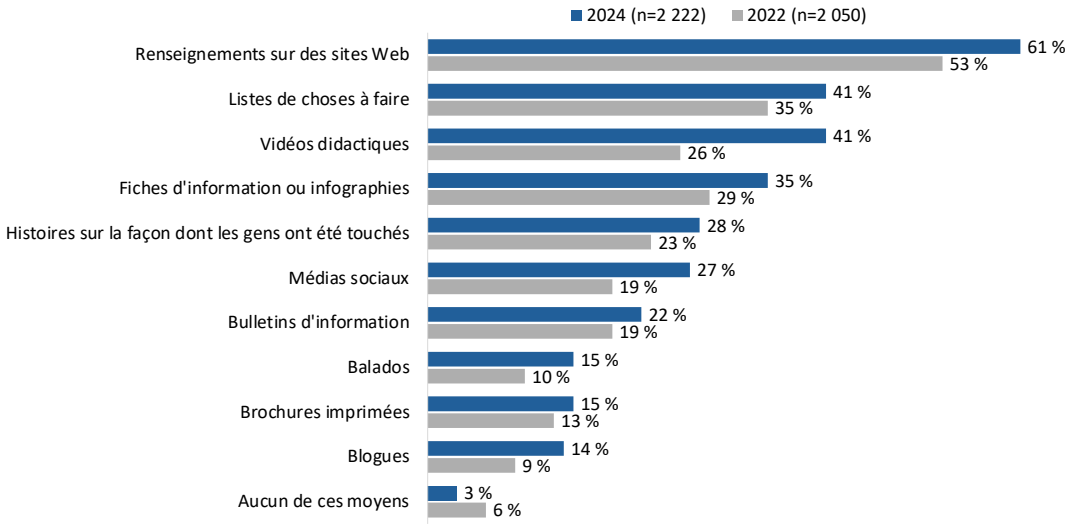
Les baby-boomers et la génération silencieuse ont le plus besoin d'information : ils sont plus susceptibles de ne pas avoir confiance en leur capacité de trouver des informations pratiques et de se protéger en ligne grâce à des renseignements fiables et ils ont plus tendance à croire qu'ils ne disposent pas d'informations suffisantes pour assurer leur protection en ligne.

Six personnes sur 10 préféreraient que l'information sur la cybersécurité soit disponible sur les sites Web.

Soixante et un pour cent des Canadiens et des Canadiennes en ligne préféreraient obtenir de l'information pour se protéger contre les cybermenaces au moyen de sites Web. Quatre personnes sur 10 ont exprimé une préférence pour les listes de choses à faire (41 %) et les vidéos didactiques (41 %). Environ le tiers (35 %) aimeraient des fiches d'information ou des infographies. Le diagramme 33 présente toute la gamme de moyens.

Les deux mêmes moyens demeurent en tête de liste d'une année à l'autre : les informations sur les sites Web et les listes de choses à faire. Cette année, cependant, un plus grand nombre de personnes ont indiqué une préférence pour chacun d'eux : les sites Web (61 % par rapport à 53 %) et les listes de choses à faire (41 % par rapport à 35 %). En effet, une plus grande proportion de répondants ont choisi chacun des moyens et les vidéos didactiques affichent l'augmentation la plus notable au fil du temps : cette année, 41 % ont exprimé une préférence pour ce moyen comparativement à 26 % en 2022. Viennent ensuite les médias sociaux : 27 % ont dit cette année préférer obtenir de l'information par l'entremise de ces plateformes, comparativement à 19 % en 2022.

Diagramme 33 : Moyens préférés pour obtenir de l'information sur la protection contre les cybermenaces



QINFO2. Comment préférez-vous obtenir de l'information pour vous protéger contre les cybermenaces? [Plusieurs réponses acceptées.] Base de référence : n=2 022; tous les répondants. Ne sait pas/refus de répondre : 6 %.

Les différences notables entre les sous-groupes sont les suivantes :

- Les Canadiens et Canadiennes en ligne âgés de 65 ans et plus sont plus susceptibles de préférer les listes de choses à faire, les brochures imprimées et les bulletins d'information (par courriel). En revanche, les jeunes (de moins de 45 ans) préfèrent davantage les médias sociaux,

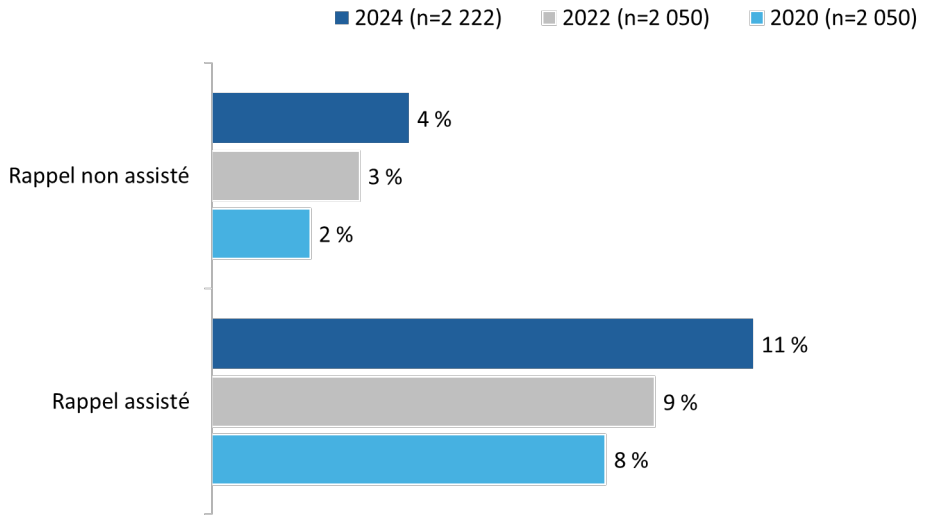
l'information sur les sites Web, les blogues et les fiches d'information. Les personnes âgées de 18 à 34 ans sont plus nombreuses à exprimer une préférence pour les histoires sur la façon dont les gens ont été touchés.

- Un nombre plus important d'hommes que de femmes préfèrent obtenir des renseignements pour se protéger contre les cybermenaces par l'entremise des balados, des blogues et des sites Web. Les femmes, en revanche, sont plus susceptibles de préférer les fiches d'information ou les infographies, les listes de choses à faire, les brochures imprimées et les médias sociaux.
- Les diplômés des collèges et des universités ont plus tendance à préférer les fiches d'information ou les infographies et les listes de choses à faire.

Relativement peu de gens ont entendu parler de la campagne Pensez cybersécurité.

Très peu (4 %) de répondants ont affirmé être en mesure de nommer la campagne de sensibilisation du gouvernement du Canada créée pour renseigner la population canadienne sur la cybersécurité et les mesures simples que les gens peuvent prendre pour se protéger en ligne. Parmi les personnes ayant déclaré connaître la campagne, seulement 2 % l'ont correctement nommée. Une proportion un peu plus importante (11 %) de répondants ont déclaré être au courant de la campagne Pensez cybersécurité lorsqu'on leur a fourni le nom de la campagne.

Diagramme 34 : Connaissance de la campagne du gouvernement du Canada sur la cybersécurité



QGCS1. Une campagne de sensibilisation du gouvernement du Canada a été créée pour informer les Canadiens et les Canadiennes sur la cybersécurité et sur les mesures simples qu'ils et qu'elles peuvent prendre pour se protéger en ligne. Pouvez-vous nommer cette campagne? Base de référence : tous les répondants. Ne sait pas : 8 %.
QGCS3. 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 de référence : tous les répondants. Ne sait pas : 8 %.

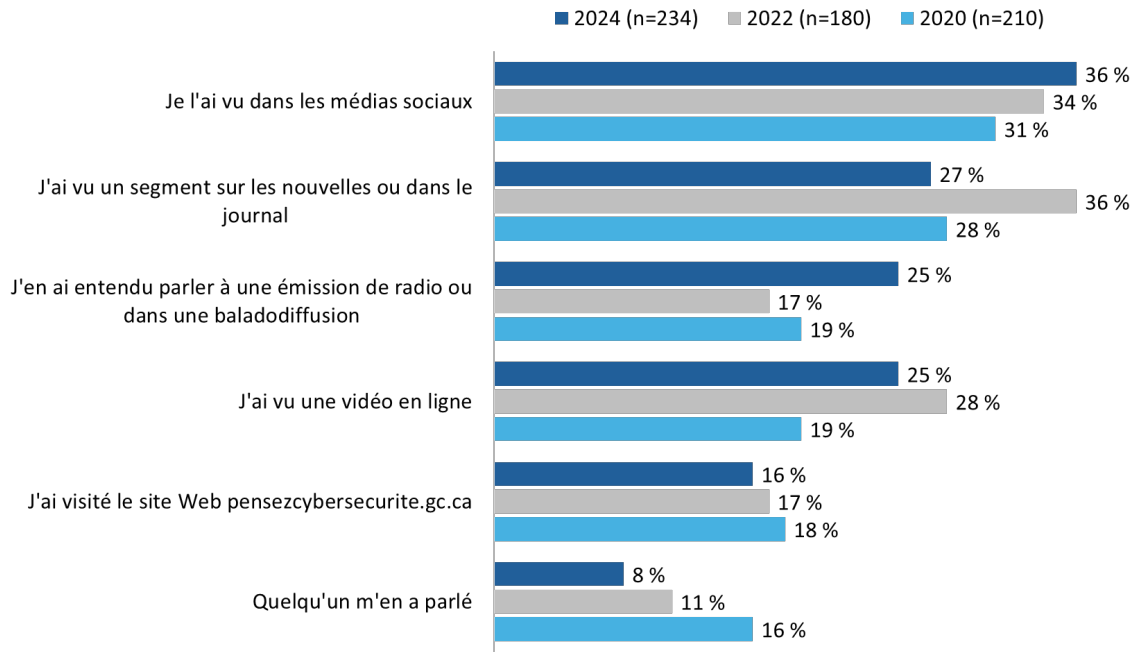
Lorsqu'on leur a donné le nom, les membres de la génération Z étaient plus susceptibles que les milléniaux, les membres de la génération X et les baby-boomers de se souvenir de la campagne.

Environ un tiers des répondants disent connaître la campagne grâce aux médias sociaux.

Parmi les personnes au courant de la campagne Pensez cybersécurité (n=234), un peu plus du tiers (36 %) ont déclaré avoir lu quelque chose à ce sujet dans les médias sociaux. Environ le quart des répondants ont vu un segment aux nouvelles ou dans le journal (27 %), en ont entendu parler dans une émission de radio ou un balado (25 %) ou ont visionné une vidéo en ligne (25 %). De plus petites proportions ont visité le site Web Pensezcybersecurite.ca (16 %) et ont entendu parler de la campagne par une autre personne (8 %).

