Government of Canada / Gouvernement du Canada

Sondage de suivi sur la connaissance de la campagne Pensez cybersécurité : Rapport final de 2026

Préparé pour le Centre de la sécurité des télécommunications Canada

Nom du fournisseur : Phoenix Strategic Perspectives Inc.
Numéro de contrat : CW2426715
Valeur du contrat : 79 075,00 $ (incluant les taxes applicables)
Date d'attribution du contrat : 2025-11-04
Date de présentation du rapport : 2026-03-11
Numéro d'enregistrement : POR nº 052-25

Pour plus d'information au sujet de ce 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 pour le Centre de la sécurité des télécommunications Canada
Nom du fournisseur : Phoenix Strategic Perspectives Inc.

Ce rapport de recherche sur l'opinion publique présente les résultats d'un sondage en ligne mené par Phoenix SPI auprès de 2 300 Canadiennes et Canadiens de 18 ans et plus pour le compte du Centre de la sécurité des télécommunications Canada (CST) entre le 9 et le 29 janvier 2026.

This publication is also available in English under the title : *Get Cyber Safe Awareness Tracking Survey: 2026 Final Report.*

Numéro de catalogue :

- D96-17/2026F-PDF

Numéro international normalisé du livre (ISBN) :

- 978-0-660-98884-9

Publications connexes (numéro d'enregistrement : POR 052-25) :

- **Numéro de catalogue :** D96-17/2026E-PDF
- **ISBN :** 978-0-660-98883-2

Préparé pour le Centre de la sécurité des télécommunications Canada

Table des matières

Liste des diagrammes

Sommaire

Le Centre de la sécurité des télécommunications Canada (CST) a chargé Phoenix Strategic Perspectives Inc. (Phoenix SPI) de mener le sondage de suivi en ligne sur la connaissance de la campagne Pensez cybersécurité, réalisé aux deux ans.

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, l'équipe de marketing du CST dirige la campagne nationale de sensibilisation du public Pensez cybersécurité[1], qui a été créée pour renseigner les Canadiennes et les Canadiens au sujet de la cybersécurité et des mesures simples qu'ils peuvent prendre pour se protéger en ligne.

Dans le contexte de la campagne, le CST mène tous les deux ans depuis 2020 une recherche sur l'opinion publique (ROP) quantitative axée sur les attitudes et les connaissances des Canadiennes et des Canadiens à l'égard de la cybersécurité. La ROP complète la recherche sur la cybersécurité effectuée par Sécurité publique Canada en 2011, 2017 et 2018. Les constatations issues des deux enquêtes fournissent un aperçu à long terme de la façon dont les Canadiennes et les Canadiens gèrent la cybersécurité afin d'assurer leur propre protection et celles de leurs proches. Les résultats révèlent une progression dans certains secteurs, mais mettent également en lumière les vulnérabilités de la population face aux cybermenaces.

Pour cette itération de l'enquête, les objectifs étaient les suivants :

- évaluer l'efficacité de la campagne de sensibilisation du public Pensez cybersécurité et 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 au sein des publics ciblés;
- déterminer et suivre les facteurs de motivation et les obstacles au changement de comportement;
- déterminer et suivre les meilleures façons de communiquer l'information relative à la cybersécurité;
- réaliser un suivi des attentes du public en ce qui a trait à la participation du gouvernement fédéral.

Les résultats de la ROP de cette année éclaireront l'orientation de la campagne Pensez cybersécurité, du Centre pour la cybersécurité ainsi que d'autres communications et messages publics du CST.

Méthodologie

Un sondage en ligne de 15 minutes a été mené auprès de 2 330 Canadiennes et Canadiens en ligne de 18 ans et plus. Entre autres, 846 parents d'enfants de moins de 18 ans y ont répondu, tout comme 300

[1] La campagne Pensez cybersécurité a été mise au point en 2011 par Sécurité publique Canada dans le cadre de la Stratégie nationale de cybersécurité du Canada. Les premiers documents relatifs à la planification de la campagne du Secrétariat du Conseil du Trésor (SCT) mentionnaient la nécessité de mener régulièrement une ROP au sujet de la cybersécurité, ce qu'a fait Sécurité publique Canada.

personnes qui sont propriétaires ou gestionnaires d'une petite ou 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 Canadiennes et des Canadiens 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 9 au 29 janvier 2026. De plus amples renseignements sur la méthodologie se trouvent à l'annexe Spécifications techniques.

Principales constatations

Les pratiques relatives à la cybersécurité des Canadiennes et des Canadiens en ligne

Plus de huit Canadiennes et Canadiens en ligne (84 %) ont déclaré qu'ils prenaient des précautions pour protéger leurs comptes en ligne et dans les médias sociaux, ainsi que leurs appareils et réseaux. Près des deux tiers (63 %) ne supposent pas que leurs appareils sont automatiquement sécurisés.

En ce qui concerne les mises à jour des logiciels, un peu plus de huit personnes sur 10 (82 %) savent comment installer les plus récentes mises à jour de logiciels et d'applications sur leurs appareils. Parmi ces répondants, 87 % le font régulièrement et 46 % le font toujours lorsqu'ils reçoivent une notification leur indiquant qu'une mise à jour est disponible. Les personnes qui installent régulièrement des mises à jour ont tendance à le faire immédiatement : 52 % ont activé la fonction des mises à jour automatiques et 17 % procèdent à la mise à jour dès qu'elles reçoivent une notification à cet effet.

Outre l'installation des mises à jour, les Canadiennes et les Canadiens en ligne sont généralement au courant des mesures possibles pour sécuriser leurs comptes et ont tendance à les utiliser. Une grande majorité (94 %) a entendu parler de l'authentification multifactorielle (AMF) et la plupart des personnes qui connaissent l'AMF (86 %) savent comment l'activer et l'utilisent régulièrement. Parmi les personnes qui n'utilisent plus l'authentification multifactorielle, la plus grande proportion (34 %) d'entre elles ont indiqué que l'AMF prend trop de temps.

Les Canadiennes et les Canadiens en ligne 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 (55 %) contient « https ». Environ la moitié des répondants (49 %) mènent des recherches pour valider la légitimité d'un site Web, alors que 40 % lisent des commentaires au sujet du respect de la confidentialité et de la réputation du site Web et 38 % vérifient si la barre d'adresse du site Web renferme un cadenas verrouillé.

La plupart des Canadiennes et des Canadiens en ligne reconnaissent les signes courants de tentatives d'hameçonnage, y compris des messages portant sur des comptes qu'ils n'ont pas ou des livraisons inattendues (88 %), des demandes de renseignements sensibles (87 %) 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 de personnes sondées reconnaissent que les messages proposant des offres trop bonnes pour être vraies (84 %) et renfermant des pièces jointes inattendues ou inutiles (79 %) sont également des signes de tentatives d'hameçonnage. Les trois quarts des répondants (76 %) remarquent le langage insistant ou menaçant, tandis que les deux tiers (65 %) des répondants associent un graphisme non professionnel à une tentative d'hameçonnage.

La majorité des Canadiennes et des Canadiens (77 %) en ligne déclarent avoir créé des mots de passe complexes en utilisant une combinaison de lettres, de chiffres et de symboles. De plus petites proportions de répondants utilisent un gestionnaire de mots de passe (35 %), un mot de passe unique pour chaque compte (32 %) ou une phrase de passe (14 %). Pour les comptes importants, la moitié des personnes se servent de mots de passe uniques en tout temps (31 %) ou la plupart du temps (28 %).

Alors que bon nombre de Canadiennes et de Canadiens adoptent des pratiques qui aideront à protéger leurs comptes en ligne, certains comportements pourraient mettre leur compte à risque. Par exemple, 38 % des répondants permettent aux navigateurs ou aux applications d'inscrire automatiquement leurs mots de passe, 27 % prennent en note leurs mots de passe et 26 % utilisent le même mot de passe pour plusieurs comptes. Parmi les personnes qui utilisent rarement, voire jamais, de mots de passe uniques, 62 % disent qu'il est difficile de se souvenir de différents mots de passe.

La cybercriminalité et les menaces

Huit Canadiennes et Canadiens sur 10 (81 %) en ligne n'ont jamais été victimes d'une escroquerie en ligne leur ayant fait perdre de l'argent ou des données. Cela dit, plus de la moitié des répondants ont été victimes d'autres types de cyberattaques, la plupart du temps des courriels frauduleux (31 %), des fraudes par texto (26 %), des attaques de la part d'un logiciel malveillant (26 %) ou des arnaques par hameçonnage (26 %). Malgré le faible nombre d'incidents déclarés, les inquiétudes sont importantes : près des trois quarts (73 %) des Canadiennes et des Canadiens en ligne s'inquiètent de la cybercriminalité liée à l'intelligence artificielle (IA) et plus de la moitié (56 %) craignent d'être victimes de la cybercriminalité en général. De plus, une forte minorité de répondants pensent qu'il est probable qu'ils soient victimes d'au moins l'une des nombreuses cybermenaces au cours de la prochaine année : une cybermenace qui compromet la sécurité de leurs renseignements personnels (26 %), qui cause la perte de fichiers ou de photos (10 %) ou qui entraîne des pertes financières (9 %).

Lorsqu'on leur a demandé quels types de cybermenaces les inquiètent le plus, le vol d'identité arrive en tête de liste (76 % des Canadiennes et des Canadiens en ligne l'ont mentionné), suivi des pertes financières (64 %) et des virus, logiciels espions et logiciels malveillants (59 %). De plus petites proportions craignent les atteintes à la vie privée (48 %), la perte de données personnelles (45 %) et les attaques par hameçonnage (42 %). La perte d'informations se classe au dernier rang (37 % des répondants en ont fait mention). Même si les trois quarts des Canadiennes et des Canadiens (73 %) disent avoir confiance qu'ils pourront repérer les tentatives d'hameçonnage, 35 % ont déclaré que cette menace les préoccupe.

La majorité des Canadiennes et des Canadiens en ligne ont déclaré être assez (43 %) ou bien (28 %) préparés pour faire face aux cybermenaces. Le quart (25 %) d'entre eux ont dit qu'ils ne se sentaient pas préparés. Ils ont principalement invoqué deux raisons : 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) et la futilité (il n'est pas possible de se protéger en ligne).

En ce qui concerne les différents types d'attaque, 4 % des personnes sondées ont été victimes d'une attaque par rançongiciel, 4 % pensent qu'il est probable qu'elles soient victimes d'une telle attaque au cours de la prochaine année et 26 % pensent qu'elles sont vulnérables à ce type d'attaque. De plus, un quart des répondants (26 %) ont été victimes d'hameçonnage et 8 % ont subi une telle attaque et ont perdu de l'argent ou des données.

Les points de vue concernant l'intelligence artificielle

Soixante-deux pour cent des Canadiennes et des Canadiens en ligne ont déclaré avoir utilisé des outils de l'IA, comme ChatGPT, CoPilot, DALL-E : 32 % se servent des outils de l'IA au travail et à la maison, 24 % les utilisent à la maison seulement et 6 % les utilisent uniquement au travail. Quatre répondants sur 10 (42 %) disent avoir confiance en leur capacité à repérer des messages, images ou vidéos générés par l'IA, ou des hypertrucages, et une proportion supplémentaire de 30 % indiquent qu'ils ont assez confiance.

Les communications et la campagne Pensez cybersécurité

Les trois quarts des Canadiennes et des Canadiens (75 %) sont convaincus qu'ils peuvent se protéger en ligne s'ils disposent de renseignements fiables concernant les mesures à prendre. Les deux tiers (67 %) estiment savoir comment trouver des renseignements pratiques pour assurer leur protection en ligne et plus de la moitié (56 %) jugent qu'ils disposent de suffisamment d'information sur les mesures à prendre pour se protéger contre les cybermenaces.

Pour ce qui est des préférences en matière de communications, 59 % des Canadiennes et des Canadiens en ligne préféreraient obtenir de l'information pour se protéger contre les cybermenaces au moyen de sites Web. Les vidéos didactiques (41 %) et les listes de choses à faire (37 %) sont d'autres options appréciées. Environ le tiers des personnes sondées seraient intéressées par des fiches d'information ou des infographies (35 %) ou les médias sociaux (33 %).

Très peu de gens (4 %) peuvent nommer spontanément la campagne Pensez cybersécurité du gouvernement du Canada. Parmi les personnes se disant au courant de la campagne lorsqu'on faisait un rappel assisté, un répondant sur 10 (10 %) a indiqué connaître la campagne. Un peu plus du tiers (37 %) de ces répondants (n=223) en avaient entendu parler dans les médias sociaux. Environ deux personnes sur 10 ont vu une vidéo en ligne (24 %), un segment aux nouvelles ou dans le journal (22 %), ou en ont entendu parler dans une émission de radio ou un balado (22 %). Un nombre moins important de personnes ont visité le site Web de pensezcybersecurite.ca (17 %) ou ont entendu parler de la campagne par une autre personne (12 %).

Les entreprises et la cybersécurité

La plupart des propriétaires et gestionnaires d'entreprise (77 %) 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 (59 %), 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 d'utilisateur pour l'accès sans fil et à distance (52 %).

Lorsqu'il s'agit de protéger leur entreprise contre les cybermenaces, environ un tiers des répondants ont déclaré que leur organisation pourrait tirer parti de directives pour réagir à une cyberattaque (36 %), d'une liste des types de menaces qui existent et des signaux à rechercher (36 %), des pratiques

exemplaires sécuritaires en informatique en nuage (35 %), ou de conseils ou de ressources concernant les logiciels ou le matériel informatique permettant de sécuriser les réseaux (35 %).

En ce qui a trait aux activités courantes de leur entreprise, deux entreprises sur 10 sondées sont préoccupées par les interruptions de travail (19 %) et presque autant s'inquiètent des pertes financières (18 %) ou des atteintes à la réputation de l'organisation (17 %). Seize pour cent craignent que les données de leur entreprise ne soient conservées en vue d'obtenir une rançon.

Les deux tiers des entreprises sont à tout le moins modérément préparés 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 l'AMF (55 %), la mise à jour des systèmes d'exploitation, des logiciels et des applications (52 %), la sauvegarde de fichiers (45 %), l'utilisation de logiciels antivirus (42 %), la sensibilisation des employés (35 %), le stockage de copies de fichiers à l'extérieur du Web (34 %) et l'accès restreint aux logiciels (33 %). Bien qu'ils soient préparés dans une certaine mesure, la moitié des propriétaires et gestionnaires d'entreprise prévoient qu'il faudrait déployer des efforts (38 %) pour se remettre d'une attaque par rançongiciel ou qu'il serait difficile (13 %) de s'en remettre.

Observations finales

En général, on observe très peu de changements dans les connaissances et les comportements des Canadiennes et des Canadiens concernant la sécurité en ligne depuis le sondage de 2024. Voici les observations finales :

- *L'adoption de comportements pour assurer sa protection demeure stable.* La majorité des Canadiennes et des Canadiens en ligne continuent de prendre des mesures pour protéger leurs comptes en ligne, leurs médias sociaux, leurs appareils et leurs réseaux. La plupart d'entre eux savent comment installer les dernières mises à jour de logiciels et d'applications et le font régulièrement. On observe un plus haut taux de connaissances relatives à l'authentification multifactorielle, bien que la proportion de ces utilisateurs soit restée inchangée depuis 2024. La majorité des répondants affirment vérifier très souvent ou toujours les messages pour détecter des signes d'hameçonnage, et plus de la moitié d'entre eux analysent l'aspect général d'un site Web ou vérifient si la barre d'adresse contient « https : » pour en confirmer la légitimité. Ces comportements sont restés inchangés au fil du temps. Enfin, bon nombre de Canadiennes et de Canadiens en ligne disent utiliser la plupart du temps des mots de passe complexes et uniques pour leurs comptes importants.
- *Les connaissances relatives aux outils de l'IA et le recours à ces derniers ont augmenté.* On observe une augmentation importante comparativement à 2024 dans la proportion de Canadiennes et de Canadiens en ligne disant avoir recours à des outils d'IA; l'utilisation de tels outils a presque doublé. La plus forte augmentation concerne les personnes qui se servent des outils de l'IA à la fois au travail et à la maison. Ce constat reflète probablement la croissance rapide de l'industrie de l'IA et l'acceptation plus générale de l'IA dans les milieux de travail. La confiance des répondants à pouvoir repérer du contenu généré par l'IA a également considérablement augmenté, possiblement en raison d'une plus grande exposition et d'une sensibilisation accrue. Malgré une augmentation des connaissances et de l'utilisation, les inquiétudes concernant la cybercriminalité liée à l'IA continuent de s'intensifier.
- *L'hameçonnage demeure une préoccupation.* Bien que la plupart des Canadiennes et des Canadiens en ligne disent vérifier les messages pour détecter des signes d'hameçonnage et estiment être capables de repérer de telles tentatives, certains sont encore des victimes d'arnaques qui mènent à

la perte d'argent ou de renseignements personnels, et la proportion de répondants signalant une attaque a augmenté au fil du temps. Le volume persistant de messages frauduleux, combinés aux avancées en matière d'IA qui donnent lieu à des arnaques encore plus sophistiquées, pourrait contribuer à cette tendance. Plusieurs Canadiennes et Canadiens en ligne continuent de s'inquiéter des tentatives d'hameçonnage et près d'un tiers d'entre eux font appel à d'autres personnes pour les aider à identifier des arnaques potentielles ou des messages d'hameçonnage, ce qui fait ressortir la nécessité de poursuivre des initiatives de sensibilisation du public comme la campagne Pensez cybersécurité.

Notes à l'intention du lecteur

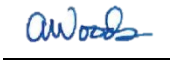
- Les prochaines sections renferment les constatations détaillées. Les résultats sont présentés dans le corps du texte et s'appuient généralement sur un graphique ou un tableau.
- Tous les résultats sont exprimés en pourcentage, sauf indication contraire. Tout au long du rapport, les pourcentages peuvent 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 suivent généralement 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 un modèle ou une tendance ou en font partie sont présentées dans le rapport.
- Le cas échéant, les résultats sont comparés à ceux de sondages similaires menés en 2018, 2020, 2022 et 2024. À moins d'une indication claire dans le rapport, les différences observées au fil du temps ne sont pas statistiquement significatives.
- Le questionnaire du sondage est annexé au rapport.