Comparativement à 2022, un plus grand nombre de Canadiens et de Canadiennes qui étaient au courant de la campagne ont déclaré en 2024 en avoir entendu parler dans une émission de radio ou un balado (25 % par rapport à 17 %), tandis que la proportion des personnes qui ont vu un segment dans les nouvelles ou les journaux a diminué cette année (de 36 % en 2022 à 27 % en 2024). Pour tous les autres changements observés au fil du temps, l'écart n'était pas supérieur à 3 %.

Diagramme 35 : Source d'information au sujet de la campagne Pensez cybersécurité



QGCS4. Où l'avez-vous vu, lu ou entendu? [Plusieurs réponses acceptées.] Base de référence : n=234; personnes au courant de la campagne Pensez cybersécurité. Ne sait pas : 7 %.

Les entreprises et la cybersécurité

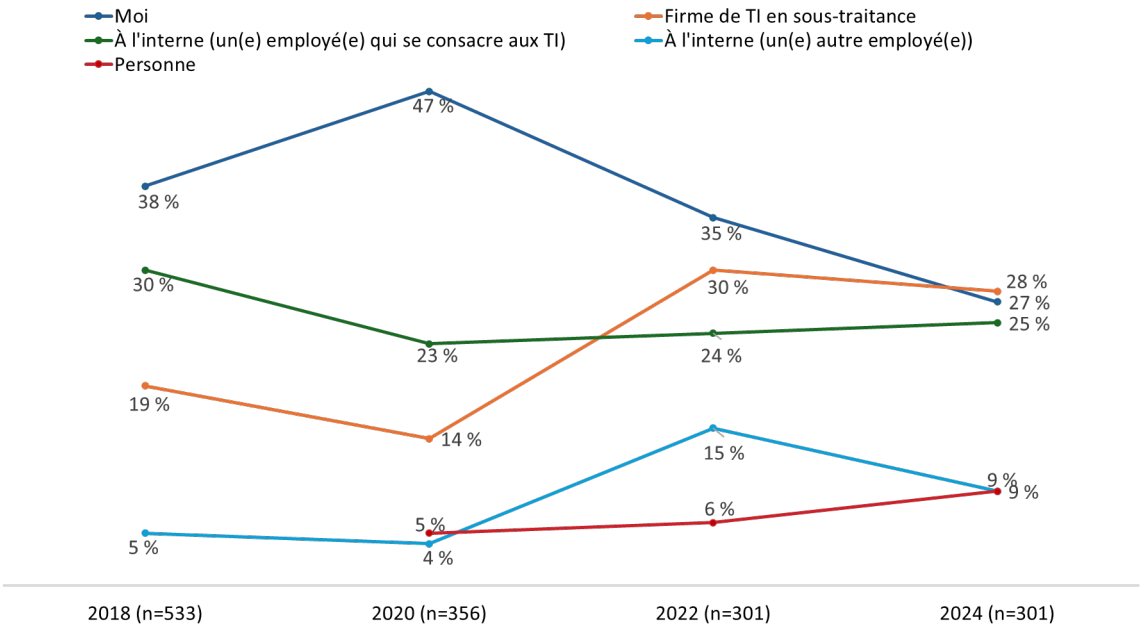
Les questions de cette section du rapport n'ont été posées qu'aux Canadiens et Canadiennes en ligne qui possèdent une entreprise ou qui gèrent des employés d'une petite entreprise (n=301). En tout, 39 % des répondants étaient propriétaires d'une petite entreprise et 61 % étaient des gestionnaires ou des superviseurs.

Aux fins de la présente étude, les petites entreprises comptent jusqu'à 100 employés. Un peu plus du tiers (35 %) des entreprises de l'échantillon emploient moins de cinq personnes. Parmi les autres, 14 % ont de cinq à neuf employés, 35 % de 10 à 49 employés et 16 % de 500 à 100 employés.

Pour ce qui est de la responsabilité des technologies de l'information (TI), 28 % des entreprises sondées ont déclaré que leur entreprise confie le soutien informatique à un sous-traitant, 27 % en assument personnellement la responsabilité et 25 % ont mandaté un employé pour s'en charger. Un répondant sur 10 a déclaré qu'un autre employé (un employé qui n'est pas affecté aux TI) est responsable (9 %) ou que personne dans son organisation n'est responsable des TI de l'entreprise (9 %).

Au fil du temps, de moins en moins de propriétaires et de gestionnaires d'entreprise assument la responsabilité de l'informatique de leur entreprise. On a observé un sommet en 2020, à 47 %, puis une diminution à 35 % en 2022 et à 27 % en 2024. Le recours à des fournisseurs de services externes est pratiquement inchangé cette année, après avoir doublé entre 2020 (14 %) et 2022 (30 %). Le soutien informatique à l'interne est demeuré constant depuis 2020, tandis que la proportion d'entreprises confiant le soutien informatique à un autre employé (plutôt qu'à un employé se consacrant exclusivement à l'informatique) a diminué cette année (de 15 % en 2022 à 9 % cette année) après avoir considérablement augmenté de 2020 à 2022 (de 4 % à 15 %).

Diagramme 36 : Responsabilité des TI



QBUS1. Qui est responsable des TI pour votre société? Base de référence : répondants qui sont des entreprises; n=301. Ne sait pas/refuse de répondre : 7 %.

Plus des trois quarts des personnes sondées (78 %) ont déclaré que leur entreprise avait pris des mesures pour se protéger contre les cybermenaces. Parmi les autres, 6 % n'ont mis en œuvre aucune mesure de protection contre les cybermenaces et 16 % ne savaient pas si leur entreprise avait pris ou non de telles mesures.

Au moins la moitié des propriétaires et gestionnaires d'entreprise sondés ont indiqué que leur entreprise exige une protection par mot de passe sur tous les appareils (57 %), qu'elle effectue les mises à jour des logiciels de sécurité sur tous les ordinateurs (55 %) et qu'elle utilise un mot de passe ou une authentification d'utilisateur pour l'accès sans fil et à distance (51 %). La liste complète des mesures prises se trouve dans le diagramme 37.

À une exception près, la proportion d'entreprises qui adoptent de telles mesures a diminué depuis 2022. La formation sur les pratiques exemplaires en matière de cybersécurité est l'exception. Il n'y a eu aucun changement au fil du temps dans le nombre d'entreprises mettant en œuvre cette mesure pour se protéger contre les cybermenaces.

Diagramme 37 : Mesures mises en œuvre par les entreprises pour se protéger contre les cybermenaces

	2024 (n=301)	2022 (n=301)	2020 (n=360)	2018 (n=533)
Exiger que l'accès à tous les appareils soit protégé par mot de passe	57 %	69 %	57 %	71 %
Tenir à jour les logiciels de sécurité sur tous les appareils	55 %	63 %	51 %	69 %
Utiliser un mot de passe ou une authentification d'utilisateur pour l'accès sans fil et à distance	51 %	60 %	52 %	67 %
Sauvegarder l'information sur tous les appareils	42 %	58 %	49 %	60 %
Établir des filtres de pourriels	40 %	49 %	39 %	54 %
Utiliser un logiciel de cryptage	31 %	34 %	23 %	36 %
Suivre les protocoles de suppression de l'information lorsque les employés quittent l'organisation	27 %	28 %	18 %	37 %
Adopter une politique en matière de cybersécurité à l'intention des employé(e)s	25 %	32 %	18 %	--
Offrir aux employé(e)s une formation sur les pratiques exemplaires en matière de cybersécurité	24 %	24 %	15 %	--
Ne pas utiliser de compte d'administrateur pour l'accès au Web	14 %	24 %	15 %	25 %
Aucune de ces mesures	*6 %*	*5 %*	*9 %*	*5 %*
Ne sait pas	*16 %*	*8 %*	*10 %*	*5 %*

QBUS2. Quelles mesures parmi les suivantes votre entreprise a-t-elle prises pour se protéger contre les cybermenaces? [Plusieurs réponses acceptées.] Base de référence : répondants qui sont des entreprises; n=301. Refuse de répondre : 2 %.

Lorsqu'il s'agit de protéger leur entreprise contre les cybermenaces, environ quatre propriétaires et gestionnaires d'entreprise sur 10 ont déclaré que leur organisation pourrait tirer profit de directives pour réagir à une cyberattaque (44 %, soit une baisse par rapport à 50 % en 2022), d'une liste des types de menaces existantes et de signaux à surveiller (42 %, une baisse comparativement à 49 % en 2022) ou de mesures pour protéger les appareils mobiles dans un lieu public (38 %, une baisse par rapport à 44 % en 2022). La gamme complète des renseignements jugés avantageux par les répondants se trouve dans le tableau ci-dessous.

Diagramme 38 : Renseignements dont les entreprises pourraient tirer profit

	2024 (n=301)	2022 (n=301)	2020 (n=360)	2018 (n=533)
Directives pour réagir à une cyberattaque	44 %	50 %	40 %	46 %
Liste de types de menaces qui existe et signaux à rechercher	42 %	49 %	41 %	47 %
Mesures pour protéger les appareils mobiles dans un lieu public	38 %	44 %	39 %	40 %

Directives pour mettre en place des règles relatives à la politique d'utilisation sécuritaire des courriels	35 %	40 %	28 %	39 %
Pratiques exemplaires sécuritaires en informatique en nuage	34 %	43 %	36 %	35 %
Conseils et ressources pour le type de logiciel ou matériel permettant de sécuriser des réseaux	33 %	41 %	29 %	36 %
Ressources sur la façon de crypter des ordinateurs, portables et dispositifs de stockage	33 %	41 %	34 %	37 %
Pratiques exemplaires sur la façon pour les employé(e)s de gérer les mots de passe	32 %	44 %	29 %	37 %
Pratiques exemplaires pour l'utilisation de dispositifs de stockage	31 %	39 %	34 %	40 %
Conseils pour communiquer aux employé(e)s l'importance de suivre des politiques de cybersécurité	28 %	35 %	25 %	32 %
Mesures pour gérer les renseignements liés au travail que possèdent les employé(e)s qui quittent l'organisation	27 %	33 %	22 %	33 %
Directives sur l'utilisation de dispositifs personnels au travail	27 %	42 %	31 %	40 %
Pratiques exemplaires pour une politique d'utilisation d'Internet claire	26 %	38 %	27 %	37 %
Directives sur la façon d'établir une politique en matière de médias sociaux	22 %	28 %	26 %	37 %
Autre	3 %	4 %	3 %	4 %
Aucune de ces mesures	*5 %*	*5 %*	*9 %*	*8 %*
Ne sait pas	*12 %*	*11 %*	*13 %*	*12 %*

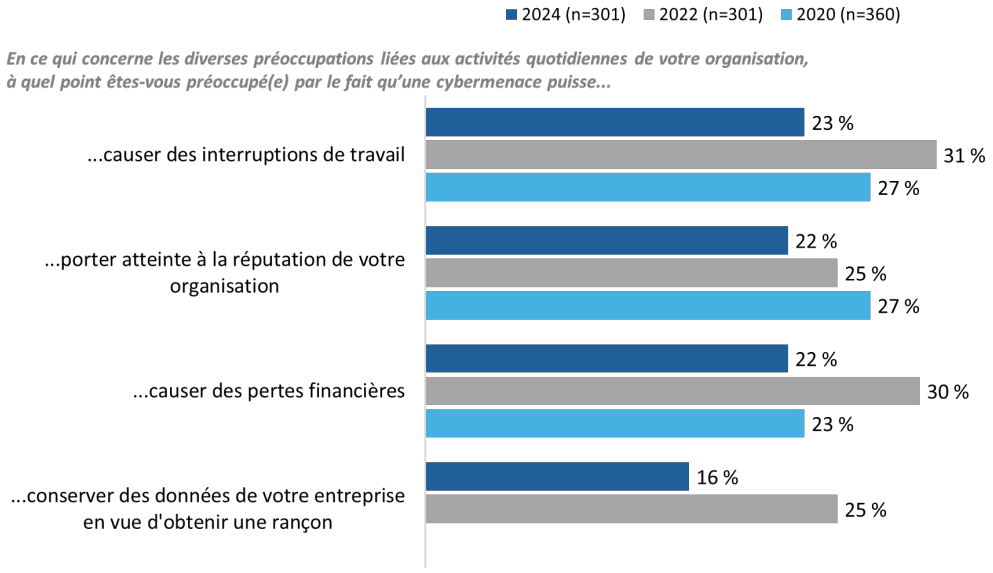
QBUS3. De quels types de renseignements parmi les suivants croyez-vous que votre organisation tirerait profit pour se protéger contre les cybermenaces? Base de référence : répondants qui sont des entreprises; n=301. Refuse de répondre : 6 %.

Les préoccupations au sujet des cybermenaces ont diminué d'une année à l'autre.

En pensant aux activités courantes de leur entreprise, près d'un quart des propriétaires et des gestionnaires d'entreprise se disent préoccupés par les interruptions de travail (23 %) et presque autant craignent une atteinte à la réputation de l'organisation (22 %) ou les pertes financières (22 %) (cotes de 5 à 7 sur une échelle de 7 points). Seize pour cent s'inquiètent du risque que les données de leur entreprise soient conservées en vue d'obtenir une rançon.

Les préoccupations par rapport à chacun de ces aspects ont diminué depuis 2022. Cependant, si l'on tient compte des répondants qui se disent « modérément » préoccupés (cotes de 4), il y a une légère augmentation de la proportion de propriétaires et de gestionnaires d'entreprise qui craignent au moins modérément les interruptions de travail (62 % en 2024 par rapport à 57 % en 2022).

Diagramme 39 : Préoccupations concernant les cybermenaces

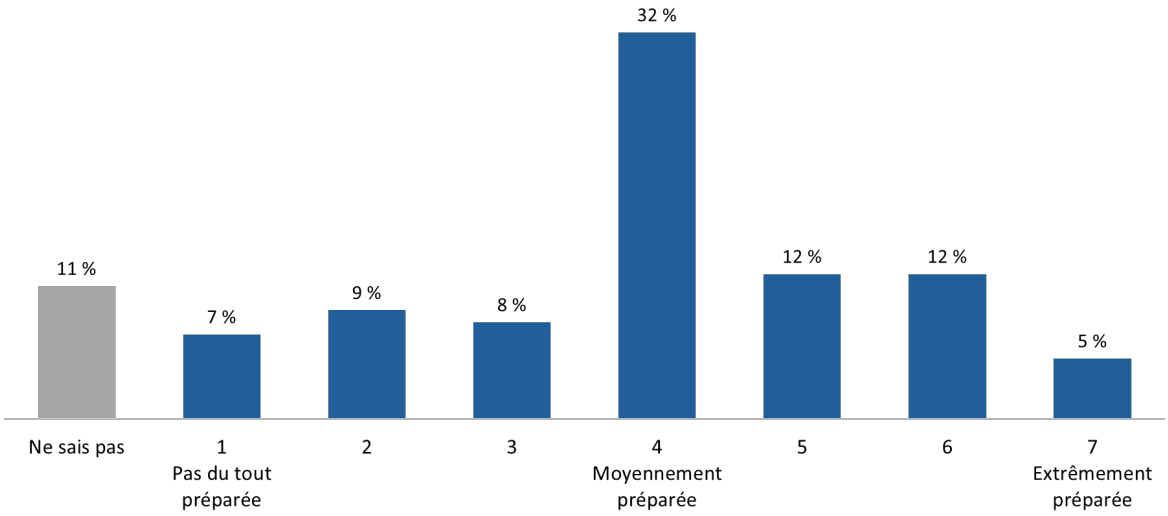


QBUS4. En ce qui concerne les diverses préoccupations liées aux activités quotidiennes de votre organisation, à quel point êtes-vous préoccupé(e) par le fait qu'une cybermenace puisse...Utilisez une échelle de 7 points où 1 veut dire « pas préoccupé(e) du tout » et 7, « extrêmement préoccupé(e) ». Base de référence : répondants qui sont des entreprises; n=301. Ne sait pas/refuse de répondre : 1 % ou moins.

Six entreprises sur 10 sont au moins modérément préparées à se défendre contre les attaques par rançongiciel.

La majorité des propriétaires et des gestionnaires d'entreprise ont déclaré que leur entreprise est modérément (32 %) ou très bien (29 %) préparée à se défendre contre les attaques par rançongiciel. Un quart (24 %) des répondants affirment ne pas être préparés et les autres (11 %) ne savaient pas comment évaluer le niveau de préparation actuel de leur entreprise par rapport aux attaques par rançongiciel.

Diagramme 40 : État de préparation pour se défendre contre les attaques par rançongiciel

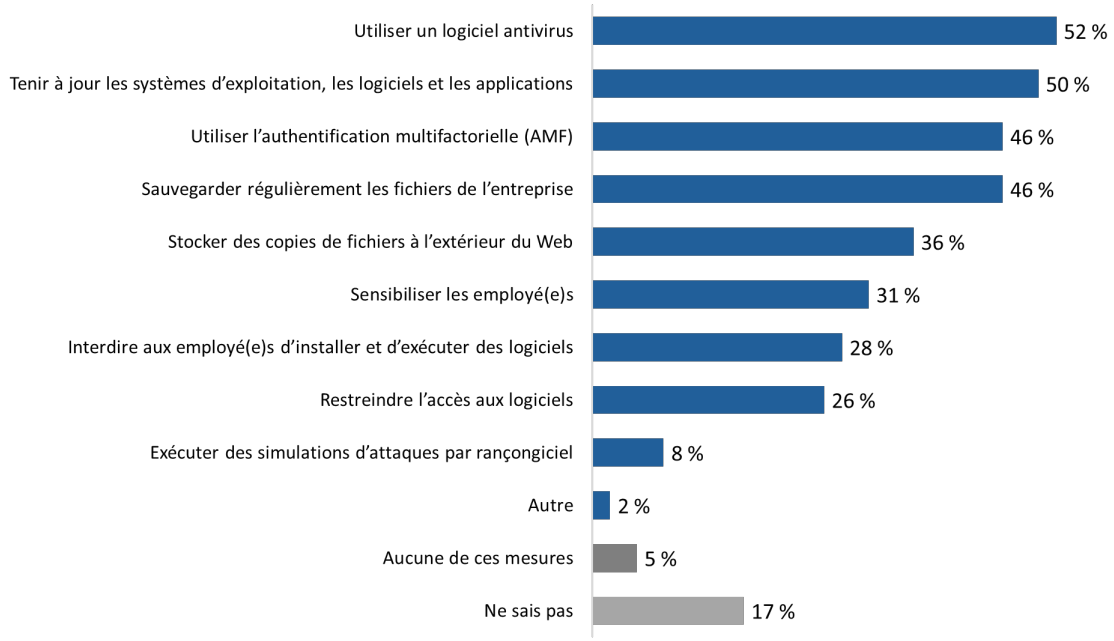


QBUS5. Selon vous, dans quelle mesure votre entreprise est-elle préparée actuellement pour se défendre contre des attaques par rançongiciel? Base de référence : répondants qui sont des entreprises; n=301. Refuse de répondre : 4 %.

Les mesures mises en œuvre par les entreprises pour se protéger contre les rançongiciels varient.

La moitié des propriétaires et des gestionnaires d'entreprise ont déclaré que leur entreprise utilise des logiciels antivirus (52 %) et effectue les mises à jour des systèmes d'exploitation, des logiciels et des applications (50 %). Une proportion semblable d'entreprises utilisent l'AMF (46 %) et sauvegardent régulièrement les fichiers de l'entreprise (46 %). Un peu plus du tiers (36 %) stockent des copies de fichiers à l'extérieur du Web, tandis qu'environ trois sur 10 renseignent les employés (31 %) et empêchent ces derniers d'installer et d'exécuter des logiciels (28 %). Environ le quart (26 %) limitent l'accès des employés aux logiciels. Un nombre relativement faible (8 %) d'employés exécutent des simulations d'attaques par rançongiciel. Notamment, 17 % des propriétaires et des gestionnaires d'entreprise ne savent pas si leur entreprise a pris des mesures pour se protéger contre les attaques par rançongiciel.