Valeur du contrat

La valeur du contrat était de 79 075,00 $ (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

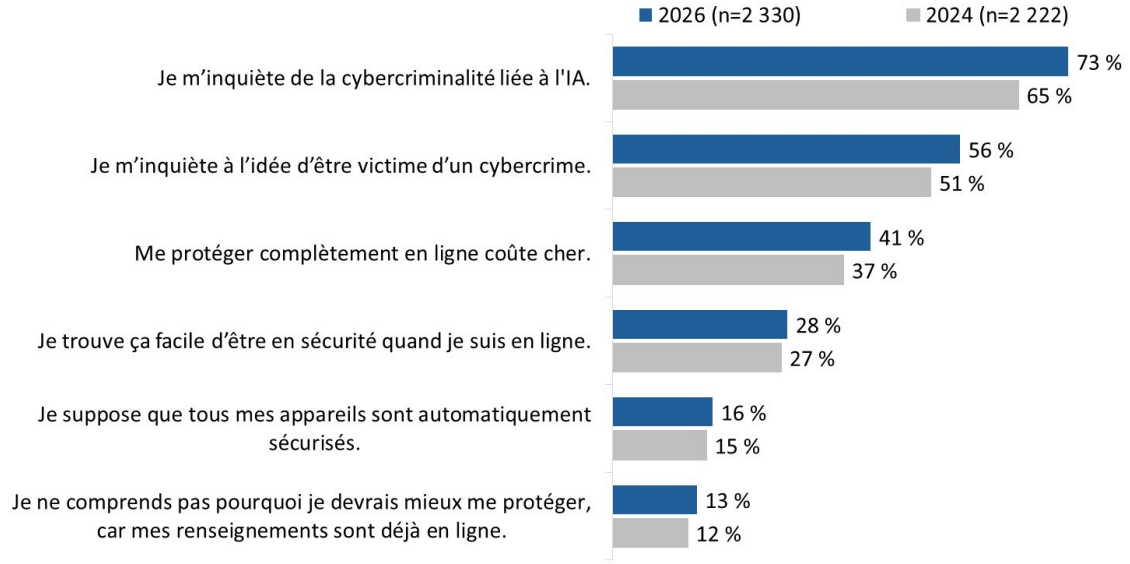
1. Les points de vue et attitudes à l'égard de la cybersécurité

La majorité des Canadiens et des Canadiennes s'inquiètent de la cybercriminalité et les préoccupations se sont intensifiées depuis 2024

On a demandé aux répondants d'indiquer dans quelle mesure ils étaient d'accord ou en désaccord avec six 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 ». Près des trois quarts (73 %) des Canadiennes et des Canadiens en ligne s'inquiètent de la cybercriminalité liée à l'intelligence artificielle (IA) (cotes de 7 à 10 sur une échelle de 10 points), ce qui représente une hausse de 8 points de pourcentage par rapport à 2024 (65 %). Un peu plus de la moitié (56 %) des répondants craignent d'être victimes d'un acte de cybercriminalité en général. Il s'agit encore là d'une hausse par rapport à 2024 (51 %).

Les opinions concernant les comportements personnels en matière de cybersécurité sont généralement cohérentes avec celles de 2024. Quatre personnes sur dix (41 %, ce qui représente une légère hausse par rapport à 37 % en 2024) estiment coûteux de se protéger pleinement en ligne, et environ trois répondants sur dix (28 %) trouvent qu'il est facile d'assurer leur sécurité en ligne. Relativement peu de gens supposent que leurs appareils sont automatiquement sécurisés (16 %) ou jugent qu'il n'y a aucun intérêt à protéger leurs informations, car elles sont déjà en ligne (13 %).

Diagramme 1 : Attitudes à l'égard de la sécurité en ligne : % de répondants d'accord avec l'énoncé



QSC1. À quel point êtes-vous d'accord avec les énoncés suivants sur la cybersécurité? Base de référence : 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 la probabilité d'être victime de cybercriminalité. Les personnes de 18 à 34 ans sont plus susceptibles que les gens

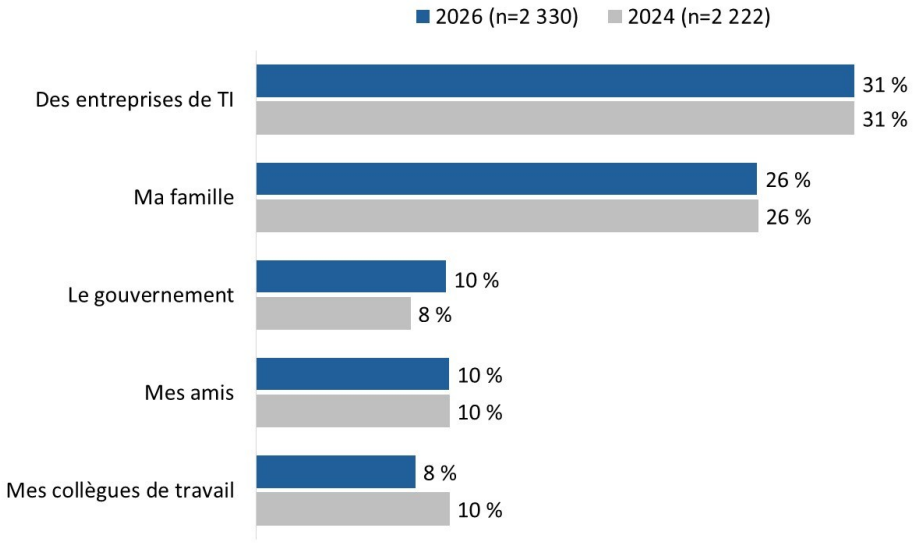
plus âgés de penser qu'il est peu probable qu'ils soient la cible d'un cybercrime et de trouver facile d'assurer leur sécurité en ligne.

- Les répondants milléniaux et de la génération X sont plus enclins à dire que des membres de leur famille font appel à eux pour assurer leur sécurité en ligne.
- Les femmes ont plus tendance que les hommes à être préoccupées par l'utilisation de l'IA aux fins de la cybercriminalité. En revanche, les hommes sont plus susceptibles que les femmes de penser qu'il est facile d'être en sécurité en ligne et de dire que des membres de leur famille se tournent vers eux pour assurer leur sécurité en ligne.
- Les personnes qui possèdent des connaissances de base ou qui sont novices en matière de sécurité en ligne sont plus susceptibles de trouver qu'il coûte cher de se protéger pleinement en ligne, de présumer que leurs appareils sont sécurisés, de croire qu'il est inutile d'essayer d'être en sécurité en ligne et de s'inquiéter de devenir des victimes de la cybercriminalité.

Les principales sources de conseils en matière de cybersécurité sont en grande partie les mêmes que celles mentionnées en 2024

Les Canadiennes et les Canadiens en ligne continuent de se tourner principalement vers les entreprises des technologies de l'information (TI) (31 %) et les membres de leur famille (26 %) pour obtenir de l'aide ou des conseils en matière de cybersécurité. Deux répondants sur 10 font appel au gouvernement (10 %) ou à des amis (10 %), tandis que moins d'un répondant sur 10 (8 %) demande à ses collègues.

Diagramme 2 : Source de soutien en matière de cybersécurité



QSC2. Sur qui comptez-vous le plus pour obtenir de l'aide ou des conseils en matière de cybersécurité? Base de référence : tous les répondants.

Les personnes âgées de 65 ans et plus sont les plus susceptibles de compter sur leur famille pour obtenir de l'aide ou des conseils en matière de cybersécurité, tandis que celles de 18 à 34 ans sont plus enclines à se tourner vers leurs amis pour obtenir de tels conseils. Les résidents du Québec sont les plus susceptibles de compter sur le gouvernement pour obtenir de l'aide ou des conseils dans ce domaine, tandis que ceux qui possèdent des connaissances de base ou qui sont novices par rapport à la sécurité en ligne ont plus

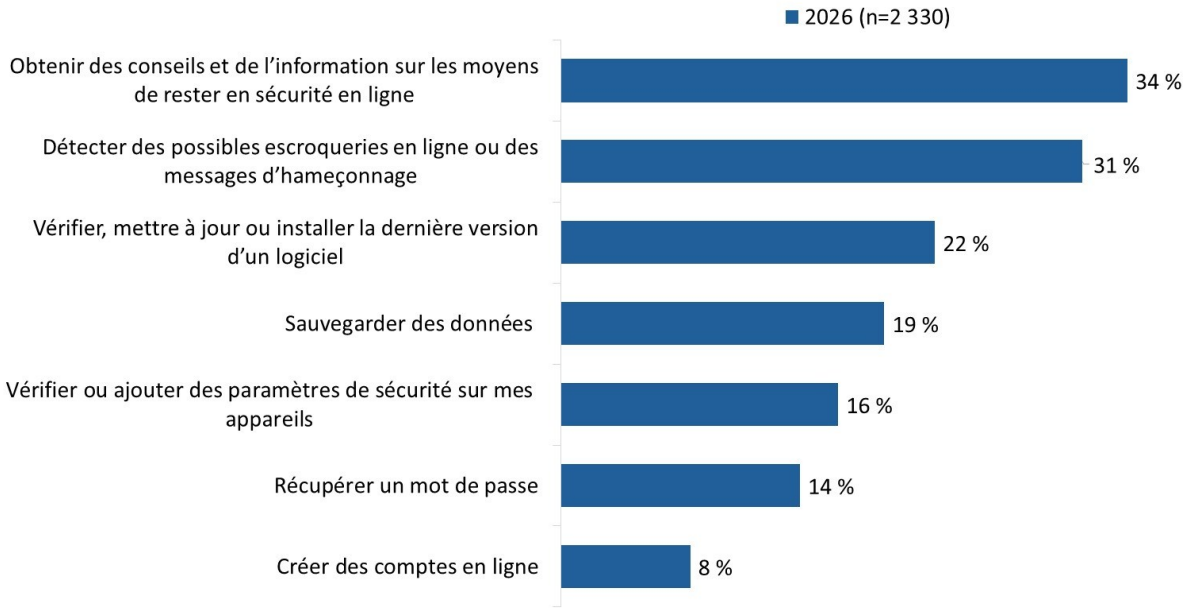
tendance à faire appel à leur famille. Les hommes sont plus susceptibles de compter sur leurs amis et les entreprises de TI, tandis que les femmes ont plus tendance à demander à leur famille.

Les Canadiennes et les Canadiens comptent sur d'autres personnes pour obtenir de l'aide dans diverses activités en ligne

Environ un tiers des Canadiennes et des Canadiens en ligne comptent sur d'autres personnes pour obtenir des conseils et de l'information sur les façons d'assurer leur sécurité en ligne (34 %) et pour aider à repérer d'éventuelles arnaques ou des messages d'hameçonnage (31 %). De plus, 22 % se tournent vers d'autres personnes pour vérifier, mettre à jour ou installer des mises à jour de logiciels, 19 % le font pour sauvegarder leurs données, 16 % pour vérifier ou ajouter des paramètres de sécurité sur leurs appareils, et 14 % pour récupérer des mots de passe. Moins d'un répondant sur dix (8 %) a besoin d'aide pour créer des comptes en ligne.

La dépendance envers d'autres personnes pour des tâches de cybersécurité varie selon les groupes démographiques. Les répondants plus âgés sont plus susceptibles de faire appel à d'autres personnes pour obtenir des conseils; c'est davantage le cas pour les baby-boomers et les répondants de la génération silencieuse que pour les milléniaux, ainsi que les membres de la génération Z et de la génération X. Les femmes sont plus enclines que les hommes à demander l'aide d'autres personnes. En revanche, les personnes possédant des connaissances approfondies de la sécurité en ligne ont moins tendance à dépendre d'autres personnes pour exécuter ces tâches.

Diagramme 3 : Activités pour lesquelles du soutien est nécessaire

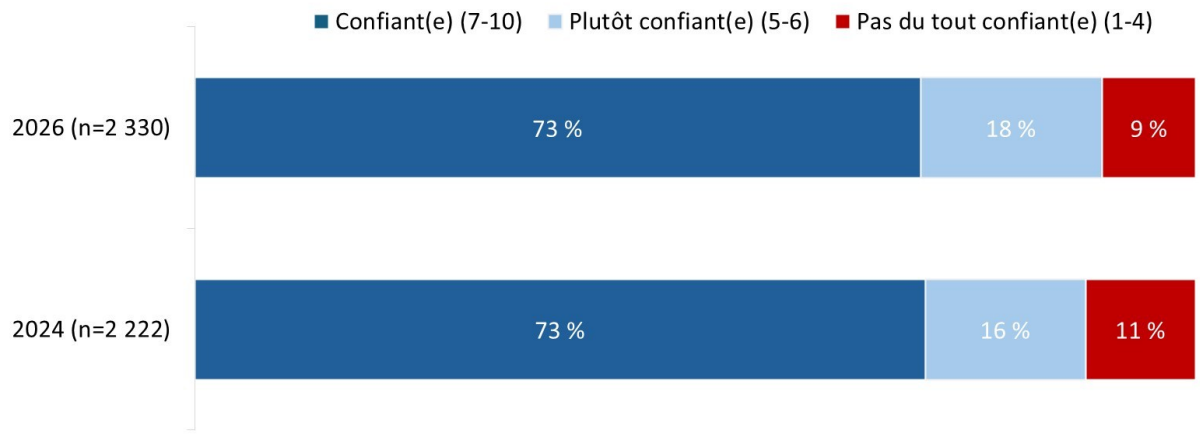


QCS3. Dans quelle mesure comptez-vous sur d'autres personnes (p. ex., des ami(e)s ou membres de famille) pour vous aider à faire ce qui suit? [Plusieurs réponses acceptées] Base de référence : tous les répondants.

Les Canadiennes et les Canadiens demeurent encore très confiants en leur capacité à détecter des messages d'hameçonnage

Près des trois quarts (73 %) des Canadiennes et des Canadiens en ligne sont confiants en leur capacité à détecter un message d'hameçonnage ou un lien malveillant, alors que 18 % se disent confiants dans une certaine mesure. On n'observe ici aucun changement par rapport à 2024. Seulement 9 % déclarent ne pas avoir confiance en leur capacité de détecter 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 : tous les répondants.

La confiance en sa capacité à détecter des messages d'hameçonnage ou des liens malveillants varie selon les groupes démographiques. Les plus jeunes répondants, en particulier ceux de la génération Z et les milléniaux, déclarent avoir une plus grande confiance que les baby-boomers et les membres de la génération silencieuse. Les hommes sont plus susceptibles que les femmes de se dire confiants, et la confiance augmente avec le revenu des ménages. Les personnes qui sont toujours branchées et celles qui possèdent des connaissances plus approfondies en matière de cybersécurité ont également plus tendance à avoir confiance qu'elles pourront repérer les tentatives d'hameçonnage.

2. Les mesures de cybersécurité

Les répondants continuent de prendre des précautions pour protéger leurs comptes en ligne, même si on observe une légère baisse

La plupart des Canadiennes et des Canadiens en ligne déclarent prendre des précautions pour protéger leurs comptes en ligne et appareils (84 %). On observe une diminution progressive au fil du temps, passant de 89 % en 2018 à 84 % en 2026.

Diagramme 5 : Pourcentage de répondants prenant des précautions

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

La probabilité de prendre des précautions pour protéger les comptes en ligne, les comptes de médias sociaux, les appareils ou les réseaux est plus élevée chez les résidents du Canada atlantique, de l'Ontario, de l'Alberta et de la Colombie-Britannique (y compris les territoires) que chez les résidents du Québec. Elle est également plus élevée chez les milléniaux que chez les membres de la génération Z, les hommes, les titulaires d'un diplôme d'études collégiales ou universitaires que chez les personnes détenant au plus un diplôme d'études secondaires et les personnes touchant un revenu annuel maximal de 100 000 $.

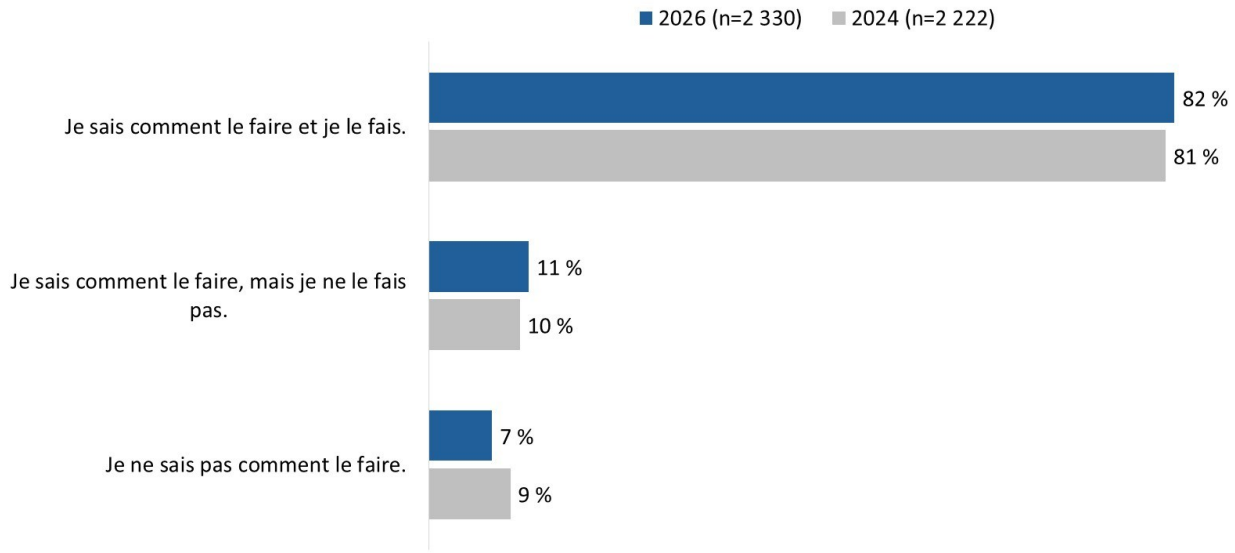
La majorité des Canadiennes et des Canadiens en ligne installent des mises à jour de logiciels et d'applications

En plus de prendre des précautions pour protéger leurs comptes en ligne, huit Canadiens sur dix (82 %) savent comment installer les dernières mises à jour de logiciels et d'applications sur leurs appareils et le font. Par ailleurs, 11 % des répondants savent comment installer ces mises à jour, mais ne le font pas, tandis que seulement 7 % déclarent ne pas savoir comment faire. Les résultats sont cohérents avec ceux de 2024.

Les Canadiennes et les Canadiens plus âgés, en particulier les personnes de 65 ans et plus, les femmes, les titulaires d'au plus un diplôme d'études secondaires ou d'un diplôme universitaire, ainsi que les personnes

ayant des connaissances de base ou de niveau débutant en ce qui concerne la sécurité en ligne sont plus susceptibles de ne pas savoir comment faire.

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

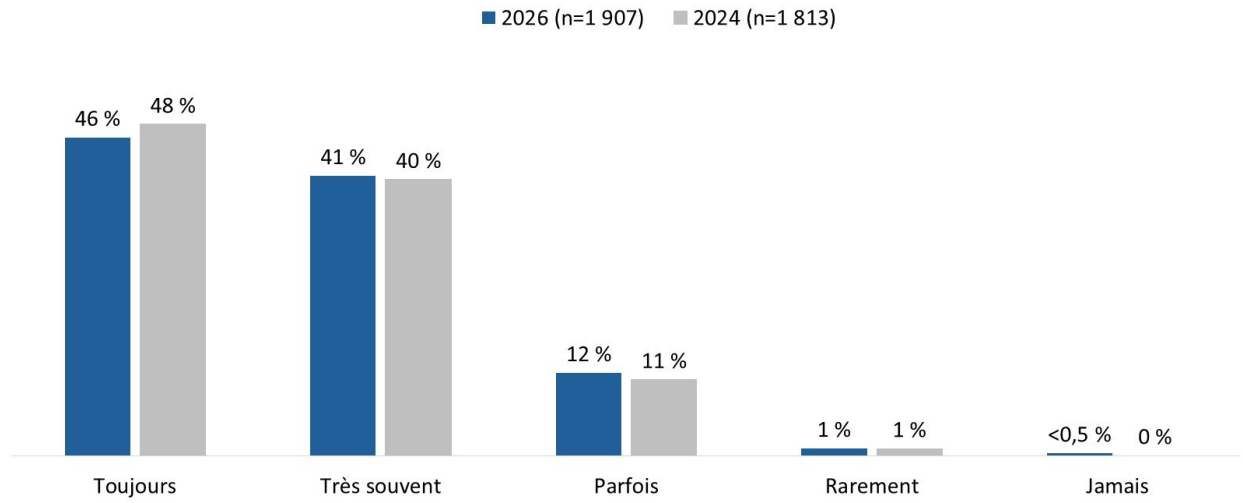


QBEH2. Savez-vous comment installer les plus récentes mises à jour de logiciels et d'applications pour tous vos appareils (p. ex., ordinateur et cellulaire)? Base de référence : tous les répondants.

L'installation à intervalles réguliers de mises à jour de logiciels et d'applications demeure répandue

Parmi les répondants qui savent comment installer les dernières mises à jour de logiciels et d'applications (n=1 907), une grande majorité (87 %) le fait régulièrement, dont 46 % qui affirment toujours installer les mises à jour lorsqu'ils reçoivent une notification. Des proportions plus faibles déclarent n'installer les mises à jour que parfois (12 %) ou rarement (1 %). Ces résultats n'ont pratiquement pas changé depuis 2024.

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



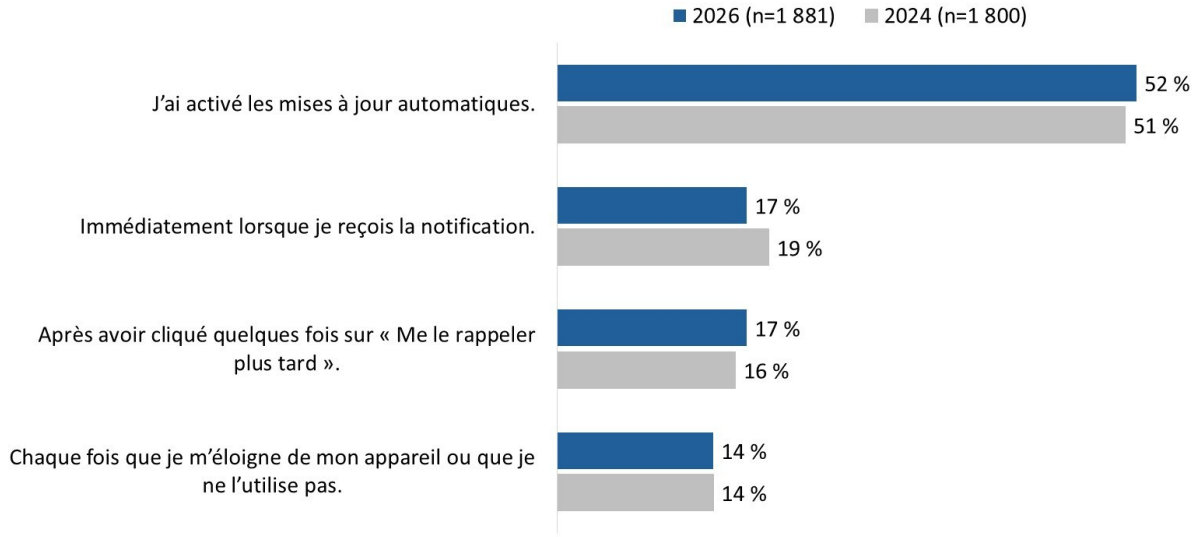
QBEH3. À quelle fréquence installez-vous les dernières mises à jour et versions des logiciels après avoir été avisé(e) qu'elles sont disponibles? Base de référence : répondants qui savent comment procéder aux installations et qui le font.

La probabilité d'installer « toujours » les dernières mises à jour de logiciels ou d'applications après en avoir été avisé augmente avec l'âge et est plus élevée chez les personnes qui possèdent des connaissances poussées relativement à la sécurité en ligne. Les membres de la génération Z sont les moins susceptibles d'installer systématiquement les mises à jour.

L'installation immédiate de mises à jour est fréquente chez les Canadiennes et les Canadiens en ligne

Parmi les personnes qui installent souvent des mises à jour de logiciels (n=1 881), 69 % le font immédiatement 52 % ont activé la fonction de mises à jour automatiques et 17 % installent les mises à jour dès qu'elles reçoivent une notification. Parmi les autres répondants, 17 % retardent les mises à jour après avoir choisi l'option d'un rappel plus tard et 14 % ne font les mises à jour que lorsqu'ils n'utilisent pas leur appareil. Les résultats sont pratiquement inchangés depuis 2024.

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 : répondants qui installent souvent des mises à jour.

Le recours aux mises à jour automatiques augmente avec l'âge. Les Canadiennes et Canadiens de 55 ans et plus sont plus susceptibles que les plus jeunes d'installer des mises à jour immédiatement après avoir reçu une notification. La génération Z est la plus encline à retarder les mises à jour en choisissant un rappel plus tard, tandis que la génération Z et les milléniaux ont plus tendance que les générations précédentes à installer des mises à jour lorsqu'ils ne se servent pas de leur appareil.

La plupart des Canadiennes et Canadiens en ligne connaissent l'AMF et l'utilisent régulièrement

La connaissance de l'authentification multifactorielle (AMF) a augmenté de 4 points de pourcentage, passant de 90 % en 2024 à 94 % en 2026.

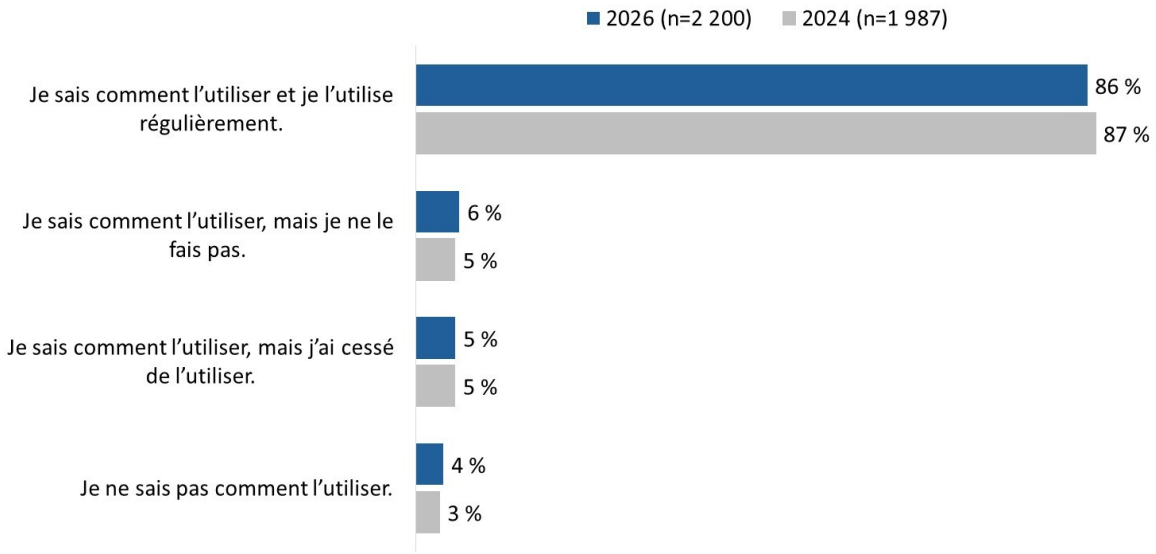
Diagramme 9 : Connaissance de l'AMF : pourcentage des répondants ayant entendu parler de l'AMF

QBEH6. Avez-vous déjà entendu parler de l'authentification multifactorielle (AMF)? Base de référence : tous les répondants.

La connaissance de l'AMF est plus élevée chez les milléniaux, ainsi que les membres de la génération Z et de la génération X. Elle est plus faible chez les résidents du Québec et les personnes novices ou possédant des connaissances de base par rapport à la sécurité en ligne.

Quatre-vingt-six pour cent des Canadiennes et des Canadiens en ligne connaissant l'AMF (n=2 200) savent l'utiliser et le font régulièrement. De plus, 11 % savent utiliser l'AMF, mais ne l'utilisent pas (6 %) ou ont cessé de l'utiliser (5 %). Très peu de répondants (4 %) ont indiqué ne pas savoir utiliser l'AMF. Ces résultats sont pratiquement inchangés depuis 2024.

Diagramme 10 : Capacité à utiliser l'AMF



QBEH7. Savez-vous comment utiliser l'authentification multifactorielle (AMF)? Base de référence : répondants ayant entendu parler de l'AMF.

Les milléniaux sont les plus susceptibles de savoir utiliser l'AMF et de s'en servir régulièrement, tandis que les baby-boomers et la génération silencieuse ont moins tendance à le faire. L'utilisation de l'AMF augmente également avec le niveau de scolarité, et les personnes qui possèdent des connaissances poussées en matière de sécurité en ligne sont les plus enclines à savoir ce que c'est et à s'en servir régulièrement.

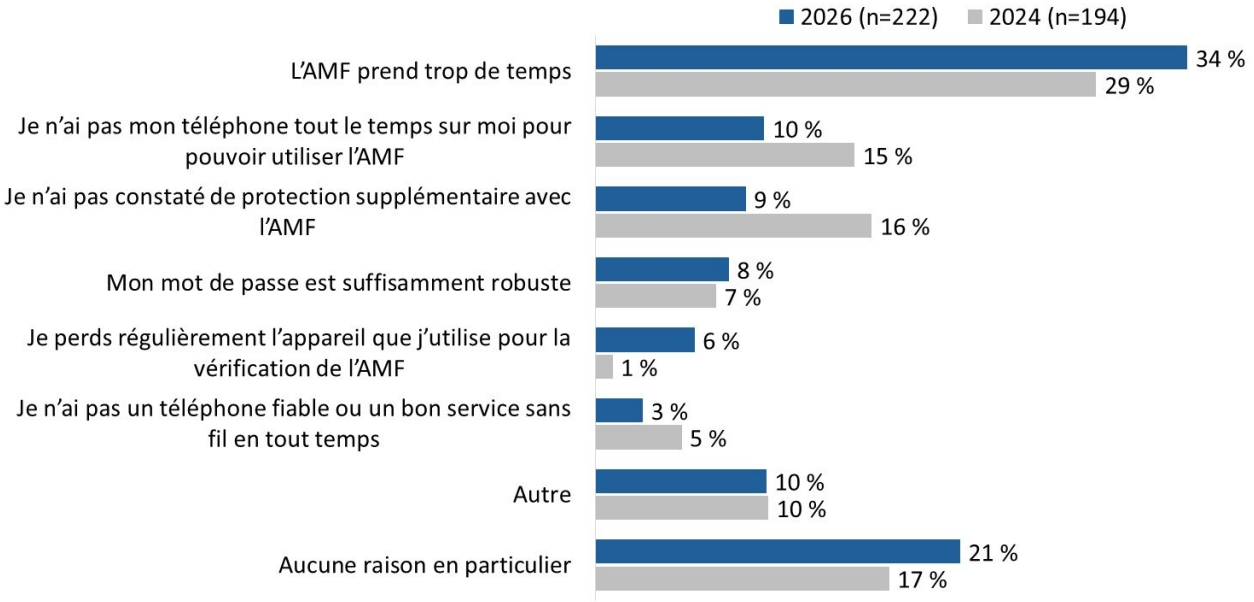
Diverses raisons sont invoquées pour ne pas ou ne plus utiliser l'AMF

Les personnes qui n'utilisent pas, ou n'utilisent plus, l'AMF (n=222) font mention de diverses raisons. La plus grande proportion de répondants (34 %, contre 29 % en 2024) estime que l'AMF prend trop de temps. Par ailleurs, 10 % des répondants n'ont pas toujours leur téléphone à portée de main pour pouvoir vérifier (comparativement à 15 % en 2024), 9 % ne pensent pas que l'AMF confère une protection supplémentaire (contre 16 %), et 8 % estiment que leur mot de passe seul est suffisamment robuste.

Les raisons mentionnées par de plus petites proportions de répondants comprenaient le fait de ne pas avoir régulièrement à portée de main l'appareil configuré pour l'AMF (6 %) et l'absence d'une ligne téléphonique ou Wi-Fi fiable en tout temps (3 %).

Deux répondants sur 10 (21 %) n'ont pas fait mention de raison particulière pour expliquer le fait qu'ils n'utilisent pas ou n'utilisent plus l'AMF.

Diagramme 11 : Principale raison de ne pas utiliser l'AMF

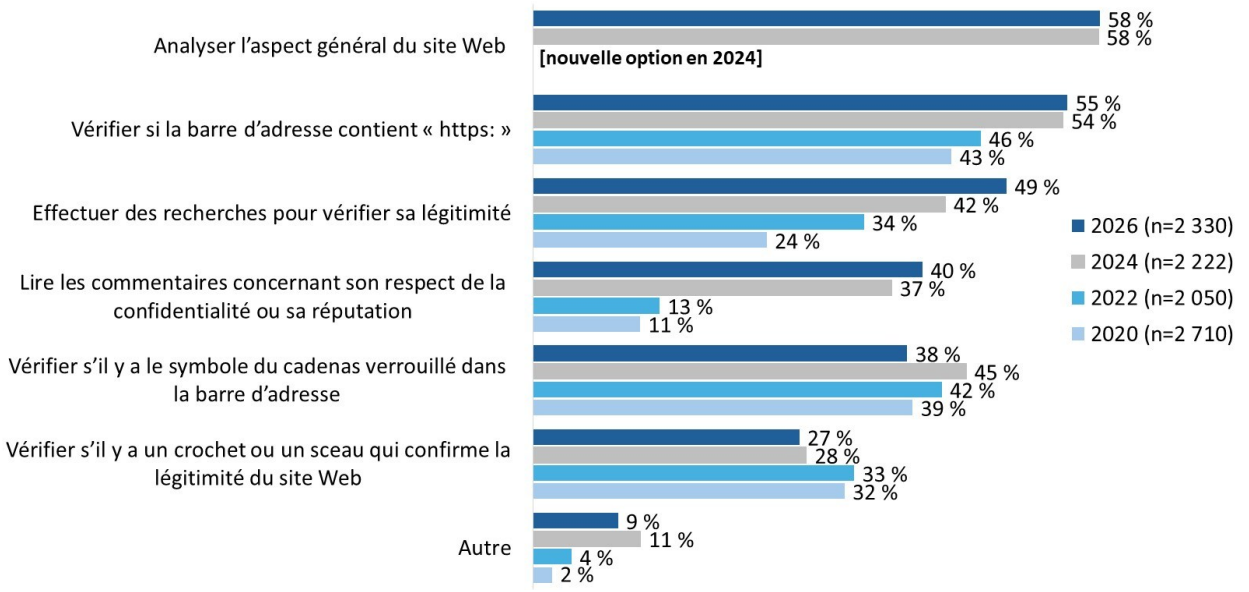


QBEH8. Quelle est la principale raison pour laquelle vous n'utilisez pas (ou que vous avez cessé d'utiliser) l'authentification multifactorielle (AMF)? Base de référence : répondants qui savent comment utiliser l'AMF, mais qui choisissent de ne pas le faire.

Les Canadiennes et Canadiens en ligne utilisent diverses stratégies pour vérifier la légitimité d'un site Web

Pour vérifier la légitimité d'un site Web, près de six Canadiens sur dix (58 %) analysent l'aspect général du site. Cette proportion n'a pas changé depuis 2024. En outre, 55 % vérifient si « https : » figure dans la barre d'adresse et environ la moitié des personnes sondées (49 % comparativement à 42 % en 2024) effectuent des recherches pour en vérifier la légitimité. Quatre personnes sur dix (40 %, contre 37 % en 2024) lisent des commentaires concernant le respect de la confidentialité ou la réputation du site Web et une proportion presque aussi importante (38 % comparativement à 45 % en 2024) vérifient la présence du symbole de cadenas dans l'adresse. Un peu plus d'un quart des répondants (27 %) vérifient s'il y a un crochet ou un sceau de confiance confirmant la légitimité du site Web.

Diagramme 12 : Mesures pour vérifier la sécurité d'un site Web



QBEH12. Quelles mesures prenez-vous pour vérifier la légitimité d'un site Web? Base de référence : tous les répondants.

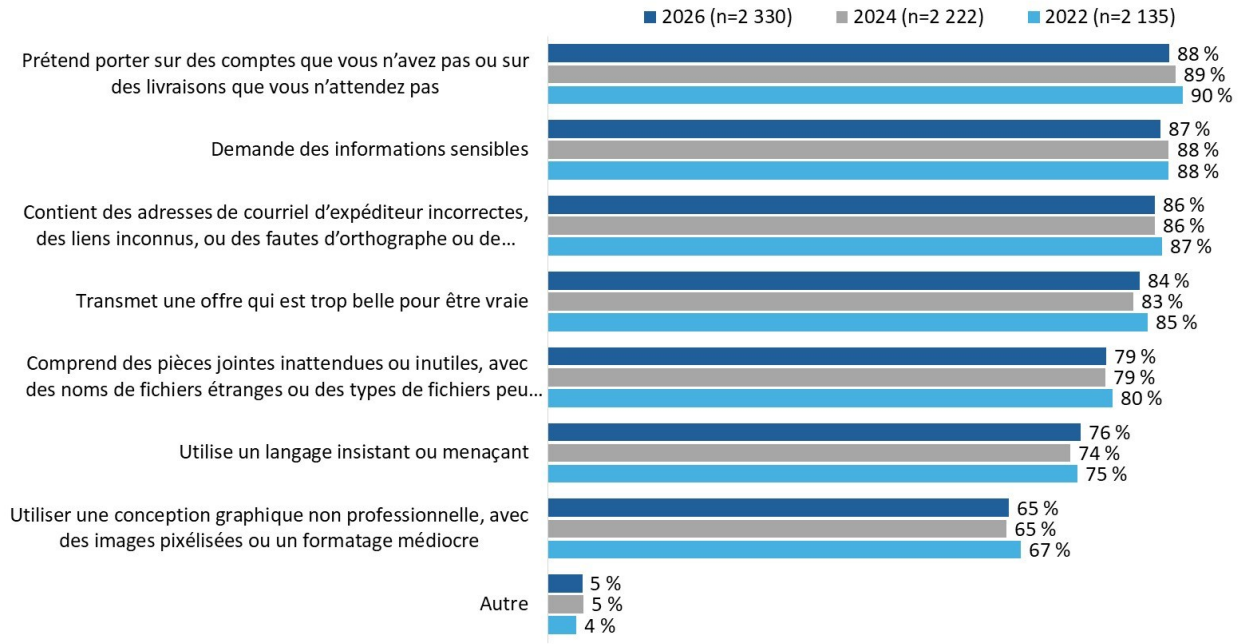
Les Canadiennes et Canadiens de 65 ans et plus ont généralement moins tendance que les plus jeunes à prendre des mesures pour vérifier la légitimité d'un site Web. En revanche, les personnes qui possèdent des connaissances poussées en ce qui concerne la sécurité en ligne ont plus tendance à prendre toutes ces mesures pour vérifier la légitimité d'un site Web.