Diagramme 41 : Mesures mises en œuvre par les entreprises pour se protéger contre les rançongiciels

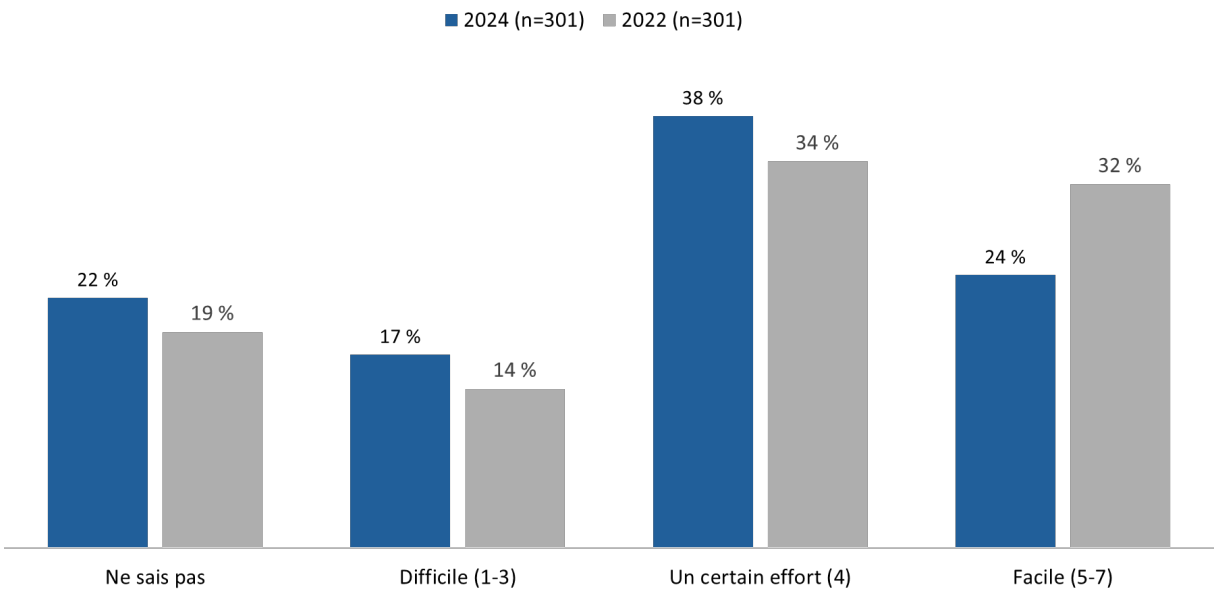


QBUS6. Qu'a fait, s'il y a lieu, votre entreprise pour se protéger contre les attaques par rançongiciel? Base de référence : répondants qui sont des entreprises; n=301. Refuse de répondre : 6 % ou moins.

Pour de nombreuses entreprises, se remettre d'une attaque par rançongiciel exigerait des efforts.

Un peu plus de la moitié des propriétaires et des gestionnaires d'entreprise (55 %, soit une hausse par rapport à 48 % en 2022) prévoient qu'il faudrait déployer des efforts (38 %) pour se remettre d'une attaque par rançongiciel ou qu'il serait difficile (17 %) de s'en remettre. Le quart des répondants (24 %, soit une baisse par rapport à 32 % en 2022) croient que leur entreprise s'en remettrait relativement facilement, avec des conséquences minimes.

Diagramme 42 : Capacité à se remettre d'une attaque par rançongiciel



QBUS7. Dans quelle mesure votre entreprise serait-elle en mesure de se remettre d'une attaque d'un rançongiciel? Base de référence : répondants qui sont des entreprises; n=301. Refuse de répondre : 3 %.

Profil des répondants au sondage

Les tableaux ci-dessous présentent un profil des répondants au sondage (à l'aide de données pondérées). Au total, 80 % des sondages ont été réalisés en anglais et 20 % en français.

Région	**%**
Canada atlantique	7 %
Québec	23 %
Ontario	39 %
Manitoba	4 %
Saskatchewan	3 %
Alberta	11 %
Colombie-Britannique et territoires	14 %

Âge	**%**
18 à 24 ans	11 %
25 à 34 ans	17 %
35 à 44 ans	16 %
45 à 54 ans	17 %
55 à 64 ans	16 %
65 ans et plus	22 %

Génération	**%**
Génération Z : 1997 à 2006	13 %
Milléniaux : 1981 à 1996	25 %
Génération X : 1965 à 1980	24 %
Baby-boomers : 1946 à 1964	30 %
Génération silencieuse : 1928 à 1945	2 %
Aucune réponse	7 %

Genre	**%**
Homme	47 %
Femme	49 %
Autre genre	2 %
Aucune réponse	2 %

Études	%
École primaires ou moins	<1 %
École secondaire	8 %
Un peu d'études postsecondaires	11 %
Collège, école technique ou de métier	25 %
Programme universitaire de premier cycle	27 %
Programme universitaire de 2e ou 3e cycles, ou professionnel	27 %
Aucune réponse	2 %

Statut d'emploi	%
Emploi à temps plein	46 %
Emploi à temps partiel	8 %
Travail autonome	10 %
Sans emploi, mais à la recherche de travail	2 %
Aux études à temps plein	6 %
À la retraite	22 %
À l'extérieur de la population active	3 %
Autre	2 %
Aucune réponse	1 %

Revenu du ménage	%
Moins de 20 000 $	4 %
De 20 000 $ à moins de 40 000 $	9 %
De 40 000 $ à moins de 60 000 $	9 %
De 60 000 $ à moins de 80 000 $	12 %
De 80 000 $ à moins de 100 000 $	14 %
De 100 000 $ à moins de 150 000 $	21 %
150 000 $ et plus	17 %
Aucune réponse	14 %

Parent	%
Oui	28 %
Non	72 %
Aucune réponse	1 %

Âge des enfants	%
Moins de 5 ans	39 %
5 à 8 ans	29 %
9 à 12 ans	32 %
13 à 15 ans	29 %
16 ou 17 ans	21 %

Fréquence de l'utilisation d'Internet	%
Quelques fois par mois	<1 %
Quelques fois par semaine	2 %
Quelques fois par jour	2 %
Je suis toujours branché(e)	69 %

Moyenne d'heures passées en ligne par semaine	%
Moins de 10 heures	15 %
10 heures ou plus	83 %
Je ne sais pas	3 %

Niveau de connaissances sur la sécurité en ligne	%
Avancé	20 %
Intermédiaire	45 %
Base	31 %
Novice/débutant	4 %
Je n'ai pas de connaissances concernant la sécurité en ligne	1 %

Annexe

Spécifications techniques

Les spécifications suivantes s'appliquaient au sondage :

- Un sondage en ligne a été mené auprès de 2 222 Canadiens et Canadiennes de 18 ans et plus qui utilisent Internet au moins quelques fois par mois. Des quotas ont été privilégiés pour sonder au moins 300 propriétaires et gestionnaires/superviseurs d'entreprise comptant moins de 100 employés (sous-échantillon d'entreprises) et 300 ménages avec enfants de moins de 18 ans (sous-échantillon de parents). En tout, 301 propriétaires et gestionnaires/superviseurs d'entreprise et 619 parents ont répondu au sondage.
- De manière générale, il a fallu 16,3 minutes pour répondre au sondage. La médiane était de 14,7 minutes.
- Selon un échantillon de cette taille, les résultats globaux peuvent être considérés comme exacts dans ±2 %, 19 fois sur 20.
- L'échantillon est tiré de l'échantillon populationnel aléatoire d'Advanis, qui a été développé à l'aide d'un recrutement fondé sur les probabilités. Ce panel de plus de 600 000 personnes peut être considéré comme représentatif du grand public au Canada.
- Un prétest a été effectué le 27 février 2024 auprès de 24 personnes. Dix sondages ont été réalisés en français et les autres l'ont été en anglais. La durée médiane du sondage était de 19 minutes. Les 28 et 29 février, des changements ont été apportés au questionnaire afin d'en réduire la longueur (la durée cible était de 15 minutes). Les changements se sont traduits par la suppression de questions seulement; aucun changement n'a été apporté au libellé ou à la structure des questions. Par conséquent, les données du prétest ont été conservées et ont été intégrées aux données du sondage final.
- Le travail sur le terrain a commencé le 29 février et s'est terminé le 19 mars 2024.
- Le travail sur le terrain a été mené par Advanis à l'aide de la méthode de téléphone vers le Web (méthode standard pour tous les sondages soumis aux panélistes de l'échantillon populationnel aléatoire). Tous les répondants au sondage ont reçu au moins un appel téléphonique. Lors du contact, on a demandé aux panélistes s'ils désiraient participer à l'étude et, avec leur consentement, on leur a transmis l'invitation par message texto ou courriel (selon la préférence du panéliste indiquée lors de son inscription au panel). Deux rappels ont été envoyés à trois jours d'intervalle aux personnes qui n'avaient pas répondu au sondage.
- En tout, 13 824 panélistes ont été recrutés pour participer à l'étude et 2 222 d'entre eux ont répondu au sondage. Le taux de participation s'élève donc à 16 %.

Les données de l'enquête ont été pondérées selon l'âge, le genre et la région à l'aide des données démographiques tirées des données du recensement de 2021 de Statistique Canada. Tous les répondants qui refusaient de fournir leur genre se sont vu accorder une pondération neutre afin de ne pas fausser les proportions de pondération. Les tableaux ci-dessous présentent les proportions non pondérées et pondérées pour les variables utilisées aux fins de la pondération.

Genre	% pondérées	% non pondérées
Homme	49 %	52 %
Femme	51 %	48 %

Région	% pondérées	% non pondérées
Canada atlantique	7 %	7 %
Québec	23 %	23 %
Ontario	39 %	36 %
Manitoba	3 %	4 %
Saskatchewan	3 %	3 %
Alberta	11 %	12 %
Colombie-Britannique et territoires	14 %	16 %

Âge	% pondérées	% non pondérées
18 à 24 ans	11 %	8 %
25 à 34 ans	16 %	18 %
35 à 44 ans	16 %	16 %
45 à 54 ans	17 %	17 %
55 à 64 ans	16 %	17 %
65 ans ou plus	23 %	23 %

Une analyse a été effectuée pour évaluer le biais potentiel de non-réponse. La non-réponse au sondage peut biaiser les résultats lorsqu'il existe des différences systématiques entre les répondants au sondage et les non-répondants. L'échantillon de l'étude (les pourcentages non pondérés dans les tableaux ci-dessus) reflétait très fidèlement la répartition démographique (les pourcentages pondérés dans les tableaux ci-dessus). Par conséquent, la non-réponse a probablement entraîné un très faible biais, voire aucun.

Questionnaire du sondage

Page d'introduction au sondage

Nous vous remercions d'avoir accepté de participer à ce court sondage mené par Phoenix SPI au nom du gouvernement du Canada. If you prefer to take part in this survey in English, please click on 'English' in the top right corner.