La plupart des Canadiennes et des Canadiens en ligne reconnaissent les signes associés aux messages d'hameçonnage

La grande majorité des Canadiennes et des Canadiens en ligne reconnaissent les signes courants d'hameçonnage. La plupart des répondants parlent de messages portant sur des comptes qu'ils n'ont pas ou de livraisons inattendues (88 %), des demandes d'informations sensibles (87 %), et des messages contenant des adresses courriel incorrectes, des liens inconnus, ou des fautes d'orthographe ou de grammaire (86 %). Presque autant de répondants reconnaissent les offres qui semblent trop belles pour être vraies (84 %) et les pièces jointes inattendues ou inutiles (79 %) comme des indicateurs d'hameçonnage. Selon les trois quarts des répondants (76 %), le langage insistant ou menaçant est un signe d'hameçonnage, tandis que 65 % font mention d'un graphisme non professionnel.

Le niveau de connaissances est demeuré le même depuis 2022.

Diagramme 13 : Connaissance des signes d'une tentative d'hameçonnage



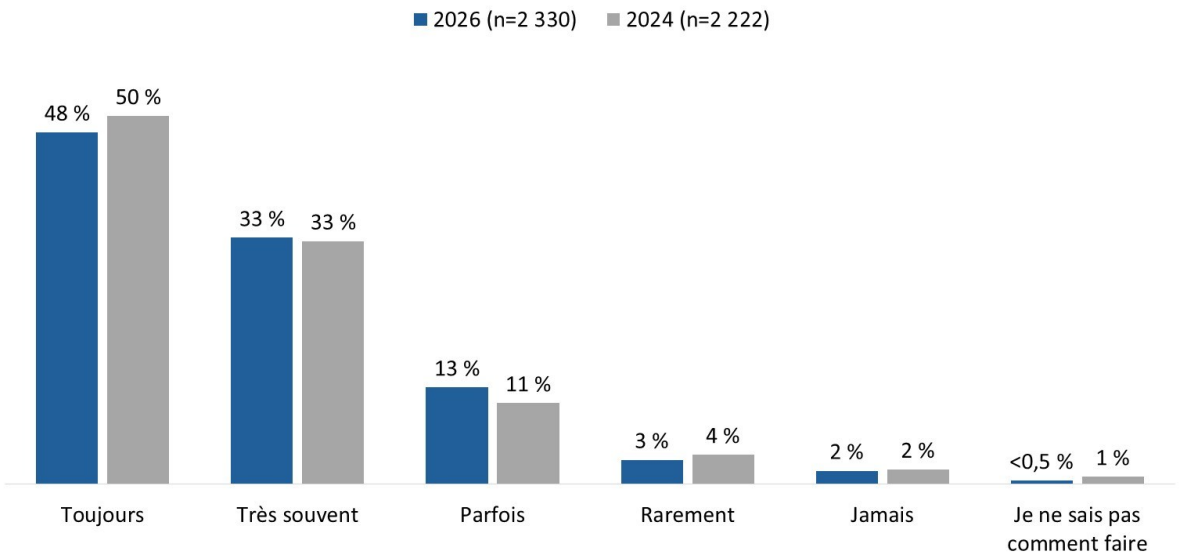
QBEH13. D'après ce que vous savez, quels sont les signes d'une tentative d'hameçonnage? Base de référence : tous les répondants.

Les milléniaux font partie des répondants les plus susceptibles de reconnaître les signes courants d'hameçonnage, tandis que les membres de la génération silencieuse ont moins tendance à le faire. Le taux de reconnaissance des signes d'hameçonnage augmente avec le niveau de scolarité et le revenu du ménage. Il est le plus élevé chez les personnes possédant des connaissances intermédiaires ou avancées concernant la sécurité en ligne.

Les Canadiennes et les Canadiens en ligne demeurent très vigilants pour ce qui est des tentatives d'hameçonnage

La plupart des Canadiennes et des Canadiens en ligne vérifient les messages pour détecter des signes d'hameçonnage avant de cliquer sur des liens ou de répondre. Près de la moitié le font toujours (48 %), et un autre tiers le fait très souvent (33 %). De plus, 13 % des répondants vérifient parfois, tandis que 5 % disent qu'ils le font rarement, voire jamais. Ces résultats sont pratiquement inchangés depuis 2024.

Diagramme 14 : Fréquence de la vérification des messages pour détecter des 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.

Les groupes suivants sont plus susceptibles de « toujours » vérifier les messages pour détecter des signes d'hameçonnage : les résidents de l'Ontario et de l'Alberta comparativement à ceux du Québec, ainsi que les répondants de moins de 65 ans et les milléniaux comparativement à la génération Z, aux baby-boomers et à la génération silencieuse. De plus, les personnes possédant des connaissances avancées concernant la sécurité en ligne et celles qui sont toujours branchées à Internet sont plus susceptibles de vérifier les messages en recherchant des signes d'hameçonnage.

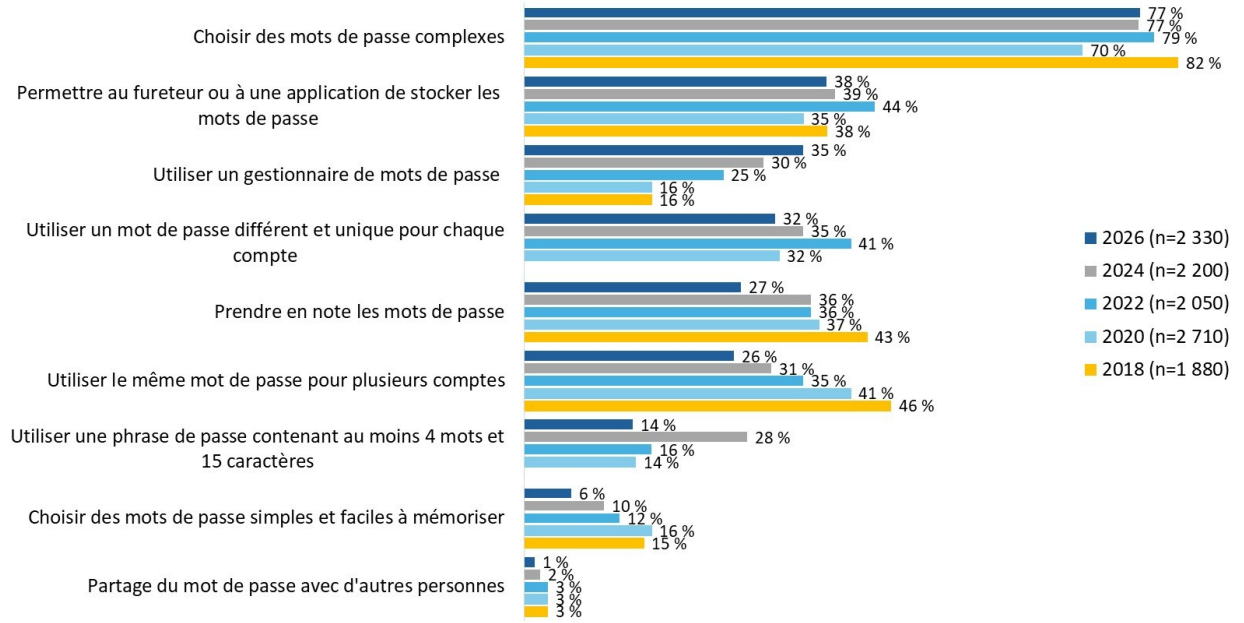
Les trois quarts des répondants choisissent des mots de passe complexes; certains ont des comportements qui les mettent à risque

Plus des trois quarts (77 %) des Canadiennes et des Canadiens en ligne déclarent créer des mots de passe complexes en combinant des lettres, des chiffres et des symboles. Des proportions plus faibles utilisent un gestionnaire de mots de passe (35 % comparativement à 30 % en 2024), un mot de passe différent et unique pour chaque compte (32 %, contre 35 %), ou une phrase de passe contenant au moins quatre mots et 15 caractères (14 %, ce qui représente une diminution comparativement à 28 %).

Certains répondants font état de comportements pouvant accroître la vulnérabilité des comptes. Par exemple, 38 % permettent aux navigateurs ou applications de stocker des mots de passe, 27 % (contre 36 % en 2024) écrivent leurs mots de passe, 26 % (contre 31 %) réutilisent les mots de passe pour plusieurs comptes, 6 % (contre 10 %) optent pour des mots de passe simples et faciles à retenir, et 1 % partagent leurs mots de passe avec d'autres personnes.

Lorsqu'on compare les réponses d'une année à l'autre, les mots de passe complexes restent la pratique la plus courante, tandis que plusieurs comportements donnant lieu à un risque important, comme le fait d'écrire les mots de passe ou de réutiliser ces derniers, ont diminué par rapport à 2024.

Diagramme 15 : Mesures prises concernant les mots de passe



QBEH15. Lorsque vient le temps de choisir vos mots de passe, lesquelles des mesures suivantes prenez-vous? Base de référence : tous les répondants.

Les comportements concernant les mots de passe varient systématiquement selon l'âge. Les Canadiennes et les Canadiens âgés de 18 à 44 ans sont plus susceptibles de privilégier l'aspect pratique, comme le stockage de mots de passe dans des navigateurs ou des applications, l'utilisation de gestionnaires de mots de passe et la réutilisation des mots de passe. Les personnes âgées de 35 à 64 ans sont les plus susceptibles d'utiliser des mots de passe complexes, tandis que les Canadiennes et les Canadiens de 65 ans et plus ont le plus tendance à écrire leurs mots de passe.

En ce qui concerne le genre, les hommes sont plus susceptibles d'utiliser un gestionnaire de mots de passe et des mots de passe uniques, tandis que les femmes sont plus enclines à écrire leurs mots de passe et à choisir d'utiliser une clé d'accès, lorsqu'une telle option est offerte, plutôt qu'un mot de passe.

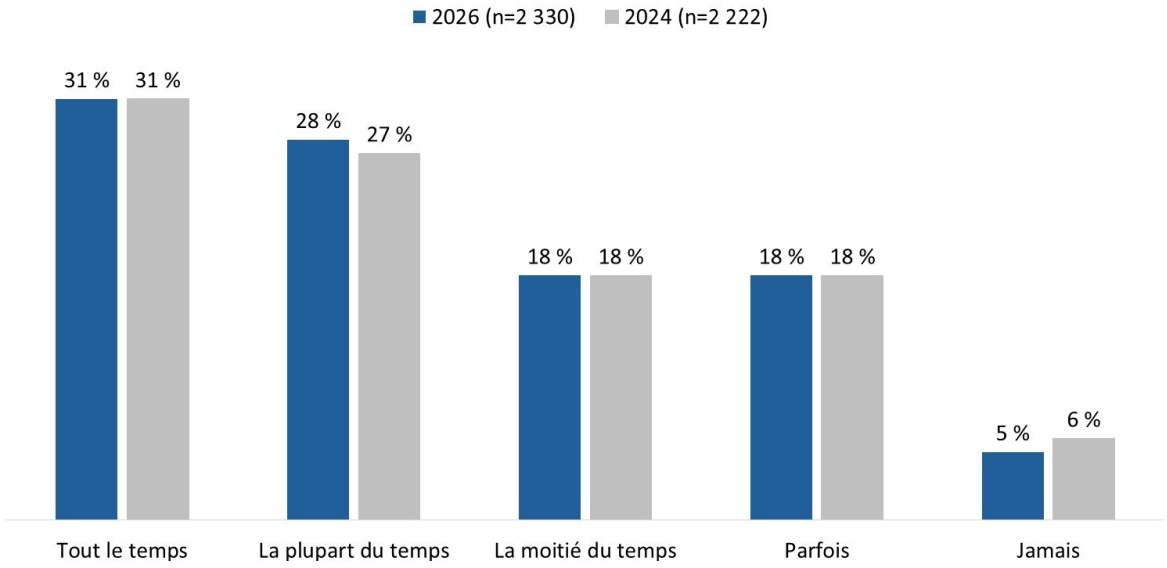
Mentionnons les autres différences entre les sous-groupes :

- La probabilité d'utiliser un gestionnaire de mots de passe et une clé d'accès augmente avec le revenu du ménage.
- Les diplômés universitaires sont plus susceptibles de choisir des mots de passe complexes.
- Les parents ont plus tendance à utiliser un mot de passe de quatre à quinze caractères, mais ils sont moins enclins à choisir un mot de passe différent pour chaque compte.

La plupart des Canadiennes et des Canadiens utilisent des mots de passe uniques au moins de temps à autre

La moitié des Canadiennes et des Canadiens en ligne déclarent utiliser des mots de passe uniques pour leurs comptes en ligne importants « tout le temps » (31 %) ou « la plupart du temps » (28 %). Un tiers des répondants le font « la moitié du temps » (18 %) ou « parfois » (18 %). Très peu de répondants (5 %) affirment ne pas utiliser de mots de passe uniques. Les résultats n'ont essentiellement pas changé depuis 2024.

Diagramme 16 : Fréquence de l'utilisation de mots de passe uniques



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)? Base de référence : tous les répondants.

La génération Z est moins encline à utiliser des mots de passe uniques « tout le temps » ou « la plupart du temps », tandis que les hommes et les personnes possédant des connaissances poussées concernant la sécurité en ligne sont plus susceptibles d'utiliser « tout le temps » des mots de passe uniques.

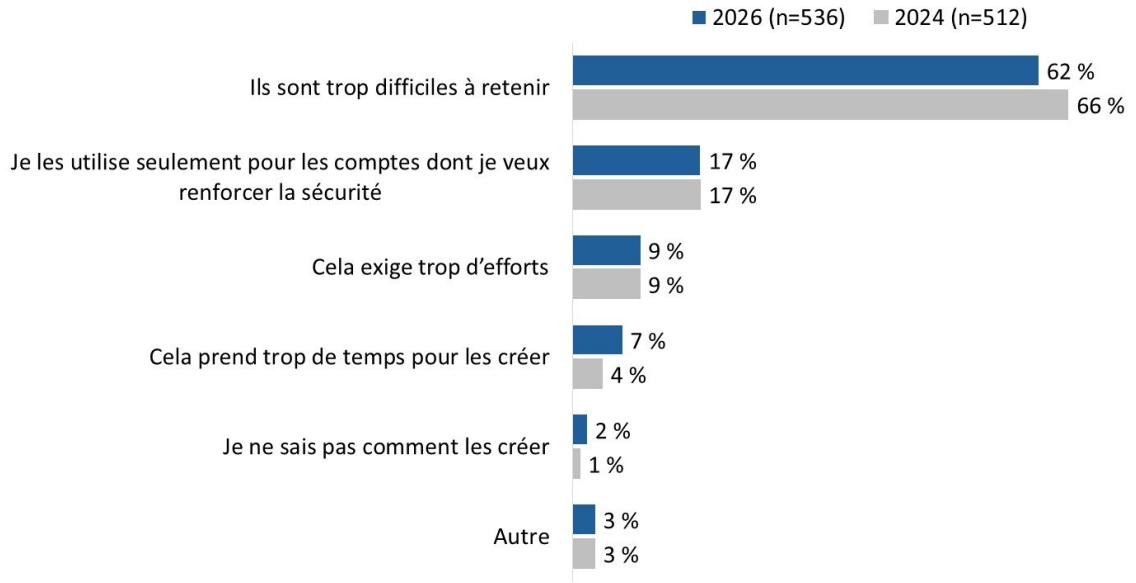
Les Canadiennes et les Canadiens réutilisent leurs mots de passe principalement parce qu'ils n'ont pas besoin de se souvenir de plusieurs mots de passe

Parmi les répondants qui utilisent rarement, voire jamais, des mots de passe uniques (n=536), environ six sur dix (62 %) disent que c'est parce qu'ils ont du mal à se souvenir de mots de passe différents. D'autres font mention de l'effort (9 %), du temps nécessaire pour les créer (7 %) ou du fait de ne pas savoir comment (2 %). Dix-sept pour cent déclarent n'utiliser des mots de passe uniques que pour les comptes où une sécurité renforcée est nécessaire.

Les résultats sont en grande partie cohérents avec ceux de 2024, bien qu'on observe une légère diminution des personnes qui parlent des difficultés à se souvenir des mots de passe (66 % contre 62 %) et une faible augmentation des répondants qui estiment que les mots de passe uniques prennent trop de temps à créer (4 % à 7 %).

Les Canadiennes et les Canadiens en ligne au Québec sont plus susceptibles que les résidents de l'Ontario, de l'Alberta et de la Colombie-Britannique, y compris des territoires, d'utiliser des mots de passe uniques pour les comptes nécessitant une sécurité accrue. Les femmes ont plus tendance que les hommes à utiliser rarement des mots de passe uniques, car ils sont difficiles à retenir.

Diagramme 17 : Principale raison de ne pas utiliser des mots de passe uniques

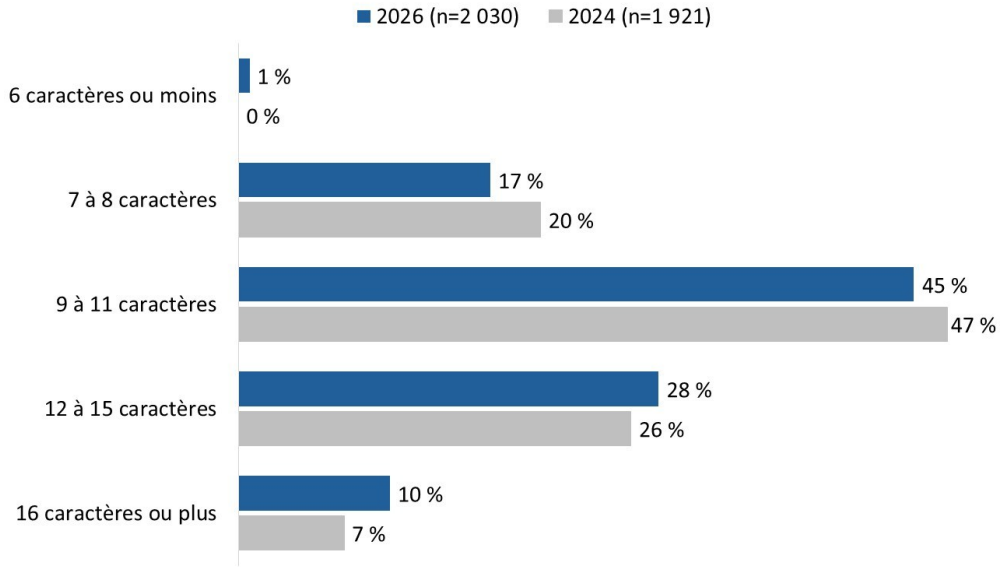


QBEH18. Quelle est la principale raison pour laquelle vous utilisez rarement, voire jamais, des mots de passe uniques pour vos comptes en ligne? Base de référence : répondants qui ne créent pas de mots de passe uniques.

La plupart des Canadiennes et des Canadiens en ligne utilisent des mots de passe d'une longueur moyenne, et certains optent pour de plus longs mots de passe

La longueur des mots de passe varie. Environ six répondants sur dix choisissent des mots de passe entre sept et huit caractères (17 %) ou neuf et onze caractères (45 %). Pour ce qui est des autres répondants, près de quatre sur dix optent pour des mots de passe plus longs : 28 % choisissent des mots de passe contenant de 12 à 15 caractères et 10 % utilisent des mots de passe de 16 caractères ou plus. L'utilisation de mots de passe d'au moins 12 caractères a légèrement augmenté depuis 2024.

Diagramme 18 : Longueur des mots de passe

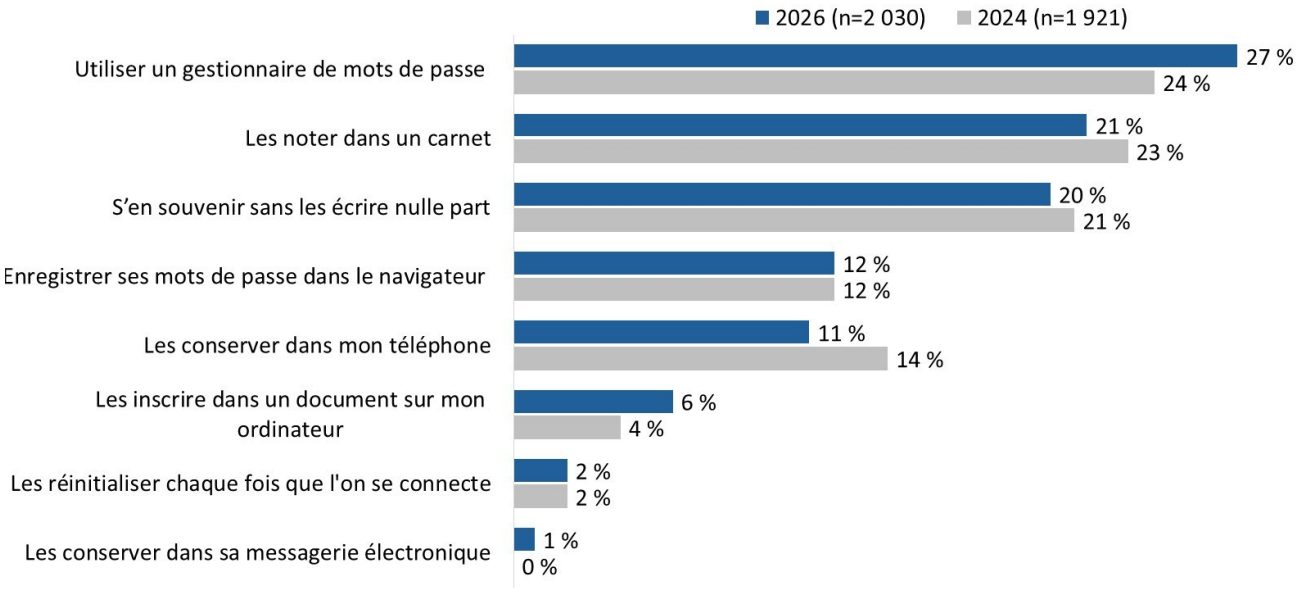


QBEH21. Combien de caractères comptent les mots de passe que vous créez habituellement? Base de référence : répondants qui ne sont pas des représentants d'une entreprise.

La méthode privilégiée pour se souvenir des mots de passe varie

Environ un quart des répondants (27 %, soit une hausse par rapport à 24 % en 2024) utilisent un gestionnaire de mots de passe pour gérer plusieurs mots de passe. De plus petites proportions disent les écrire dans un carnet (21 %) ou s'en souvenir sans les écrire (20 %).

Diagramme 19 : Méthode privilégiée pour se souvenir des mots de passe



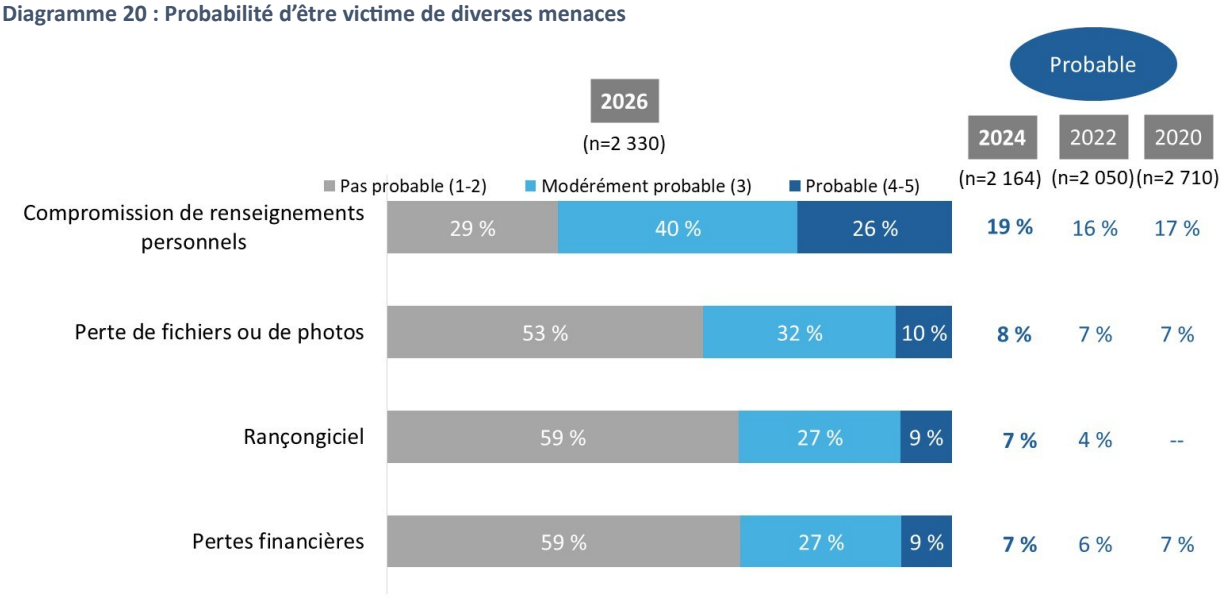
QBEH22. Quelle est la méthode que vous privilégiez pour vous souvenir de plusieurs mots de passe? Base de référence : répondants qui ne sont pas des représentants d'une entreprise.

3. Les cybermenaces

Un tiers des Canadiennes et des Canadiens en ligne croient qu'ils risquent d'être victimes d'une cybermenace

Un tiers (33 %) des Canadiennes et des Canadiens en ligne croient qu'ils seront probablement victimes d'au moins l'une des quatre cybermenaces au cours de la prochaine année (comparativement à 8 % en 2022 et à 24 % en 2024). Un quart des Canadiennes et des Canadiens en ligne (26 %, contre 19 % en 2024) pensent qu'il est probable qu'ils soient victimes d'une cybermenace qui compromettra leurs renseignements personnels. À l'instar des années précédentes, peu de gens pensent qu'ils seront visés par une menace entraînant la perte de fichiers ou de photos (10 %), la conservation de leurs données contre rançon (9 %) ou des pertes financières (9 %).

Diagramme 20 : Probabilité d'être victime de diverses menaces



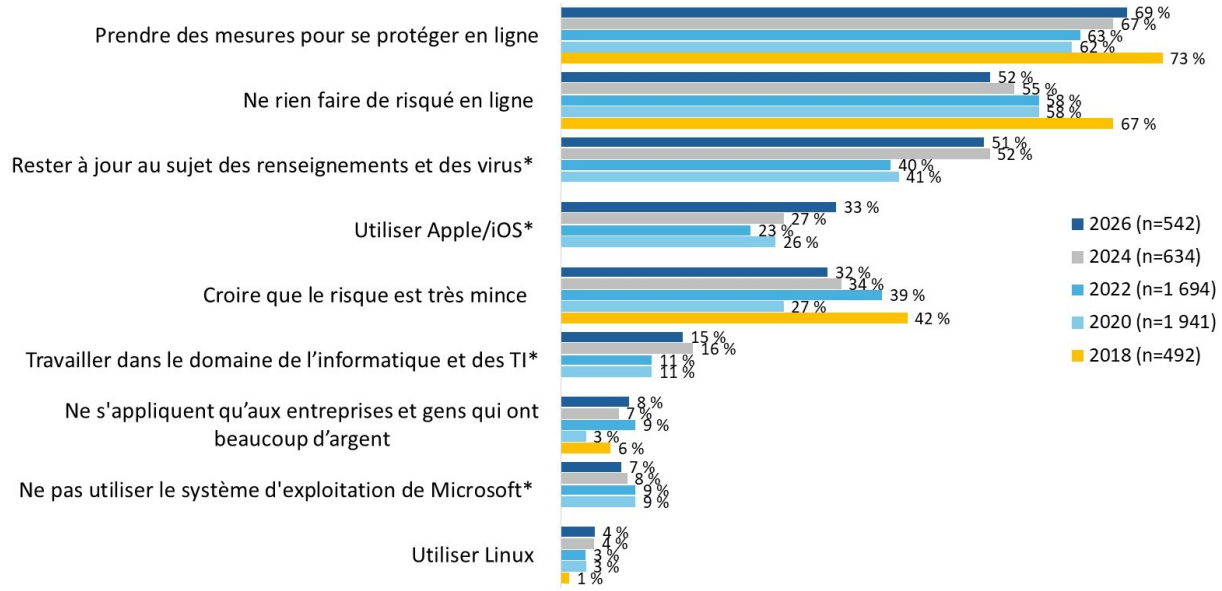
QCT1. Au cours de la prochaine année, à quel point avez-vous l'impression qu'il est probable que vous soyez victime d'une cybermenace...? Base de référence : tous les répondants.

La probabilité de croire qu'ils ne seraient pas visés par des cybermenaces augmente à mesure que l'âge diminue. Une tendance similaire est observée chez les personnes possédant des connaissances poussées en matière de sécurité en ligne. Ces personnes sont également plus susceptibles d'être du même avis.

Les personnes qui se sentent peu à risque d'être victimes de cybermenaces font mention de leurs pratiques et de leurs comportements en ligne

La plupart des répondants qui se considèrent peu susceptibles d'être visés par une cybermenace (n=542) font mention de leurs habitudes, notamment des mesures qu'ils prennent pour se protéger en ligne (69 %), le défaut d'adopter des comportements à risque en ligne (52 %, contre 55 % en 2024), et le fait de rester informés des menaces et virus (51 %). Environ un tiers des répondants parlent également de l'utilisation d'Apple/iOS (33 %, contre 27 % en 2024) ou estiment que les risques sont tout simplement très faibles (32 %). Toutes les raisons sont indiquées dans le diagramme 21.

Diagramme 21 : Raisons invoquées pour expliquer la faible probabilité d'être victime de cybermenaces



*Pas un choix de réponse en 2018.
QCT2. Pourquoi ne croyez-vous pas qu'il est probable que vous soyez victime d'une cybermenace? Base de référence : répondants estimant qu'il est peu probable qu'ils soient victimes d'une cybermenace. [Plusieurs réponses acceptées].

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

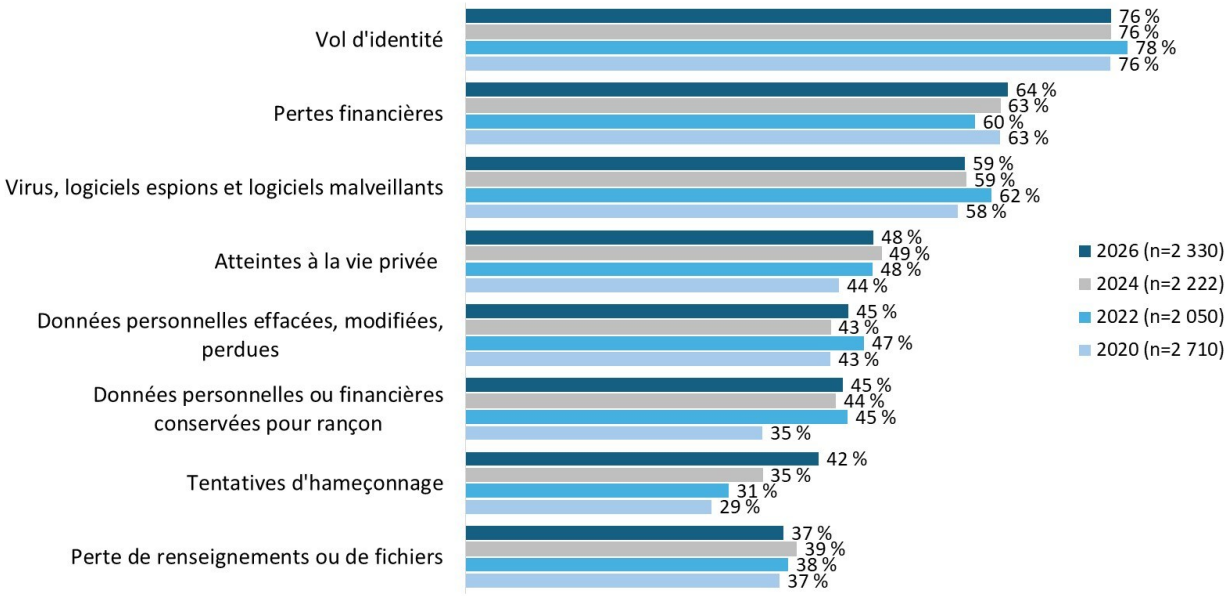
Les trois quarts (76 %) des Canadiennes et des Canadiens en ligne expriment des inquiétudes concernant le vol d'identité. Ils craignent également les pertes financières (64 %), ainsi que les virus, les logiciels espions et les logiciels malveillants (59 %). Environ la moitié des répondants (48 %) sont préoccupés par des atteintes à la protection de leurs renseignements personnels, 45 % ont peur des attaques concernant les données personnelles ou par rançongiciel, et 42 % se soucient des arnaques par hameçonnage. Un peu plus d'un tiers (37 %) s'inquiètent surtout de la perte d'informations ou de fichiers.

Dans l'ensemble, les résultats sont restés relativement stables, la plupart des indicateurs n'ayant pas changé de plus de trois points de pourcentage entre 2024 et 2026. Les préoccupations liées aux arnaques par hameçonnage, qui n'ont cessé d'augmenter au fil du temps (passant de 29 % en 2020 à 42 % en 2026), sont l'exception.

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

- Les répondants âgés de 45 ans et plus sont plus susceptibles que les jeunes Canadiennes et Canadiens en ligne de craindre l'hameçonnage que les virus, logiciels espions ou logiciels malveillants. Les Canadiennes et les Canadiens en ligne âgés de 18 à 34 ans ont moins tendance à s'inquiéter du vol d'identité et sont plus susceptibles de se soucier du non-respect de la confidentialité.
- L'inquiétude concernant le non-respect de la confidentialité, les pertes financières et la perte d'informations, de fichiers ou de données personnelles est plus élevée chez les femmes.
- La probabilité de s'inquiéter du non-respect de la protection des renseignements personnels est plus élevée chez les personnes faisant partie de ménages déclarant un revenu annuel inférieur à 40 000 $.
- Les préoccupations liées au vol d'identité et aux pertes financières augmentent avec le niveau de scolarité.
- Les résidents du Québec sont les plus susceptibles de se soucier du vol d'identité, tandis que les préoccupations concernant les virus, les logiciels espions et les logiciels malveillants sont généralement plus importantes chez les résidents de l'Ontario et de la Colombie-Britannique, y compris ceux des territoires.

Diagramme 22 : Types de cybermenaces les plus préoccupants

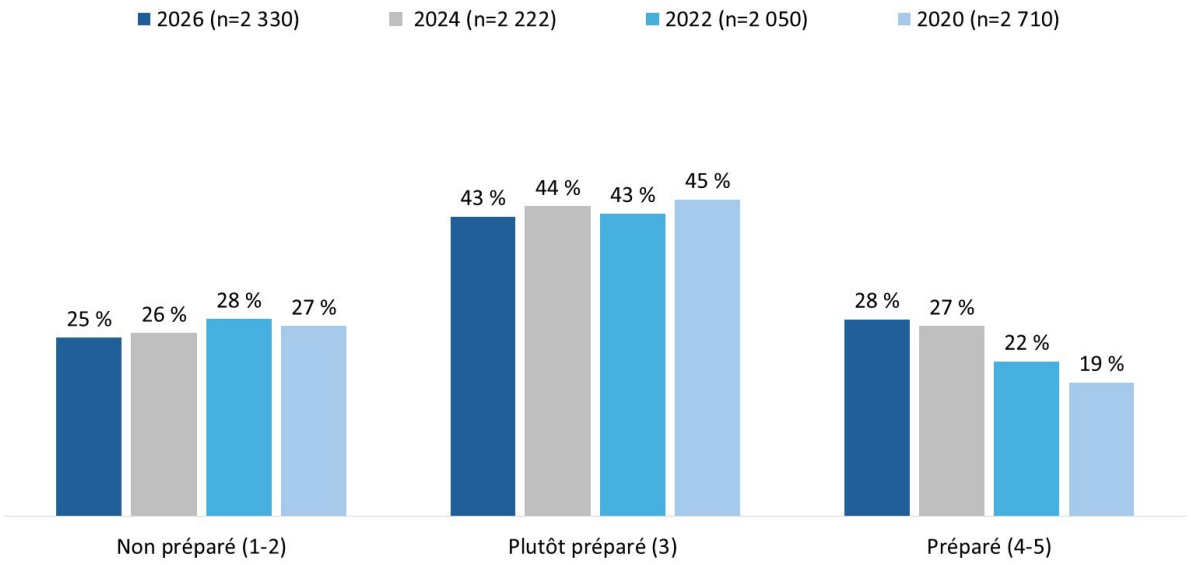


QCT3. Quels types de cybermenaces vous préoccupent le plus? Base de référence : tous les répondants. [Plusieurs réponses acceptées].