Le présent sondage est conçu pour recueillir des informations sur les questions liées à la sécurité en ligne. Vous devriez avoir besoin d'au plus 15 minutes pour y répondre, et votre participation est volontaire et entièrement confidentielle. Les renseignements fournis seront gérés conformément aux exigences de la *Loi sur la protection des renseignements personnels*. Vos réponses ne seront pas utilisées pour vous identifier, et aucune de vos opinions ne vous sera attribuée personnellement de quelque manière que ce soit. Pour consulter la politique de confidentialité de Phoenix SPI, cliquez <ici>.

Ce sondage est enregistré auprès du Service de vérification des recherches du Conseil de recherche et d'intelligence marketing canadien. Le code de vérification du projet est **20240202-PH841**. Cliquez <ici> pour vérifier la légitimité du sondage.

Admissibilité et présélection

S1. Quelle est l'année de votre naissance?
01. Année :
02. Je préfère ne pas répondre [PASSER À LA S3]

S2. [SI S1=2006] Avez-vous au moins 18 ans?
01. Oui
02. Non [REMERCIER ET METTRE FIN AU SONDAGE]
03. Préfère ne pas répondre [REMERCIER ET METTRE FIN AU SONDAGE]

S3. [SI S1=02] À quelle catégorie d'âge appartenez-vous?
01. Moins de 18 ans [REMERCIER ET METTRE FIN AU SONDAGE]
02. 18 à 24 ans
03. 25 à 34 ans
04. 35 à 44 ans
05. 45 à 54 ans
06. 55 à 64 ans
07. 65 ans ou plus
08. Je préfère ne pas répondre [REMERCIER ET METTRE FIN AU SONDAGE]

S4. À quelle fréquence faites-vous une utilisation active d'Internet? Cela veut dire une utilisation d'applications ou de sites Web à l'aide d'un appareil connecté à Internet. [CAB24; Q1]
06. Moins de quelques fois par mois [REMERCIER ET METTRE FIN AU SONDAGE]
01. Quelques fois par mois
02. Une fois par semaine
03. Quelques fois par semaine
04. Quelques fois par jour
05. J'y suis toujours connecté(e)

S5. En moyenne, combien d'heures par semaine passez-vous en ligne? On veut dire le temps que vous passez à utiliser des applications ou des sites Web sur un appareil connecté à Internet.
01. Moins de 10 heures
02. 10 heures ou plus
03. Je ne sais pas [REMERCIER ET METTRE FIN AU SONDAGE]

S6. Dans quelle province ou quel territoire habitez-vous actuellement?
01. Alberta
02. Colombie-Britannique
03. Manitoba
04. Nouveau-Brunswick
05. Terre-Neuve-et-Labrador
06. Territoires du Nord-Ouest
07. Nouvelle-Écosse
08. Nunavut
09. Ontario
10. Île-du-Prince-Édouard
11. Québec
12. Saskatchewan
13. Yukon
14. Préfère ne pas répondre [REMERCIER ET METTRE FIN AU SONDAGE]

S7. Laquelle des catégories suivantes décrit le mieux votre situation d'emploi actuelle? Vous êtes...?
01. Employé(e) à temps plein (35 heures par semaine ou plus)
02. Employé(e) à temps partiel (moins de 35 heures par semaine)
03. Travailleur/travailleuse autonome [PASSER À S11]
04. Sans emploi, mais à la recherche d'un emploi [PASSER À S11]
05. Étudiant(e) à temps plein [PASSER À S11]
06. Retraité(e) [PASSER À S11]
07. Hors du marché du travail [au foyer à plein temps, sans emploi, ne cherchant pas d'emploi] [PASSER À S11]
08. Autre [PASSER À S11]
09. Je préfère ne pas répondre [PASSER À S11]

S8. [SI S7=01,02] Combien d'employés compte votre entreprise?
01. Moins de 5
02. 5 à 9
03. 10 à 49
04. 50 à 100
05. 101 à 249 [PASSER À S11]
06. 250 à 499 [PASSER À S11]
07. 500 ou plus [PASSER À S11]
08. Je ne sais pas
09. Je préfère ne pas répondre

S9. [SI S8=01-04] Êtes-vous le/la propriétaire de l'entreprise?
01. Oui [QUOTA DES ENTREPRISES; PASSER À S11]
02. Non
03. Je préfère ne pas répondre

S10. [SI S9=02,03] Vous a-t-on confié l'une ou l'autre des responsabilités suivantes?
Veuillez choisir toutes les réponses pertinentes

01. Des employé(e)s relèvent de vous
02. Vous supervisez le travail d'autres employé(e)s
03. Vous participez aux décisions concernant les processus ou les procédures s'appliquant aux employé(e)s
04. Aucune de ces responsabilités
05. Je préfère ne pas répondre

[QUOTA DES ENTREPRISES : SI S8=01-04 ET S9=01 OU S10=01-03]

S11. Est-ce que des enfants de moins de 18 ans habitent actuellement sous votre toit?
01. Oui [QUOTA DES PARENTS]
02. Non
03. Je préfère ne pas répondre

S12. [SI S11=01] Quel âge ont les enfants qui habitent chez vous?
Veuillez choisir toutes les réponses pertinentes

01. Moins de 5 ans
02. Entre 5 et 8 ans
03. Entre 9 et 12 ans
04. Entre 13 et 15 ans
05. De 16 à 17 ans
06. Je préfère ne pas répondre

S13. Quel est votre niveau de connaissances de la sécurité en ligne? [CAB24; Q3]
01. Avancé
02. Intermédiaire
03. De base
04. Novice/débutant
05. Je n'ai aucune connaissance concernant la sécurité en ligne.

Points de vue et attitudes à l'égard de la cybersécurité

[TOUS]
Les prochaines questions portent sur la sécurité en ligne, qu'on appelle souvent « cybersécurité ».

QCS1. À quel point êtes-vous d'accord avec les énoncés suivants sur la cybersécurité? [CAB24; Q4-Q7]
[ALTERNER L'ORDRE DES ÉNONCÉS]
a) Je trouve ça facile d'être en sécurité quand je suis en ligne.
b) La plupart des informations sur les moyens de rester en sécurité en ligne portent à confusion.

e) Je suppose que tous mes appareils sont automatiquement sécurisés.
f) Me protéger complètement en ligne coûte cher.
g) Je ne comprends pas pourquoi je devrais mieux me protéger, car mes renseignements sont déjà en ligne.
h) Je m'inquiète à l'idée d'être victime d'un cybercrime.
i) Je suis peu susceptible d'être la cible d'un cybercrime.
k) Je m'inquiète de la cybercriminalité liée à l'intelligence artificielle (IA).

[NE PAS ALTERNER L'ORDRE DES ÉNONCÉS SUIVANTS; LES PRÉSENTER TOUJOURS EN DERNIER]
l) Les membres de ma famille comptent sur moi pour assurer leur sécurité en ligne.
m) Je compte sur d'autres personnes (p. ex., ma famille, mes collègues) pour assurer ma sécurité en ligne.

[CHOIX DE RÉPONSE]
1-Fortement en désaccord
2
3
4
5
6
7
8
9
10-Fortement d'accord

QCS2. Sur qui comptez-vous le plus pour obtenir de l'aide ou des conseils en matière de cybersécurité? [CAB24; Q8]
01. Ma famille (p. ex., conjoint(e), enfant, proches).
02. Mes ami(e)s
03. Mes collègues de travail
04. Le gouvernement (p. ex., sites Web du gouvernement)
05. Des entreprises de TI (p. ex., entreprises spécialisées dans le soutien technique ou vendeur d'appareils connexes).
06. Autre (veuillez préciser) :____

QCS3. Dans quelle mesure comptez-vous sur d'autres personnes (p. ex., des ami(e)s ou membres de famille) pour vous aider à faire ce qui suit? [CAB24; Q10]
[ALTERNER L'ORDRE DES ÉLÉMENTS]
a) Obtenir des conseils et de l'information sur les moyens de rester en sécurité en ligne.
b) Créer des comptes en ligne.
c) Vérifier ou ajouter des paramètres de sécurité sur mes appareils (p. ex., NIP).
d) Vérifier, mettre à jour ou installer la dernière version d'un logiciel.
e) Récupérer un mot de passe (p. ex., si vous ne parvenez plus à accéder à vos comptes en ligne).
f) Sauvegarder des données (p. ex., des fichiers et des photos).
g) Détecter des possibles escroqueries en ligne ou des messages d'hameçonnage (p. ex., courriels, textos, messages directs).

[CHOIX DE RÉPONSE]

1-Pas fiable du tout
2
3
4
5
6
7
8
9
10-Tout à fait fiable

QCS5. À quel point avez-vous confiance en votre capacité à identifier un message d'hameçonnage ou un lien malveillant? [CAB24; Q25]
1-Pas du tout confiant(e)
2
3
4
5
6
7
8
9
10-Très confiant(e)

Mesures relatives à la cybersécurité

[TOUS]
Les prochaines questions portent sur les mesures relatives à la cybersécurité.

QBEH1. Prenez-vous des précautions pour protéger vos comptes en ligne, vos comptes de médias sociaux, vos appareils ou vos réseaux? [Cyber22; Q1-KPI]
01. Oui
02. Non
03. Je ne sais pas

QBEH2. Savez-vous comment installer les plus récentes mises à jour de logiciels et d'applications pour tous vos appareils (p. ex., ordinateur et cellulaire)? [CAB24; Q29]
01. Je ne sais pas comment le faire. [PASSER À QBEH5]
02. Je sais comment le faire, mais je ne le fais pas. [PASSER À QBEH5]
03. Je sais comment le faire et je le fais.

QBEH3. [SI QBEH2=03] À quelle fréquence installez-vous les dernières mises à jour et versions des logiciels après avoir été avisé(e) qu'elles sont disponibles? [CAB24; Q60]
01. Jamais [PASSER À QBEH5]
02. Rarement [PASSER À QBEH5]
03. Parfois
04. Très souvent
05. Toujours

QBEH4. [SI QBEH3=03-05] Quand installez-vous généralement les mises à jour sur vos appareils? [CAB24; Q61]
01. J'ai activé les mises à jour automatiques.
02. Immédiatement lorsque je reçois la notification.
03. Après avoir cliqué quelques fois sur « Me le rappeler plus tard ».
04. Chaque fois que je m'éloigne de mon appareil ou que je ne l'utilise pas (p. ex., durant la nuit).

QBEH6. Avez-vous déjà entendu parler de l'authentification multifactorielle (AMF)? [CAB24; Q17]
On l'appelle également l'authentification à deux facteurs ou la vérification en deux étapes.

01. Oui
02. Non [PASSER À QBEH10]

QBEH7. [SI QBEH6=01] Vous avez indiqué avoir entendu parler de l'authentification multifactorielle (AMF). Savez-vous comment l'utiliser? [CAB24; Q18]

01. Je ne sais pas comment l'utiliser. [PASSER À QBEH9]
02. Je sais comment l'utiliser, mais je ne le fais pas.
03. Je sais comment l'utiliser, mais j'ai cessé de l'utiliser.
04. Je sais comment l'utiliser et je l'utilise régulièrement. [PASSER À QBEH10]

QBEH8. [QBEH7=02, 03] Quelle est la principale raison pour laquelle vous n'utilisez pas (ou que vous avez cessé d'utiliser) l'authentification multifactorielle (AMF)? [CAB24; Q19]
[ALTERNER L'ORDRE DES CHOIX DE RÉPONSE]
01. L'AMF prend trop de temps.
02. Je n'ai pas mon téléphone tout le temps sur moi pour pouvoir vérifier.
03. Je n'ai pas constaté de protection supplémentaire avec l'AMF.
04. Mon mot de passe est suffisamment robuste.
05. Je n'ai pas un téléphone fiable ou un bon service sans fil en tout temps pour pouvoir vérifier.
06. Je perds régulièrement l'appareil que j'utilise pour la vérification de l'AMF.
07. [ANCRAGE] Autre (veuillez préciser)
08. [ANCRAGE] Aucune raison en particulier; je ne le fais juste pas.

QBEH9 [QBEH7=01, 02, 03] Veuillez indiquer à quel point vous êtes d'accord avec les énoncés suivants : [CAB24; Q23]
« J'utiliserais l'authentification multifactorielle (AMF), mais… »
[ALTERNER L'ORDRE DES ÉNONCÉS]
a) ...je ne comprends pas comment utiliser l'AMF.
b) ...je doute d'être capable d'utiliser l'AMF.
c) ...je n'ai pas le temps d'utiliser l'AMF.
d) ...je ne crois pas que c'est nécessaire d'utiliser l'AMF si mon appareil fonctionne comme il faut.
f) ...l'utilisation de l'AMF ne freinera pas les cybercriminels.
g) ...l'utilisation de l'AMF ne présente pas d'avantages pour moi.
h) ...je ne fais pas confiance aux logiciels d'AMF.
j) ...cela crée de l'interférence avec mes applications et j'ai peur de « briser » mon appareil.

[CHOIX DE RÉPONSE]
1-Fortement en désaccord

2
3
4
5
6
7
8
9
10-Fortement d'accord

QBEH12. Quelles mesures prenez-vous pour vérifier la légitimité d'un SITE WEB? [CAB24; Q27]
Veuillez choisir toutes les réponses pertinentes

[ALTERNER L'ORDRE DES CHOIX DE RÉPONSE]
01. Avant d'accéder à l'adresse d'un site Web, j'effectue des recherches pour vérifier sa légitimité.
02. Je vérifie si la barre d'adresse contient « https: ».
03. Je vérifie s'il y a le symbole du cadenas verrouillé dans la barre d'adresse.
04. Je vérifie s'il y a un crochet ou un sceau qui confirme la légitimité du site Web.
05. J'analyse l'aspect général du site Web (p. ex., son apparence, s'il a une allure professionnelle).
06. Je lis les commentaires sur d'autres sites Web concernant son respect de la confidentialité ou sa réputation.
07. [ANCRAGE] Autre (veuillez préciser) :___

QBEH13. D'après ce que vous savez, quels sont les signes d'une tentative d'hameçonnage? [Cyber22; B11B]
Veuillez choisir toutes les réponses pertinentes

[ALTERNER L'ORDRE DES CHOIX DE RÉPONSE]
01. Le message utilise un langage insistant ou menaçant
02. Le message demande des informations sensibles, comme des renseignements financiers ou identificatoires
03. Le message transmet une offre qui est trop belle pour être vraie
04. Le message prétend porter sur des comptes que vous n'avez pas ou sur des livraisons que vous n'attendez pas
05. Le message contient des adresses de courriel d'expéditeur incorrectes, des liens inconnus, ou des fautes d'orthographe ou de grammaire
06. Le message comprend des pièces jointes inattendues ou inutiles, qui peuvent avoir des noms de fichiers étranges ou des types de fichiers peu courants
07. Le message peut utiliser une conception graphique non professionnelle, avec des images pixélisées ou un formatage médiocre
08. [ANCRAGE] Autre (veuillez préciser)
09. [ANCRAGE] Rien de ce qui précède
10. [ANCRAGE] Je ne sais pas

QBEH14. À quelle fréquence vérifiez-vous les messages (p. ex., courriels, textos ou médias sociaux) pour détecter des tentatives d'hameçonnage avant de cliquer sur un lien ou de répondre au message? [CAB24; Q62]
01. Jamais
02. Rarement

03. Parfois
04. Très souvent
05. Toujours
06. Je ne sais pas comment identifier les messages qui sont des tentatives d'hameçonnage.

QBEH15. Lorsque vient le temps de choisir vos mots de passe, lesquelles des mesures suivantes prenez-vous? [Cyber22; Q5-02,03,05,09=KPIs]
Veuillez choisir toutes les réponses pertinentes

[ALTERNER L'ORDRE DES CHOIX DE RÉPONSE]
01. Mots de passe simples et faciles à mémoriser
02. Mots de passe complexes, avec une combinaison de lettres, de chiffres et de symboles
03. Mot de passe contenant au moins 4 mots et 15 caractères
04. [NE PEUT ÊTRE SÉLECTIONNÉ AVEC LE CHOIX DE RÉPONSE 05] Utilisation du même mot de passe pour plusieurs comptes
05. [NE PEUT ÊTRE SÉLECTIONNÉ AVEC LE CHOIX DE RÉPONSE 04] Utilisation d'un mot de passe différent et unique pour chaque compte
06. Partage d'un mot de passe avec d'autres personnes
07. Prendre en note vos mots de passe
08. Utilisation d'un gestionnaire de mots de passe
09. Permettre à votre fureteur ou à une application de se rappeler ou de stocker les mots de passe

10. [ANCRAGE] Autre (veuillez préciser) :
11. [ANCRAGE] Rien de ce qui précède
12. [ANCRAGE] Je ne sais pas

QBEH17. À quelle fréquence utilisez-vous des mots de passe uniques pour vos comptes en ligne importants (p. ex., sites de paiement, comptes de médias sociaux et comptes professionnels)? [CAB24; Q52]
« Uniques » veut dire complètement différents, pas seulement le changement d'un caractère ou deux.

01. Tout le temps
02. La plupart du temps
03. La moitié du temps
04. Parfois
05. Jamais

QBEH18. [SI QBEH17=04,05] Vous avez indiqué que vous utilisez rarement des mots de passe uniques pour vos comptes en ligne ou que vous n'en utilisez jamais. [CAB24; Q53]
[ALTERNER L'ORDRE DES CHOIX DE RÉPONSE]
01. Cela prend trop de temps pour les créer.
02. Ils sont trop difficiles à retenir.
03. Cela exige trop d'efforts.
04. Je ne sais pas comment les créer.
05. Je les utilise seulement pour les comptes dont je veux renforcer la sécurité.
06. [ANCRAGE] Autre (veuillez préciser) : _

[QUOTA DES ENTREPRISES : SI S8=01-04 ET S9=01 OU S10=01-03, PASSER À LA PROCHAINE SECTION; TOUS LES AUTRES, CONTINUER]

QBEH21. Combien de caractères comptent les mots de passe que vous créez habituellement? [CAB24; Q59]
01. 6 caractères ou moins
02. 7 ou 8 caractères
03. 9 à 11 caractères
04. 12 à 15 caractères
05. 16 caractères ou plus

QBEH22. Quelle est la méthode que vous privilégiez pour vous souvenir de plusieurs mots de passe? [CAB24; Q66]
[ALTERNER L'ORDRE DES CHOIX DE RÉPONSE]
01. Je les note dans un carnet.
02. Je les inscris dans un document sur mon ordinateur (sous forme électronique).
03. Je les conserve dans mon téléphone.
04. Je les conserve dans ma messagerie électronique.
05. Je ne fais que m'en souvenir (sans les écrire nulle part).
06. J'enregistre mes mots de passe dans le navigateur (p. ex., Google Chrome ou Firefox).
07. J'utilise un gestionnaire de mots de passe (p. ex., 1Password, LastPass, trousseau iCloud).
08. Je les réinitialise chaque fois que je me connecte.

Cybercriminalité

[TOUS]
Les prochaines questions portent sur la cybercriminalité.

QCCE1. Avez-vous subi personnellement une perte d'argent ou de données à cause d'activités nuisibles en ligne? [CAB24; Q31]
Veuillez choisir toutes les réponses pertinentes

[ALTERNER L'ORDRE DES CHOIX DE RÉPONSE]
01. Tentative d'hameçonnage (par courriel ou message texte).
02. Arnaque amoureuse en ligne [PASSER À QCT1]
03. Vol d'identité [PASSER À QCT1]
05. Autre (veuillez préciser) [PASSER À QCT1]
04. [ANCRAGE; EXCLUSIF] Non, je n'ai pas subi une perte d'argent ou de données à cause d'activités nuisibles en ligne [PASSER À QCT1]

Ajouter des cases pour du texte lorsque la souris pointe le mot :

- « Hameçonnage » : Les cybercriminels trompent les gens pour qu'ils fournissent des informations ou installent des logiciels malveillants afin de leur voler de l'argent ou des données. Cela se fait souvent via de faux courriels qui semblent provenir d'expéditeurs de confiance, qui encouragent les gens à cliquer sur des liens malveillants vers de faux sites Web ou à ouvrir des pièces jointes malveillantes.
- « Arnaque amoureuse en ligne » : Les fraudeurs adoptent une fausse identité en ligne dans le but de créer l'illusion d'une relation amoureuse ou intime avec la victime pour la manipuler ou la voler. Souvent, les demandes du fraudeur font grandement appel aux émotions, qui dit avoir

besoin d'argent pour recevoir des soins médicaux d'urgence ou s'il est à l'étranger, afin de payer les frais de transport à débourser pour venir visiter la victime.
- « Vol d'identité » : Le vol d'identité se produit lorsqu'un fraudeur a accès à suffisamment de renseignements sur l'identité d'une personne (p. ex., son nom, sa date de naissance, son adresse actuelle et ses anciennes adresses) pour recevoir des biens ou des services de façon frauduleuse, comme ouvrir un compte bancaire ou obtenir une carte de crédit ou un prêt.