La plupart des répondants se sentent préparés au moins dans une certaine mesure à faire face aux cybermenaces

La majorité des Canadiennes et des Canadiens en ligne déclarent être assez préparés (43 %) ou très bien préparés (28 %). Un quart des personnes sondées disent se sentir non préparées. La proportion de répondants qui s'estiment bien préparés a augmenté progressivement, passant de 19 % à 2020 à 28 % en 2026.

Diagramme 23 : Préparation pour faire face aux cybermenaces



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

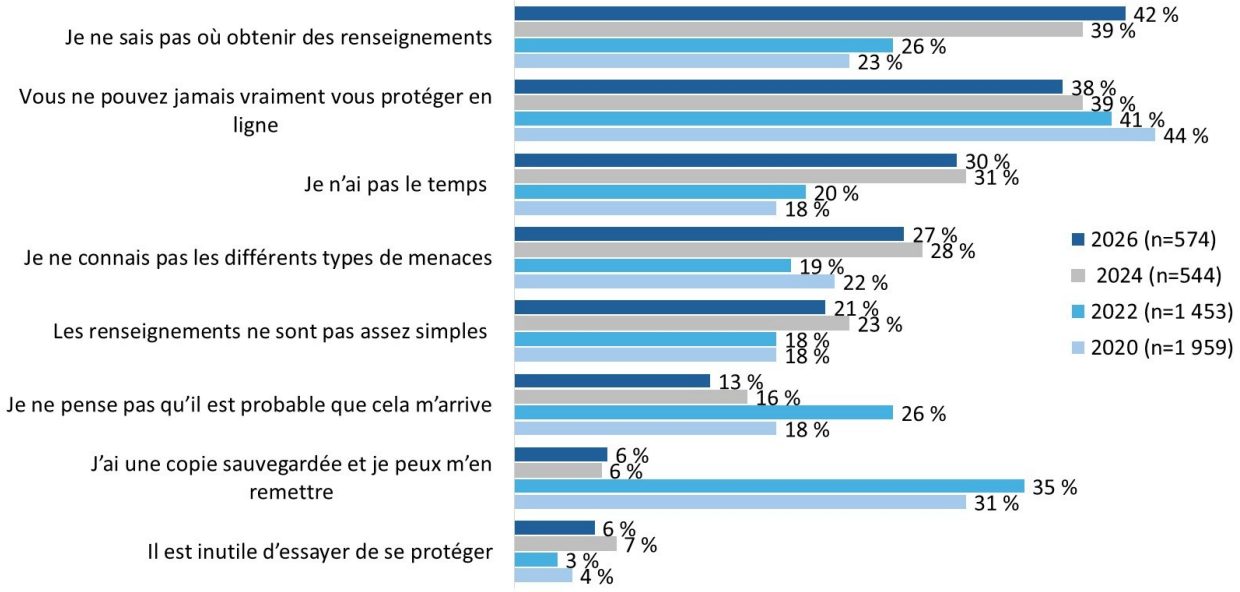
Les résidents du Québec sont plus susceptibles que les habitants de la plupart des autres régions du Canada (sauf en Saskatchewan et au Manitoba) de se sentir mal préparés à faire face aux cybermenaces. Cette perception est également plus courante chez les personnes gagnant moins de 100 000 $ par an, les femmes et les répondants novices ou possédant des connaissances de base concernant la sécurité en ligne.

Le fait de ne pas avoir assez d'information est la raison la plus souvent invoquée pour expliquer le sentiment de ne pas être préparé face aux cybermenaces

Les personnes qui se sentent mal préparées pour gérer une cybermenace (n=574) invoquent principalement le fait de ne pas savoir où trouver des informations (42 %, contre 39 % en 2024) et la conviction qu'on ne pourra jamais se protéger pleinement en ligne (38 %). Les autres raisons comprennent le manque de temps (30 %), la connaissance limitée des types de menaces (27 %) et des informations portant à confusion (21 %). Le diagramme 24 contient la liste complète des raisons.

Comparativement aux données de référence de 2020, un plus grand nombre de répondants indiquent ne pas savoir où trouver des informations (23 % à 42 % en 2026). Au cours de la même période, la perception selon laquelle on ne peut jamais se protéger pleinement en ligne a progressivement diminué, passant de 44 % à 38 %.

Diagramme 24 : Raisons invoquées afin d'expliquer l'absence de préparation pour faire face aux cybermenaces



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

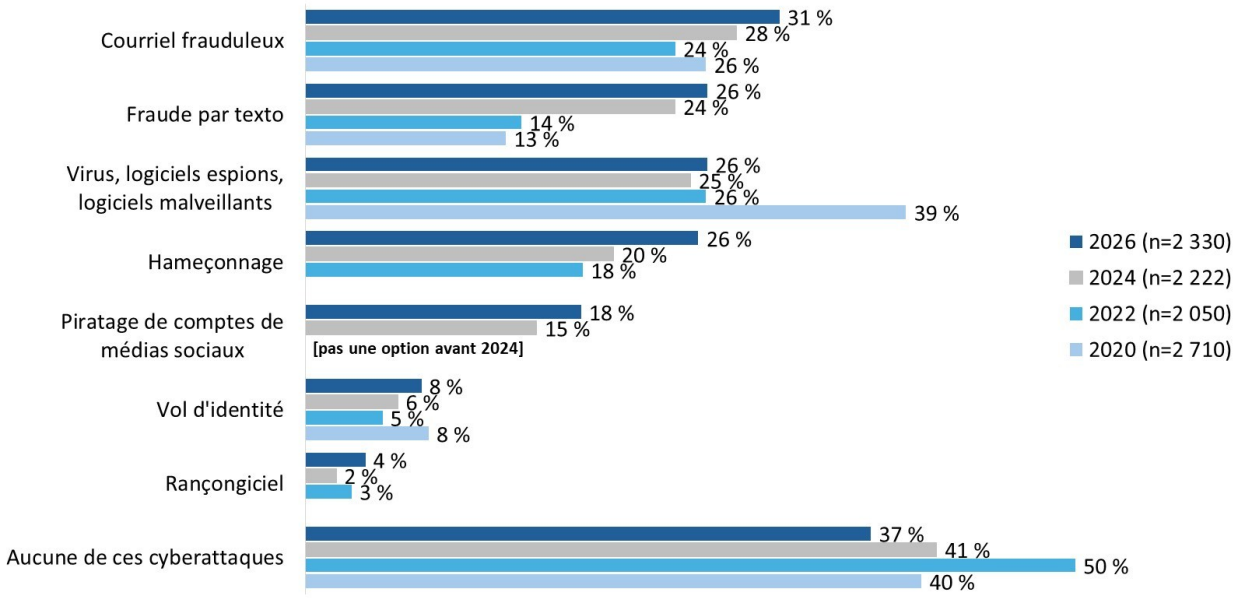
Les raisons de ne pas se sentir préparé varient selon le groupe démographique. La génération Z est la plus susceptible d'être convaincue que les cybermenaces sont peu susceptibles de la toucher. En revanche, les répondants âgés de 65 ans et plus sont plus enclins que les jeunes Canadiennes et Canadiens à expliquer qu'ils ne disposent pas de suffisamment de ressources ou de connaissances. Ils mentionnent notamment leur difficulté à trouver des informations claires, leur incapacité à savoir où obtenir des conseils et une connaissance limitée des différents types de menaces. Les femmes ont également plus tendance à dire qu'elles se sentent mal préparées parce qu'elles ne savent pas où trouver des informations sur les étapes à suivre.

Les courriels frauduleux arrivent au premier rang des incidents de cybercriminalité touchant les Canadiennes et les Canadiens en ligne

Les types de cybercriminalité les plus fréquents signalés par les Canadiennes et les Canadiens en ligne sont les courriels frauduleux (31 %), suivis des fraudes par texto (26 %), des attaques par des logiciels malveillants (26 %) et des arnaques par hameçonnage (26 %). Dix-huit pour cent des répondants ont fait mention d'un piratage de leurs comptes dans les médias sociaux, tandis que relativement peu de personnes ont subi un vol d'identité (8 %) ou une attaque par rançongiciel (4 %).

Au fil du temps, de plus en plus de Canadiennes et de Canadiens en ligne déclarent avoir subi des cyberattaques, et un moins grand nombre d'entre eux affirment n'avoir vécu aucun de ces types d'incidents (37 % en 2026, contre 41 % en 2024 et 50 % en 2022). Le changement le plus notable est la hausse d'attaques par hameçonnage, passant de 18 % en 2022 à 26 % en 2026. En revanche, la proportion de Canadiennes et de Canadiens en ligne signalant une attaque par un virus, un logiciel espion ou un logiciel malveillant reste inférieure au seuil observé dans le premier sondage, où 39 % avaient signalé ce type d'incident.

Diagramme 25 : Expérience des cyberattaques



QCT6. Avez-vous déjà été victime de l'une des cyberattaques suivantes? Base de référence : tous les répondants. [Plusieurs réponses acceptées].

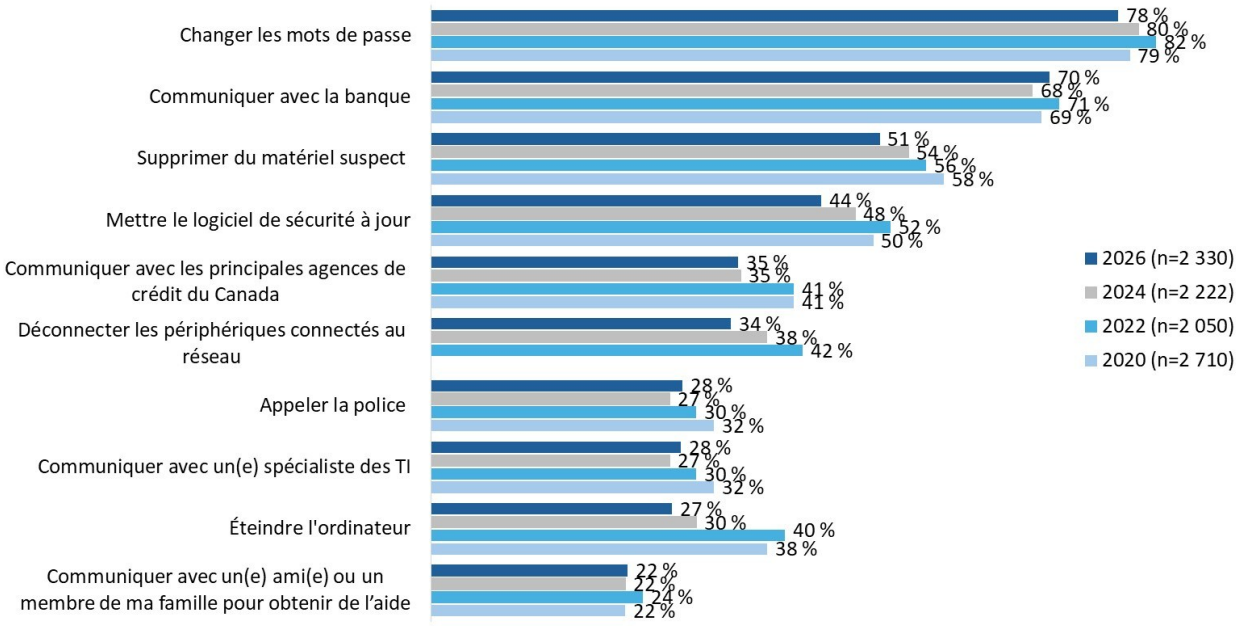
Des différences régionales et démographiques sont observées dans les expériences de cyberattaques ayant été déclarées. Les résidents du Québec sont plus susceptibles que les autres répondants au Canada de signaler avoir été victimes d'une arnaque par courriel. Les Canadiennes et les Canadiens plus âgés, en particulier ceux de 55 ans et plus, sont plus susceptibles de faire mention d'arnaques par courriel et par hameçonnage. Les hommes sont plus susceptibles d'avoir subi des attaques par un virus, un logiciel espion, un logiciel malveillant ou un rançongiciel. En revanche, les Canadiennes et les Canadiens possédant des connaissances avancées en matière de sécurité en ligne sont plus susceptibles de déclarer n'avoir jamais été victimes de ce type de cyberattaques.

Le changement de mot de passe et les communications avec la banque continuent d'être les principales réponses à une cyberattaque

Si les répondants apprenaient qu'ils avaient été victimes d'une cyberattaque, ou soupçonnaient de l'avoir été, la plupart affirment qu'ils prendraient des mesures de protection. Les réponses les plus fréquentes comprennent le changement de mot de passe (78 %), les communications avec leur banque (70 %) et la suppression de contenus suspects (51 %). Des proportions plus faibles affirment qu'elles mettraient à jour les logiciels de sécurité (44 %), contacteraient les principales agences d'évaluation de crédit canadiennes (35 %) ou débrancheraient les appareils de leur réseau (34 %). Environ un quart des répondants appelleraient la police (28 %), communiqueraient avec un spécialiste informatique (28 %) ou éteindraient leur ordinateur (27 %). Deux personnes sur dix (22 %) déclarent qu'elles demanderaient l'aide d'un ami ou d'un membre de la famille.

Au fil du temps, les mesures que les Canadiennes et les Canadiens en ligne prendraient pour se protéger sont restées relativement stables.

Diagramme 26 : Réponses à une cyberattaque



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

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

- Les résidents du Québec sont plus susceptibles que les autres personnes au pays de contacter les principales agences d'évaluation de crédit du Canada.
- Les Canadiennes et les Canadiens en ligne âgés de 65 ans et plus sont plus susceptibles que les plus jeunes de fermer leur ordinateur et de supprimer le contenu suspect.
- Les femmes sont plus susceptibles que les hommes de se tourner vers un tiers pour obtenir de l'aide et, plus précisément, de communiquer avec leur banque, un spécialiste des TI, un ami ou un membre de leur famille.

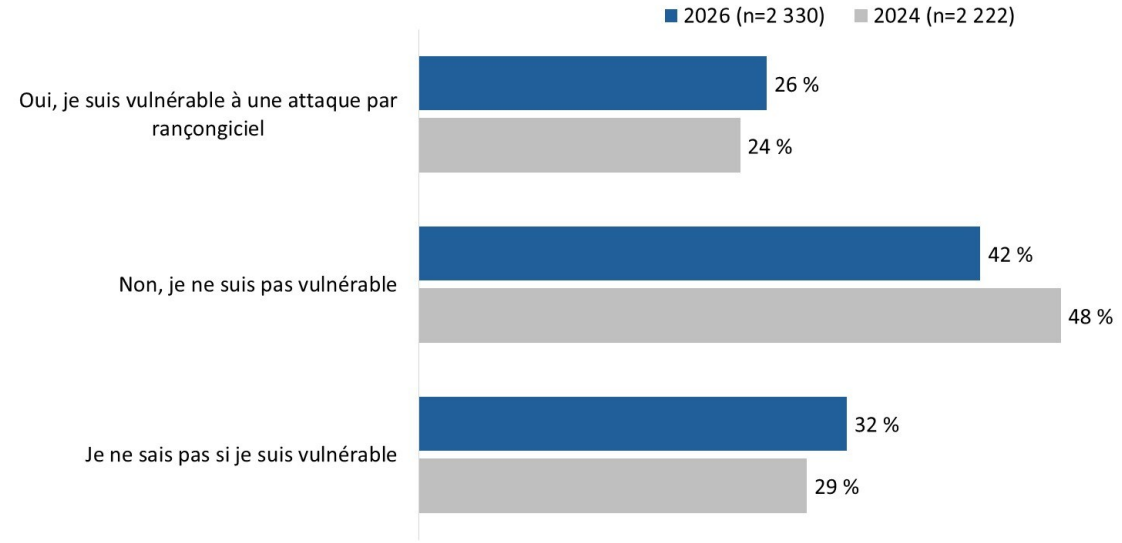
Un quart des répondants croient qu'ils sont vulnérables à une attaque par rançongiciel

Un quart (26 %) des Canadiennes et des Canadiens en ligne pensent être vulnérables à une attaque par rançongiciel, tandis que 42 % estiment ne pas l'être (contre 48 % en 2024). Les autres répondants (32 %) ne savent pas s'ils sont vulnérables à une telle attaque.

L'impression de vulnérabilité face aux attaques par rançongiciel varie selon les groupes. Les résidents de la Saskatchewan et du Manitoba (comparativement à ceux du Canada atlantique, du Québec et de la Colombie-Britannique, y compris ceux des territoires), la génération X, les hommes et les propriétaires d'entreprise se disent plus vulnérables. Les répondants possédant un niveau de connaissances avancé concernant la sécurité en ligne sont plus susceptibles de croire qu'ils ne sont pas vulnérables.

Les Canadiennes et les Canadiens âgés de 35 à 64 ans sont plus susceptibles que les plus jeunes de se sentir vulnérables, tandis que les répondants de 65 ans et plus ont plus tendance à dire qu'ils ne sont pas certains d'être vulnérables.

Diagramme 27 : Vulnérabilité à une attaque par rançongiciel

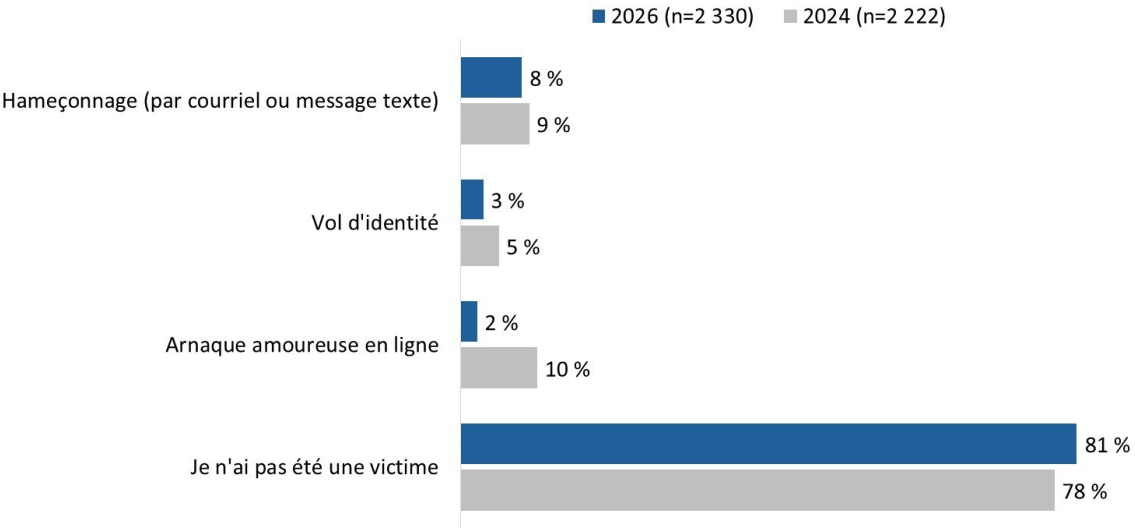


QCT8. Croyez-vous être vulnérable à une attaque par rançongiciel? Base de référence : tous les répondants.

Peu de Canadiennes et de Canadiens en ligne disent avoir été victimes d'une arnaque en ligne

La plupart des Canadiennes et des Canadiens en ligne (81 %) déclarent ne pas avoir été victimes d'une arnaque en ligne impliquant une perte d'argent ou de données. Les arnaques par hameçonnage sont le type le plus fréquemment signalé (8 %), suivi du vol d'identité (3 %) et des arnaques amoureuses en ligne (2 %, contre 10 %).

Diagramme 28 : Expérience personnelle des arnaques en ligne ayant mené à une perte d'argent ou de données



QCCE1. Avez-vous subi personnellement une perte d'argent ou de données à cause d'arnaques en ligne? / QCCE1B. Est-ce que c'était à cause…? Base de référence : tous les répondants.

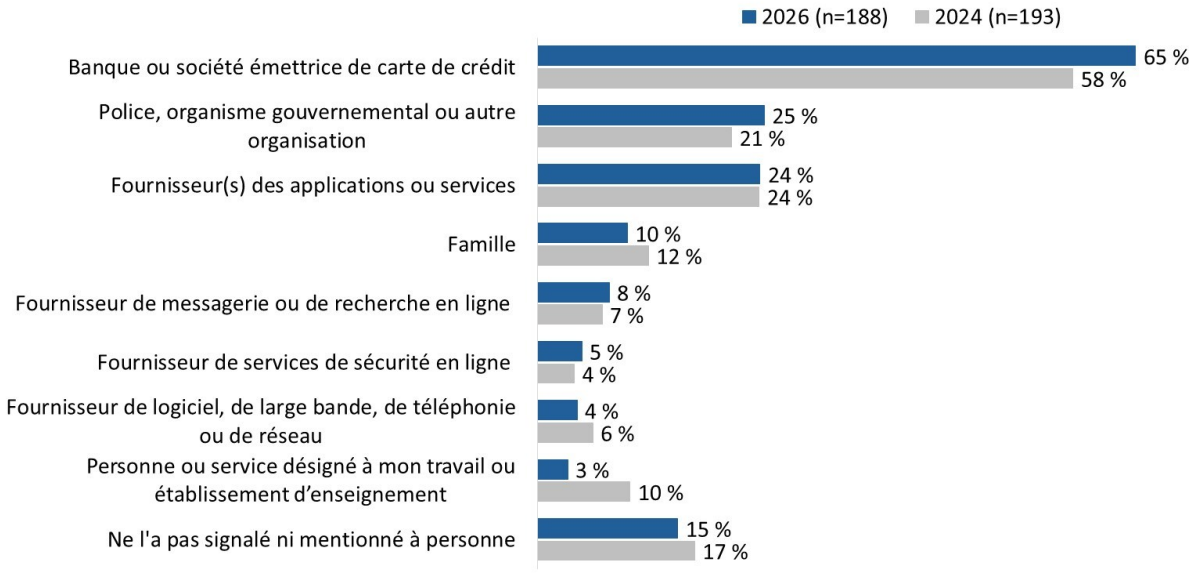
La fréquence des arnaques en ligne impliquant des pertes financières ou de données est plus élevée chez les ménages à faible revenu (moins de 40 000 $ par an) et les personnes possédant des connaissances de base ou de niveau débutant concernant la sécurité en ligne.

Les expériences déclarées varient selon la région et l'âge. Les résidents du Canada atlantique sont plus susceptibles que ceux du Québec, de l'Ontario, de l'Alberta et de la Colombie-Britannique, y compris des territoires, de signaler avoir été victimes d'hameçonnage. Les résidents de l'Ontario sont plus nombreux que ceux du Canada atlantique, de la Saskatchewan, du Manitoba et de l'Alberta d'avoir subi un vol d'identité. Les baby-boomers sont plus susceptibles que les membres de la génération Z et les milléniaux d'avoir été victimes d'hameçonnage.

Les victimes d'hameçonnage sont les plus susceptibles de signaler l'incident à leur institution financière

Parmi les personnes ayant été victimes d'hameçonnage (n=188), la plupart déclarent avoir signalé l'incident à leur banque ou à leur société émettrice de carte de crédit (65 %). De plus, environ un quart des répondants ont contacté la police ou un organisme gouvernemental (25 %) ou le fournisseur de services ou d'applications concerné (24 %). D'autres réponses ont été mentionnées moins fréquemment; elles figurent toutes dans le diagramme 29.

Diagramme 29 : Signalement par les victimes des tentatives d'hameçonnage

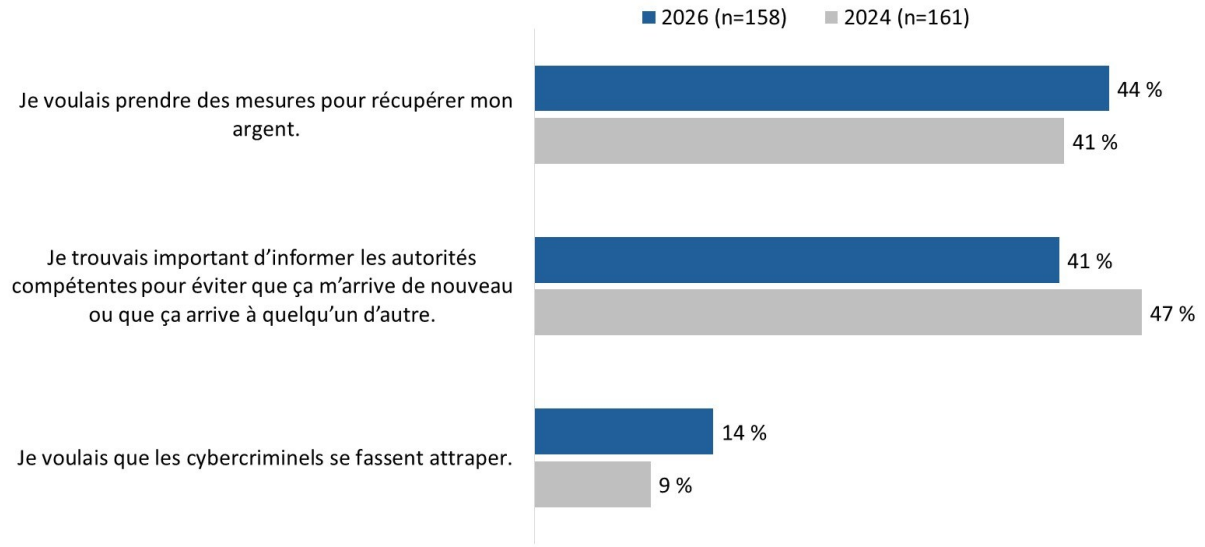


QCCE2. Vous avez mentionné avoir subi une perte d'argent ou de données à cause d'une tentative d'hameçonnage. L'avez-vous signalé à quelqu'un? Base de référence : répondants ayant été victimes d'hameçonnage. [Plusieurs réponses acceptées].

La raison de signaler les arnaques par hameçonnage varie, tout comme les raisons de ne pas signaler un tel incident

Parmi les personnes ayant été victimes d'hameçonnage et l'ayant signalé (n=158), 44 % l'ont fait parce qu'elles voulaient récupérer leur argent et 41 % estimaient qu'il était important d'en informer les autorités compétentes afin d'éviter qu'un tel incident ne se reproduise. Seulement quatorze pour cent des répondants déclarent avoir signalé l'incident parce qu'ils voulaient que les cybercriminels soient arrêtés.

Diagramme 30 : Raisons invoquées pour signaler les tentatives d'hameçonnage



QCCE3. Quelle est la principale raison pour laquelle vous avez signalé une tentative d'hameçonnage? Base de référence : répondants ayant été victimes d'hameçonnage et qui l'ont signalée.

Les personnes ayant été victimes d'hameçonnage et qui ne l'ont pas signalé (n=30) ont le plus souvent justifié leur décision en disant que le montant d'argent perdu était négligeable ou que les données compromises avaient peu d'importance, ou elles avaient l'impression qu'aucune mesure ne serait prise.

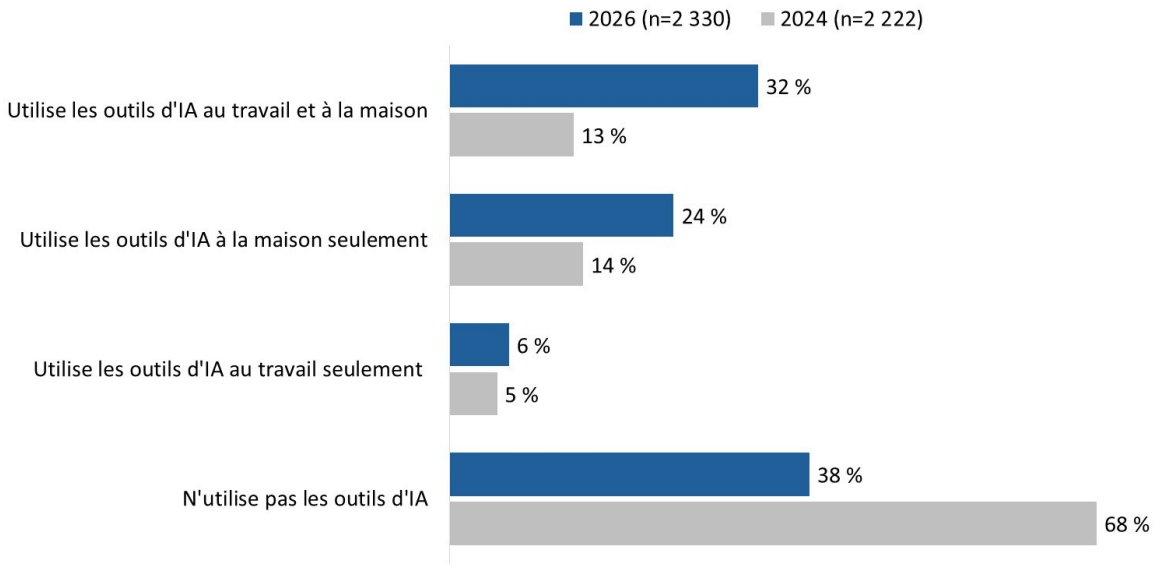
4. Les perspectives concernant l'intelligence artificielle

L'utilisation d'outils de l'IA a augmenté considérablement depuis 2024

L'utilisation d'outils de l'IA, tels que ChatGPT, CoPilot, DALL-E, a considérablement augmenté depuis 2024, alors qu'un tiers des répondants (32 %) avaient déclaré utiliser ces outils. En 2026, ce pourcentage a presque doublé pour atteindre 62 %. En ce qui concerne l'utilisation des outils de l'IA en ligne par les Canadiennes et les Canadiens, 32 % déclarent utiliser les outils de l'IA au travail et à la maison (contre 13 % en 2024), 24 % ne les utilisent qu'à la maison (contre 14 %) et 6 % ne s'en servent qu'au travail.

L'utilisation des outils de l'IA varie selon l'âge et le revenu. L'utilisation uniquement à domicile est plus fréquente chez les Canadiennes et les Canadiens de 65 ans et plus, tandis que l'utilisation au travail et à la maison est plus courante chez les répondants de moins de 45 ans et ceux dont le revenu du ménage dépasse 150 000 $. Les baby-boomers et la génération silencieuse sont plus susceptibles de ne pas utiliser d'outils de l'IA.

Diagramme 31 : Utilisation des outils de l'IA

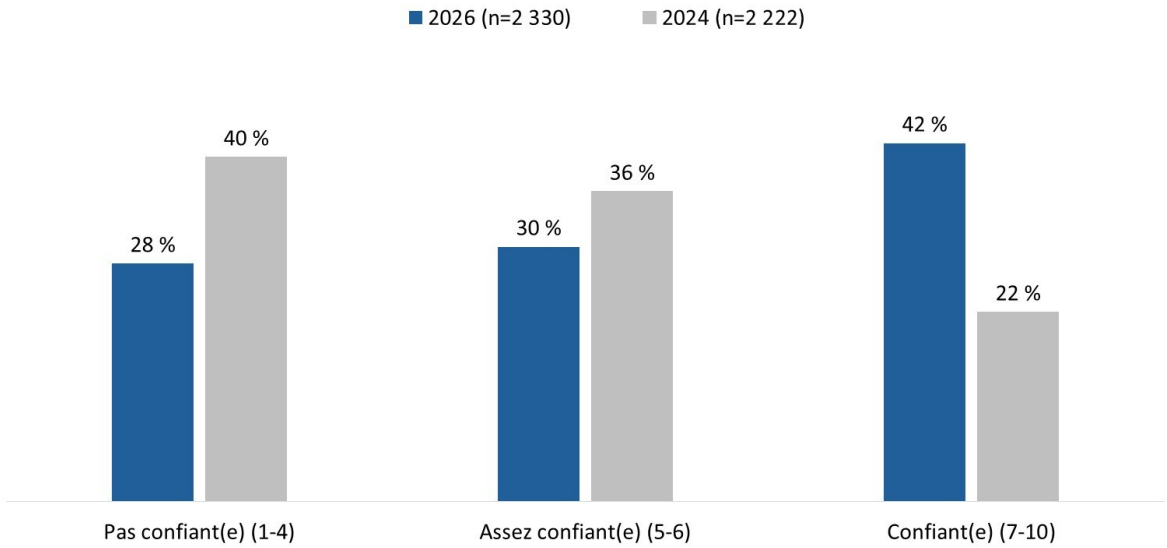


QAI1: Utilisez-vous des outils de l'intelligence artificielle (IA) à la maison ou au travail? Base de référence : tous les répondants.

La confiance des répondants en leur capacité à reconnaître du contenu généré par l'IA augmente

Parallèlement à l'utilisation croissante des outils de l'IA, de plus en plus de Canadiennes et de Canadiens en ligne déclarent avoir confiance en leur capacité à reconnaître du contenu généré par l'IA. Quatre personnes sur dix (42 %) se disent capables (cotes de 7 à 10) de repérer les messages, images, vidéos ou hypertrucages générés par l'IA. Il s'agit d'une augmentation de 20 points depuis 2024, lorsque 22 % déclaraient posséder ce niveau de confiance. Par ailleurs, 30 % des répondants étaient relativement confiants, tandis que 28 % n'avaient pas confiance en leur capacité à identifier du contenu généré par l'IA.

Diagramme 32 : Confiance en sa capacité de reconnaître 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 : tous les répondants.

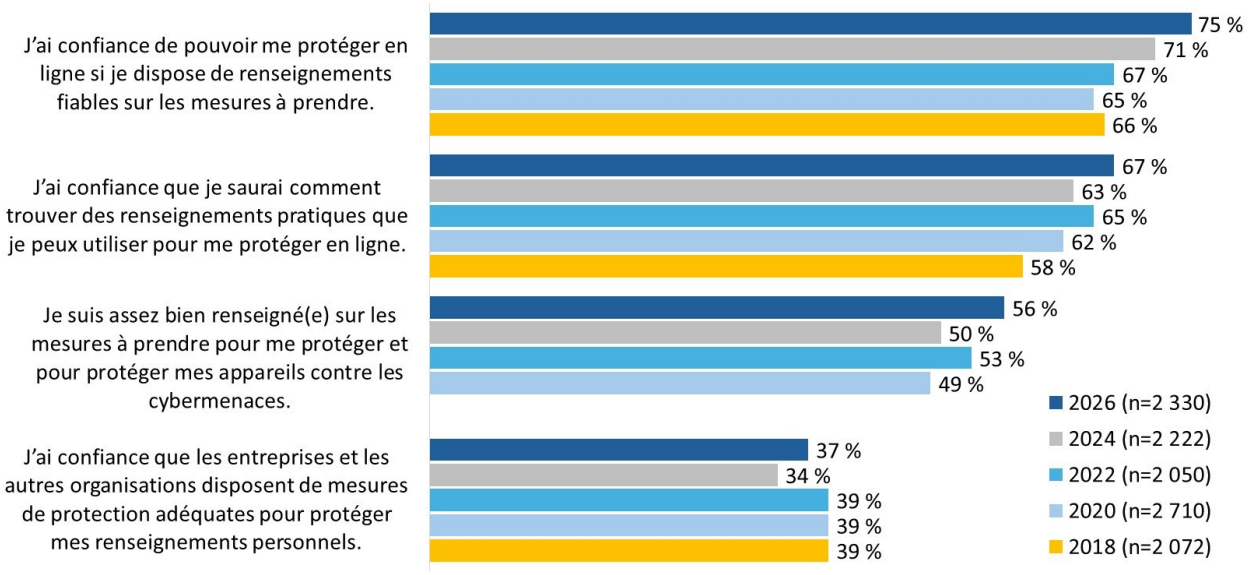
Les jeunes Canadiennes et Canadiens en ligne, les hommes, les titulaires d'un diplôme d'études secondaires et les personnes possédant des connaissances avancées concernant la sécurité en ligne sont plus susceptibles d'avoir confiance en leur capacité à reconnaître le contenu généré par l'IA.

5. Les communications et la campagne Pensez cybersécurité

Le niveau de confiance des répondants en leur capacité à obtenir et à utiliser des renseignements sur la cybersécurité a augmenté

Les trois quarts (75 %) des Canadiennes et des Canadiens en ligne ont confiance qu'ils pourront se protéger en ligne tant qu'ils disposent d'informations fiables sur les étapes à suivre. Les deux tiers (67 %) ont confiance qu'ils sauront comment trouver des informations pratiques qu'ils peuvent utiliser pour se protéger en ligne. De plus, un peu plus de la moitié des répondants (56 %, contre 50 %) estiment avoir suffisamment d'informations sur la manière de prendre des mesures pour se protéger, eux et leurs appareils, contre les cybermenaces. Une proportion beaucoup moins importante (37 %) est convaincue que les entreprises et autres organisations disposent de mesures de sécurité adéquates pour protéger leurs renseignements personnels.

Diagramme 33 : Renseignements sur la prévention des cybermenaces : pourcentage de répondants se disant d'accord avec l'énoncé



QINFO1. Veuillez indiquer dans quelle mesure vous êtes d'accord ou en désaccord avec les énoncés ci-dessous. Base de référence : tous les répondants. [Plusieurs réponses acceptées].

Voici certaines différences entre les sous-groupes qui sont dignes de mention :

- Les jeunes Canadiennes et Canadiens en ligne sont plus susceptibles de penser avoir assez d'informations pour prendre des mesures afin de se protéger, d'avoir confiance qu'ils peuvent se protéger eux-mêmes et de trouver des informations pratiques.
- Les hommes sont plus susceptibles que les femmes de déclarer qu'ils ont suffisamment d'informations sur les façons de prendre des mesures pour se protéger contre les cybermenaces et d'être certains de pouvoir trouver des informations pratiques pour se protéger en ligne.