QCCE2. [SI QCCE1=01] Vous avez mentionné avoir subi une perte d'argent ou de données à cause d'une tentative d'hameçonnage. L'avez-vous signalé à quelqu'un? *Si vous avez subi une perte d'argent ou de données plus d'une fois, veuillez penser à la plus récente fois où cela s'est produit.* [CAB24; Q32]
Veuillez choisir toutes les réponses pertinentes

[ALTERNER L'ORDRE DES CHOIX DE RÉPONSE]
01. Oui, à ma banque/société émettrice de carte de crédit.
02. Oui, à la police, à un organisme gouvernemental ou à une autre organisation.
03. Oui, à la personne ou au service désigné à mon travail ou établissement d'enseignement.
04. Oui, à mon fournisseur de logiciel, de large bande, de téléphonie ou de réseau.
05. Oui, à mon fournisseur de messagerie ou de recherche en ligne (p. ex., Gmail).
06. Oui, au(x) fournisseur(s) des applications ou services que j'utilisais quand j'ai perdu de l'argent ou des données.
07. Oui, à mon fournisseur de services de sécurité en ligne (p. ex., Norton, McAfee).
08. Oui, j'en ai parlé à ma famille, qui a ensuite pris des mesures en mon nom.
09. [ANCRAGE; EXCLUSIF] Non, je ne l'ai pas signalé ni mentionné à personne.

QCCE3. [SI QCCE2=01-08] Quelle est la principale raison pour laquelle vous avez signalé une tentative d'hameçonnage? Si vous avez subi une perte d'argent ou de données plus d'une fois, veuillez penser à la plus récente fois où cela s'est produit. [CAB24; Q33]
01. Je trouvais important d'informer les autorités compétentes pour éviter que ça m'arrive de nouveau ou que ça arrive à quelqu'un d'autre
02. Je voulais prendre des mesures pour récupérer mon argent.
03. Je voulais que les cybercriminels se fassent attraper.
04. Autre (veuillez décrire) :

QCCE4. [SI QCCE2=09] Quelle est la principale raison pour laquelle vous n'avez pas signalé la tentative d'hameçonnage? [CAB24; Q34]
[ALTERNER L'ORDRE DES CHOIX DE RÉPONSE]
01. Je n'avais pas le temps.
02. Je ne savais pas à qui faire le signalement.
03. Je ne savais pas comment faire le signalement.
04. Le processus nécessitait trop d'efforts.
05. Ça ne servait à rien, car aucune mesure n'aurait été prise.
06. J'ai oublié de le faire.
07. J'avais trop honte.
08. Le montant d'argent ou la quantité de données était trop minime ou pas suffisamment important pour moi.
09. [ANCRAGE] Autre (veuillez préciser) :

Cybermenaces

[TOUS]
Les prochaines questions portent sur les cybermenaces. Une cybermenace est une activité visant à compromettre la sécurité d'un ordinateur.

QCT1. Au cours de la prochaine année, à quel point avez-vous l'impression qu'il est probable que vous soyez victime d'une cybermenace... [Cyber22; Q11A-D]
[ALTERNER LES CHOIX DE RÉPONSE A À C COMME UN BLOC]
a) ... compromettant vos renseignements personnels?
b) ... causant des pertes financières?
c) ... causant la perte de fichiers ou de photos?
d) … où vos données seront conservées en vue d'obtenir une rançon?

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

QCT2. [SI QCT1A-D=01, 02] Pourquoi ne croyez-vous pas qu'il est probable que vous soyez victime d'une cybermenace? [Cyber22; K8A]
Veuillez choisir toutes les réponses pertinentes

[ALTERNER L'ORDRE DES CHOIX DE RÉPONSE]
01. Je prends des mesures pour me protéger en ligne
02. Je ne fais rien de risqué en ligne
03. Le risque me semble être très mince
04. Les menaces en ligne ne s'appliquent qu'aux entreprises et gens qui ont beaucoup d'argent
05. Je reste à jour ou je suis bien informé(e) au sujet des renseignements et des virus
06. Je travaille dans le domaine de l'informatique et des technologies de l'information
07. J'utilise Apple/iOS, qui n'est pas aussi susceptible aux virus
08. J'utilise Linux, qui n'est pas aussi susceptible aux virus
09. Je n'utilise pas un système d'exploitation de Microsoft
10. [ANCRAGE] Autre réponse (veuillez préciser)
11. [ANCRAGE] Je ne sais pas

QCT3. Quels types de cybermenaces vous préoccupent le plus? [Cyber22; Q15]
Veuillez choisir toutes les réponses pertinentes
[ALTERNER L'ORDRE DES CHOIX DE RÉPONSE]
01. Tentatives d'hameçonnage
02. Virus, logiciels espions et logiciels malveillants
03. Vol d'identité
04. Atteintes à la vie privée
05. Pertes financières
06. Données personnelles ou financières conservées pour rançon (rançongiciel)
07. Perte de renseignements ou de fichiers
08. Données personnelles effacées, modifiées, perdues

09. [ANCRAGE] Autre réponse (veuillez préciser)
10. [ANCRAGE] Rien de ce qui précède
11. [ANCRAGE] Je ne sais pas

QCT4. À quel point êtes-vous bien préparé(e) pour faire face aux cybermenaces? [Cyber22; Q16-KPI]
01. Pas du tout préparé(e)
02. Pas préparé(e)
03. Assez préparé(e)
04. Bien préparé(e)
05. Très bien préparé(e)
06. Je ne sais pas

QCT5. [SI QCT4=01,02] Pourquoi n'étiez-vous pas bien préparé(e) pour faire face aux cybermenaces? [Cyber22; Q17]
Veuillez choisir toutes les réponses pertinentes

[ALTERNER L'ORDRE DES CHOIX DE RÉPONSE]
01. Je ne pense pas qu'il est probable que cela m'arrive
02. Je n'ai pas le temps ou je ne me penche jamais sur ce problème
03. Je ne connais pas les différents types de menaces
04. Je ne sais pas où obtenir des renseignements sur les mesures à prendre
05. Les renseignements que je trouve ne sont pas assez simples pour m'aider
06. Vous ne pouvez jamais vraiment vous protéger en ligne
07. Il est inutile d'essayer de se protéger
08. J'ai une copie sauvegardée et je peux m'en remettre
09. [ANCRAGE] Rien
10. [ANCRAGE] Autre (veuillez préciser)
11. [ANCRAGE] Je ne sais pas

QCT6. Avez-vous déjà été victime de l'une des cyberattaques suivantes? [Cyber22; Q18]
Veuillez choisir toutes les réponses pertinentes

[ALTERNER L'ORDRE DES CHOIX DE RÉPONSE]
01. Courriel frauduleux
02. Fraude par texto
03. Virus, logiciels espions, logiciels malveillants sur votre ordinateur
04. Vol d'identité
05. Piratage de comptes de médias sociaux
06. Hameçonnage
07. Rançongiciel
08. [ANCRAGE] Rien de ce qui précède
09. [ANCRAGE] Je ne sais pas

QCT7. **Si vous saviez ou pensiez avoir été victime d'une cyberattaque, quelles mesures prendriez-vous pour vous protéger? [Cyber22; Q19]**
Veuillez choisir toutes les réponses pertinentes

[ALTERNER L'ORDRE DES CHOIX DE RÉPONSE]
01. J'éteindrais mon ordinateur
02. Je déconnecterais tous les périphériques connectés à mon réseau
03. Je supprimerais du matériel suspect (courriel, texte, contenu téléchargé, etc.)
04. Je mettrais mon logiciel de sécurité à jour
05. Je changerais mes mots de passe
06. Je communiquerais avec ma banque
07. Je communiquerais avec les principales agences de crédit du Canada (TransUnion, Equifax)
08. Je communiquerais avec un(e) spécialiste des TI
09. Je communiquerais avec un(e) ami(e) ou un membre de ma famille pour obtenir de l'aide
10. J'appellerais la police
11. [ANCRAGE] Rien
12. [ANCRAGE] Autre (veuillez préciser)
13. [ANCRAGE] Je ne sais pas

QCT8. Croyez-vous être vulnérable à une attaque par rançongiciel? [NOUVELLE]
Ajouter une case pour du texte lorsque la souris pointe le mot : « Attaque par rançongiciel » : Un rançongiciel est un type de logiciel malveillant qui bloque l'accès de la victime à ses données personnelles jusqu'à ce qu'une somme d'argent (une rançon) soit payée.
01. Oui
02. Non
03. Je ne sais pas si je suis vulnérable à une attaque par rançongiciel

QCT9. Si vous étiez victime d'une attaque par rançongiciel, que feriez-vous? [NOUVELLE]
Veuillez choisir toutes les réponses pertinentes

[ALTERNER L'ORDRE DES CHOIX DE RÉPONSE]
01. Prendre une photo du message du rançongiciel
02. Signaler l'attaque à la police locale
03. Déconnecter mon appareil d'Internet
04. Éteindre ma connexion Internet
05. Déconnecter les dispositifs de stockage externes comme des lecteurs de disques durs, des clés USB et le nuage
06. Appeler un(e) ami(e) ou un membre de la famille pour de l'aide
07. Effectuer des recherches pour trouver une solution
08. Exécuter un logiciel antivirus
09. Réinitialiser tous mes mots de passe
10. Appeler une entreprise spécialisée dans le soutien technique pour obtenir de l'aide
11. [ANCRAGE] Autre (veuillez préciser)
12. [ANCRAGE] Je ne sais pas

Intelligence artificielle

[TOUS]
Les prochaines questions portent sur l'intelligence artificielle (IA).

QAI1 : Utilisez-vous des outils de l'intelligence artificielle (IA)* à la maison ou au travail? [CAB24; Q72]
***Par exemple : ChatGPT, CoPilot, DALL-E.**

01. Oui, à la maison seulement.
02. Oui, au travail seulement.
03. Oui, à la maison et au travail.
04. Non, je n'utilise pas d'outils de l'IA.

QAI3. Dans quelle mesure avez-vous confiance en votre capacité de reconnaître du contenu généré par l'IA (p. ex., messages, photos, vidéos, hypertrucages)? [CAB24; Q77]
1-Pas du tout confiant(e)
2
3
4
5
6
7
8
9
10-Très confiant(e)
Je ne sais pas

Entreprises et cybersécurité

[ENTREPRISE : SI S8=01-04 ET S9=01 OU S10=01-03]

Pour ce qui est de votre travail,

QBUS1. Qui est responsable des TI pour votre société? [Cyber22; QBUS4]
Veuillez choisir toutes les réponses pertinentes

[ALTERNER L'ORDRE DES CHOIX DE RÉPONSE]
01. Moi
02. Un autre employé(e) (préciser le rôle au sein de la société) :
03. Un(e) employé(e) de l'organisation qui se consacre aux TI
04. Firme de TI en sous-traitance
05. [ANCRAGE] Personne
06. [ANCRAGE] Autre (veuillez préciser)
07. [ANCRAGE] Rien de ce qui précède
08. [ANCRAGE] Je ne sais pas
09. [ANCRAGE] Je préfère ne pas répondre

QBUS2. Quelles mesures parmi les suivantes votre entreprise a-t-elle prises pour se protéger contre les cybermenaces? [Cyber22; BUS1]
Veuillez choisir toutes les réponses pertinentes

[ALTERNER L'ORDRE DES CHOIX DE RÉPONSE]
01. Tenir à jour les logiciels de sécurité sur tous les appareils
02. Établir des filtres de pourriels

03. Exiger que l'accès à tous les appareils soit protégé par mot de passe
04. Sauvegarder l'information sur tous les appareils
05. Utiliser un logiciel de cryptage
06. Ne pas utiliser de compte d'administrateur pour l'accès au Web
07. Utiliser un mot de passe ou une authentification d'utilisateur pour l'accès sans fil et à distance
08. Suivre les protocoles de suppression de l'information lorsque les employés quittent l'organisation
09. Offrir aux employé(e)s une formation sur les pratiques exemplaires en matière de cybersécurité
10. Adopter une politique en matière de cybersécurité à l'intention des employé(e)s
11. [ANCRAGE] Rien de ce qui précède
12. [ANCRAGE]Je ne sais pas
13. [ANCRAGE] Je préfère ne pas répondre

QBUS3. **De quels types de renseignements parmi les suivants croyez-vous que votre organisation tirerait profit pour se protéger contre les cybermenaces? [Cyber22; QBUS3]**

Veuillez choisir toutes les réponses pertinentes

[ALTERNER L'ORDRE DES CHOIX DE RÉPONSE]
01. Liste de types de menaces qui existe et signaux à rechercher
02. Conseils pour communiquer aux employé(e)s l'importance de suivre des politiques de cybersécurité
03. Pratiques exemplaires pour une politique d'utilisation d'Internet claire
04. Directives pour mettre en place des règles relatives à la politique d'utilisation sécuritaire des courriels
05. Directives sur la façon d'établir une politique en matière de médias sociaux
06. Conseils et ressources pour le type de logiciel ou matériel permettant de sécuriser des réseaux
07. Pratiques exemplaires sur la façon pour les employé(e)s de gérer les mots de passe
08. Mesures pour protéger les appareils mobiles dans un lieu public
09. Mesures pour gérer les renseignements liés au travail que possèdent les employé(e)s qui quittent l'organisation
10. Directives pour réagir à une cyberattaque
11. Pratiques exemplaires sécuritaires en informatique en nuage (avec la définition)
12. Pratiques exemplaires pour l'utilisation de dispositifs de stockage (p. ex., clés USB)
13. Ressources sur la façon de crypter des ordinateurs, portables et dispositifs de stockage
14. Directives sur l'utilisation de dispositifs personnels au travail
15. [ANCRAGE] Autre réponse (veuillez préciser)
16. [ANCRAGE] Rien de ce qui précède
17. [ANCRAGE] Je ne sais pas
18. [ANCRAGE] Je préfère ne pas répondre

QBUS4. 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... [Cyber22; QBUS5A1-4]
[ALTERNER L'ORDRE DES ÉNONCÉS]
a) ... causer des interruptions de travail?
b) ... porter atteinte à la réputation de votre organisation?
c) ... causer des pertes financières?

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

[CHOIX DE RÉPONSE]
1- Pas du tout préoccupé(e)
2
3
4- Moyennement préoccupé(e)
5
6
7- Extrêmement préoccupé(e)
Je ne sais pas
Je préfère ne pas répondre

QBUS5. Selon vous, dans quelle mesure votre entreprise est-elle préparée actuellement pour se défendre contre des attaques par rançongiciel? [NOUVELLE]
1-Pas du tout préparée
2
3
4-Moyennement préparée
5
6
7-Extrêmement préparée
Je ne sais pas
Je préfère ne pas répondre

QBUS6. Qu'a fait, s'il y a lieu, votre entreprise pour se protéger contre les attaques par rançongiciel? [NOUVELLE]
Veuillez choisir toutes les réponses pertinentes

[ALTERNER L'ORDRE DES CHOIX DE RÉPONSE]
01. Sensibiliser les employé(e)s
02. Tenir à jour les systèmes d'exploitation, les logiciels et les applications
03. Interdire aux employé(e)s d'installer et d'exécuter des logiciels
04. Restreindre l'accès aux logiciels aux employé(e)s qui en ont besoin
05. Utiliser un logiciel antivirus
06. Utiliser l'authentification multifactorielle (AMF)
07. Sauvegarder régulièrement les fichiers de l'entreprise
08. Stocker des copies de fichiers à l'extérieur du Web
09. Exécuter des simulations d'attaques par rançongiciel pour pratiquer la réponse de l'entreprise
10. [ANCRAGE] Autre (veuillez préciser)
11. [ANCRAGE] Rien de ce qui précède
12. [ANCRAGE] Je ne sais pas
13. [ANCRAGE] Je préfère ne pas répondre

QBUS7. Dans quelle mesure votre entreprise serait-elle en mesure de se remettre d'une attaque d'un rançongiciel? [Cyber22; BUSBA42]
1- Très difficilement
2

3
4- Difficilement mais assez bien
5
6
7- Facilement, avec des conséquences limitées
Je ne sais pas
Je préfère ne pas répondre

Besoins en matière d'information et préférences liées aux communications

[TOUS]
Vous avez presque terminé de répondre au sondage. Merci de nous avoir fait part de vos opinions.

QINFO1. Veuillez indiquer dans quelle mesure vous êtes d'accord ou en désaccord avec les énoncés ci-dessous. [Cyber22; QA13, 111B, 118, A120; C=KPI]
[ALTERNER L'ORDRE DES ÉNONCÉS]
a) Je suis assez bien renseigné(e) sur les mesures à prendre pour me protéger et pour protéger mes appareils contre les cybermenaces.
b) J'ai confiance de pouvoir me protéger en ligne si je dispose de renseignements fiables sur les mesures à prendre.
c) J'ai confiance que je saurai comment trouver des renseignements pratiques que je peux utiliser pour me protéger en ligne
d) J'ai confiance que les entreprises et les autres organisations disposent de mesures de protection adéquates pour protéger mes renseignements personnels.

[CHOIX DE RÉPONSE]
1-Fortement en désaccord
2-2
3-3
4-Ni d'accord ni en désaccord
5-5
6-6
7-Fortement d'accord
Je ne sais pas

QINFO2. Comment préférez-vous obtenir de l'information pour vous protéger contre les cybermenaces? [Cyber22; Q20]
Veuillez choisir toutes les réponses pertinentes

[ALTERNER L'ORDRE DES CHOIX DE RÉPONSE]
01. Balados
02. Blogues
03. Fiches d'information ou infographies
04. Listes de choses à faire
05. Vidéos didactiques
06. Histoires sur la façon dont les gens ont été touchés
07. Renseignements sur des sites Web
08. Brochures imprimées
09. Bulletins d'information (p. ex., abonnement à un courriel)

10. Médias sociaux
11. [ANCRAGE] Autre (veuillez préciser)
12. [ANCRAGE] Rien de ce qui précède
13. [ANCRAGE] Je ne sais pas

Campagne Pensez cybersécurité

[TOUS]
QGCS1. Une campagne de sensibilisation du gouvernement du Canada a été créée pour informer les Canadiens et les Canadiennes sur la cybersécurité et sur les mesures simples qu'ils et qu'elles peuvent prendre pour se protéger en ligne. Pouvez-vous nommer cette campagne? [Cyber22; Q23-KPI]
01. Oui
02. Non [PASSER À QGCS3]
03. Je ne sais pas [PASSER À QGCS3]

QGCS2. [SI QGCS1=01] Quel est le nom de cette campagne?
[OUVERT]

QGCS3. 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? [Cyber22; GOCAD-KPI]
01. Oui
02. Non [PASSER À D1]
03. Je ne sais pas [PASSER À D1]

QGCS4. [SI QGCS3=01] Où l'avez-vous vu, lu ou entendu? [Cyber22; GOCADA]
[ALTERNER L'ORDRE DES CHOIX DE RÉPONSE]
01. J'ai visité le site Web pensezcybersecurite.gc.ca
02. J'en ai entendu parler à une émission de radio ou dans une baladodiffusion
03. Je l'ai vu dans les médias sociaux
04. J'ai vu une vidéo en ligne
05. Quelqu'un m'en a parlé
06. J'ai vu un segment sur les nouvelles ou dans le journal
07. [ANCRAGE] Autre réponse (veuillez préciser)
08. [ANCRAGE] Je ne sais pas

Renseignements démographiques

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

D1. À quel genre vous identifiez-vous?
01. Homme
02. Femme
03. Je m'identifie à un autre genre
04. Je préfère ne pas répondre

D2. Quel est le plus haut niveau de scolarité que vous avez atteint?
01. École primaire ou moins
02. École secondaire
03. Un peu d'études postsecondaires
04. Collège, école technique ou de métier
05. Programme universitaire de premier cycle
06. Programme universitaire de 2e ou 3e cycles, ou professionnel
07. Je préfère ne pas répondre

D3. 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?
01. Moins de 20 000 $
02. De 20 000 $ à un peu moins de 40 000 $
03. De 40 000 $ à un peu moins de 60 000 $
04. De 60 000 $ à un peu moins de 80 000 $
05. De 80 000 $ à un peu moins de 100 000 $
06. De 100 000 $ à un peu moins de 150 000 $
07. 150 000 $ et plus
08. Je préfère ne pas répondre

Page de clôture

Le sondage est terminé. Il a été mené au nom du Centre de la sécurité des télécommunications. Au cours des prochains mois, un rapport contenant les résultats de l'étude sera disponible auprès de Bibliothèque et Archives Canada. Merci à toutes les personnes qui ont participé au projet. Nous l'apprécions beaucoup.