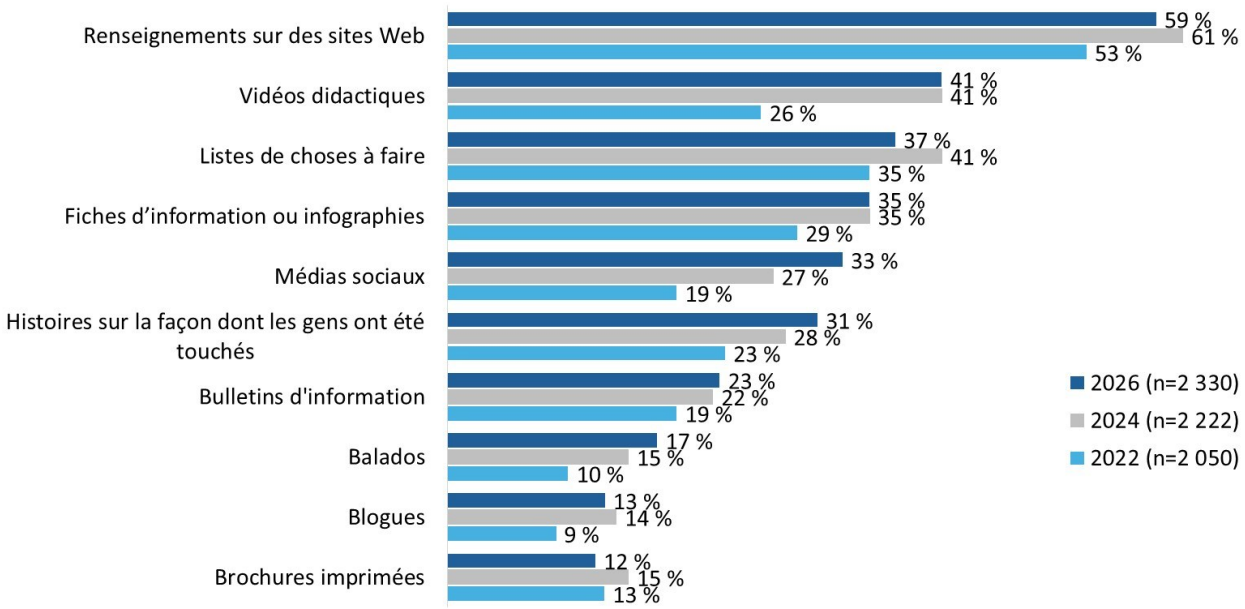
- Les personnes qui touchent un revenu annuel plus élevé (100 000 $ et plus) ont plus tendance à dire qu'elles disposent de suffisamment d'informations pour se protéger elles-mêmes et protéger leurs appareils.
- La génération silencieuse, suivie des baby-boomers, a le plus besoin d'informations : ces personnes n'ont pas beaucoup confiance en leur capacité de trouver des renseignements pratiques et de se protéger en ligne grâce à des informations fiables, et elles ont plus souvent l'impression de ne pas avoir suffisamment d'informations pour prendre des mesures afin d'assurer leur protection en ligne.

Les sites Web continuent d'être la source préférée pour obtenir de l'information sur la cybersécurité

Cinquante-neuf pour cent des Canadiennes et des Canadiens en ligne déclarent préférer recevoir des informations sur les façons de se protéger contre les cybermenaces par l'entremise des sites Web. Les vidéos didactiques (41 %) et les listes de choses à faire (37 %) sont deux autres sources privilégiées. Environ un tiers des répondants s'intéressent aux fiches d'information ou aux infographies (35 %) ou aux médias sociaux (33 %). La liste complète des formats préférés figure dans le diagramme 34.

Les trois mêmes formats — sites Web, vidéos didactiques et listes de choses à faire — continuent de se classer en tête de liste. Les résultats sont généralement cohérents avec ceux de 2024; la plupart des différences annuelles comportent moins de cinq points de pourcentage. Les médias sociaux, qui sont cités plus fréquemment cette année que lors des vagues précédentes, en sont l'exception.

Diagramme 34 : Source préférée pour se renseigner sur les cybermenaces



QINFO2. Comment préférez-vous obtenir de l'information pour vous protéger contre les cybermenaces? Base de référence : tous les répondants. [Plusieurs réponses acceptées].

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

- Les Canadiennes et les Canadiens en ligne âgés de 65 ans ou plus sont les plus susceptibles de préférer les listes de choses à faire et les brochures imprimées. En revanche, les jeunes Canadiennes et Canadiens (ceux de moins de 35 ans) ont tendance à préférer les médias sociaux et l'information sur

les sites Web, tandis que les personnes de moins de 45 ans préfèrent les histoires concernant les répercussions sur les gens.

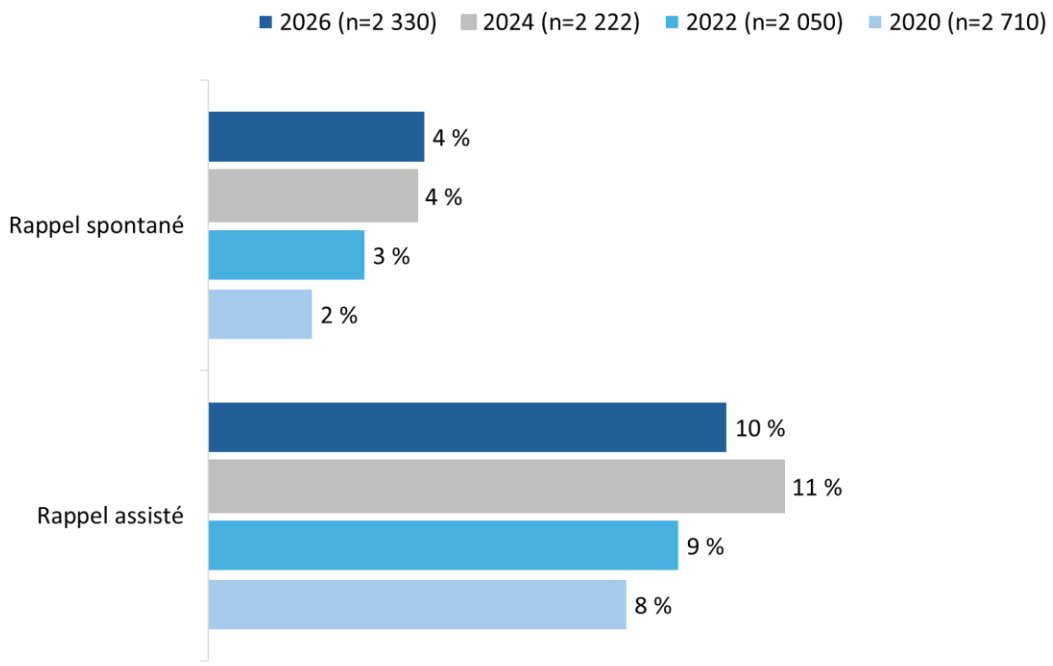
- De plus en plus d'hommes se tournent vers des balados, des blogues et des sites d'information pour obtenir des renseignements sur les façons de se protéger. Les femmes, en revanche, ont tendance à préférer les fiches d'information ou les infographies, les listes de choses à faire et les brochures imprimées.
- Les diplômés universitaires sont plus susceptibles de préférer les fiches d'information ou les infographies, ainsi que les vidéos didactiques.

Encore peu de gens ont entendu parler de la campagne Pensez cybersécurité

Le niveau de connaissances relatives à la campagne demeure inchangé depuis 2024 : 4 % des Canadiennes et des Canadiens en ligne peuvent nommer spontanément la campagne de sensibilisation à la cybersécurité du gouvernement du Canada. Lorsqu'on donne de l'information, un répondant sur dix (10 %) dit connaître la campagne Pensez cybersécurité.

Les membres de la génération Z sont plus susceptibles de se souvenir de la campagne quand ils reçoivent de l'information à ce sujet.

Diagramme 35 : Connaissance de la campagne du gouvernement du Canada sur la cybersécurité



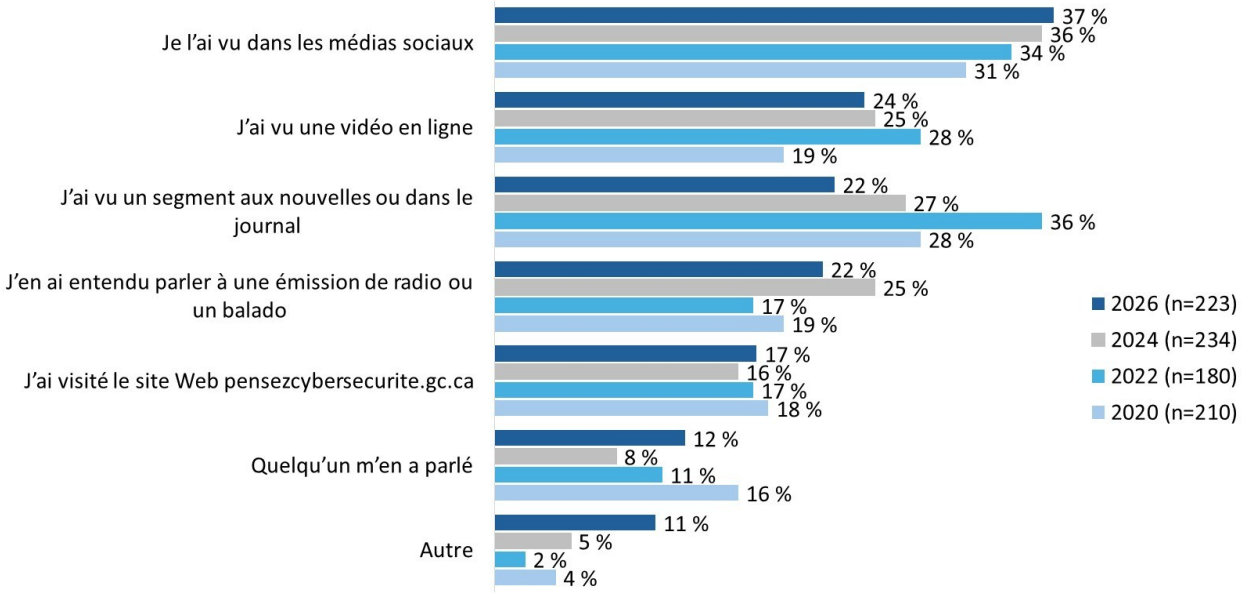
QGCS1. Une campagne de sensibilisation du gouvernement du Canada a été créée pour informer les Canadiens et les Canadiennes sur la cybersécurité et sur les mesures simples qu'ils et qu'elles peuvent prendre pour se protéger en ligne. Pouvez-vous nommer cette campagne? / QGCS3. Avez-vous vu, lu ou entendu 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.

Environ quatre personnes sur 10 disent avoir été mises au courant de la campagne par l'entremise des médias sociaux

Parmi les répondants qui connaissent la campagne Pensez cybersécurité (n=223), un peu plus d'un tiers (37 %) déclarent en avoir entendu parler dans les médias sociaux. Environ deux personnes sur dix indiquent avoir vu une vidéo en ligne (24 %), un segment aux nouvelles ou dans un journal (22 %), ou en avoir entendu parler grâce à une émission de radio ou un balado (22 %). Des proportions plus faibles de répondants mentionnent avoir visité le site Web de la campagne Pensez cybersécurité (17 %) ou avoir entendu parler de la campagne par une autre personne (12 %).

La proportion de Canadiennes et de Canadiens en ligne qui indiquent avoir vu un segment aux nouvelles ou dans un journal continue de diminuer, passant de 36 % en 2022 à 27 % en 2024 et à 22 % en 2026.

Diagramme 36 : Source d'information au sujet de la campagne Pensez cybersécurité



QGCS4. Où l'avez-vous vu, lu ou entendu? Base de référence : répondants ayant entendu parler de la campagne Pensez cybersécurité. [Plusieurs réponses acceptées].

6. Les entreprises et la cybersécurité

Les questions de cette section du rapport ont été posées uniquement aux Canadiennes et aux Canadiens en ligne qui possèdent une entreprise ou gèrent les employés d'une petite entreprise (n=300).

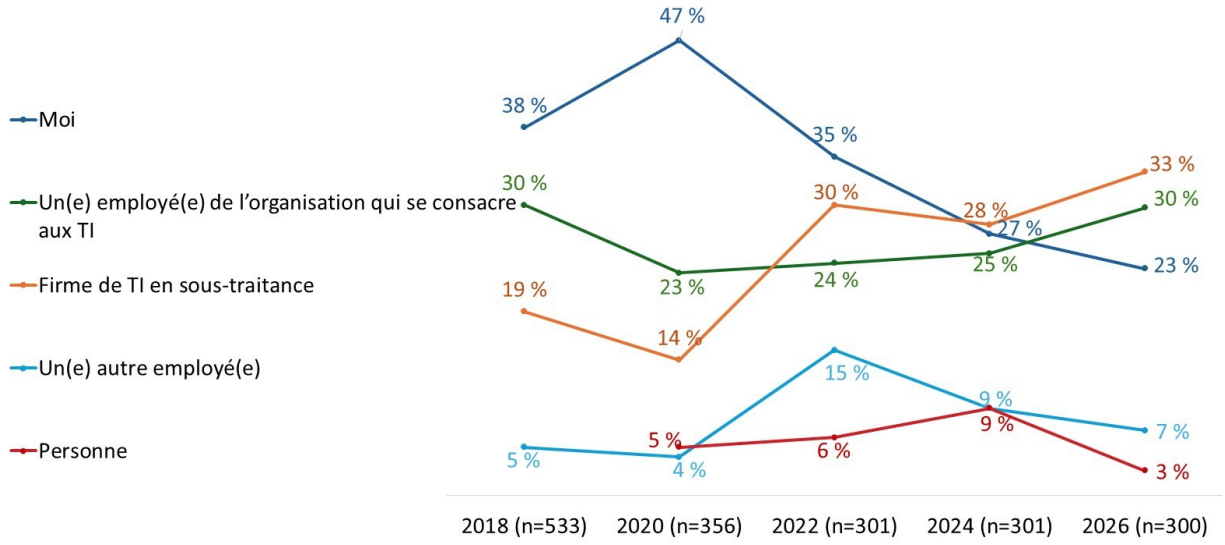
Aux fins du présent sondage, les petites entreprises sont considérées comme des établissements employant jusqu'à 100 personnes. Un peu plus d'un quart (26 %) des entreprises de l'échantillon emploie moins de cinq personnes. Parmi les autres, 16 % emploient entre cinq et neuf personnes, 38 % entre 10 et 49 personnes, et 20 % entre 50 et 100 personnes.

La responsabilité des TI est confiée à d'autres entreprises

Un tiers (33 %) des personnes interrogées représentant une entreprise déclarent confier le soutien informatique à une autre entreprise. Trois personnes sur dix (30 %) disent avoir un employé des TI à l'interne, tandis que 23 % affirment être personnellement responsables de l'informatique de leur entreprise. Relativement peu de répondants de ce groupe indiquent qu'un employé qui ne consacre pas exclusivement son temps à l'informatique s'occupe de l'informatique (7 %) ou que personne n'est responsable (3 %).

Un moins grand nombre de propriétaires et de gestionnaires déclarent gérer personnellement l'informatique de leur entreprise; la proportion est passée de 47 % en 2020 à 35 % en 2022, à 27 % en 2024 et à 23 % en 2026. Le recours à des fournisseurs informatiques externes a généralement augmenté au fil du temps (14 % en 2020 contre 33 % en 2026), bien que les niveaux aient légèrement fluctué entre les vagues. Le recours à un soutien informatique spécial à l'interne a augmenté cette année après avoir été constant entre 2020 et 2024; il est revenu aux résultats de référence de 2018.

Diagramme 37 : Responsabilité des TI de l'entreprise



QBUS1. Qui est responsable des TI pour votre société? Base de référence : répondants qui sont des entreprises.

La plupart des entreprises ont pris des mesures pour se protéger contre les cybermenaces

La plupart des répondants (77 %) affirment que leur entreprise a pris des mesures pour se protéger contre les cybermenaces. Parmi les autres, 4 % affirment qu'aucune mesure n'a été mise en œuvre, tandis que 18 % ne savent pas si leur entreprise a agi en ce sens.

Au moins la moitié des propriétaires et gestionnaires d'entreprise déclarent que leur organisation exige une protection par mot de passe sur tous les appareils (59 %), tient à jour les logiciels de sécurité sur tous les appareils (55 %), et utilise la protection par mot de passe ou l'authentification d'utilisateur pour l'accès sans fil et à distance (52 %). La liste complète des mesures est présentée dans le diagramme 38.

Les mesures de cybersécurité sont restées stables au fil du temps, à quelques exceptions près. De plus en plus d'entreprises adoptent une politique en matière de cybersécurité pour les employés (25 % contre 33 %) et proposent des formations concernant les pratiques exemplaires en matière de cybersécurité (24 % contre 32 %), tandis qu'un moins grand nombre d'entre elles sauvegardent l'information sur tous les appareils (42 % en 2024 contre 37 % en 2026).

Diagramme 38 : Mesures mises en œuvre par les entreprises pour se protéger contre les cybermenaces

	2026 (n=300)	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	59 %	57 %	69 %	57 %	71 %
Tenir à jour les logiciels de sécurité sur tous les appareils	55 %	55 %	63 %	51 %	69 %
Utiliser un mot de passe ou une authentification d'utilisateur pour l'accès sans fil et à distance	52 %	51 %	60 %	52 %	67 %
Établir des filtres de pourriels	39 %	40 %	49 %	39 %	54 %
Sauvegarder l'information sur tous les appareils	37 %	42 %	58 %	49 %	60 %
Adopter une politique en matière de cybersécurité à l'intention des employés	33 %	25 %	32 %	18 %	--
Offrir aux employés une formation sur les pratiques exemplaires en matière de cybersécurité	32 %	24 %	24 %	15 %	--
Utiliser un logiciel de cryptage	31 %	31 %	34 %	23 %	36 %
Suivre les protocoles de suppression de l'information lorsque les employés quittent l'organisation	27 %	27 %	28 %	18 %	37 %
Ne pas utiliser de compte d'administrateur pour l'accès au Web	14 %	14 %	24 %	15 %	25 %
Aucune de ces mesures	4 %	*6 %*	*5 %*	*9 %*	*5 %*
Ne sait pas	18 %	*16 %*	*8 %*	*10 %*	*5 %*

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

La plupart des entreprises bénéficieraient de renseignements sur les cybermenaces

En ce qui concerne la protection de leur entreprise contre les cybermenaces, environ un tiers des propriétaires et gestionnaires d'entreprise ont déclaré que leur organisation bénéficierait de directives pour réagir à une cyberattaque (36 %, contre 44 % en 2024), d'une liste des types de menaces existantes et de signaux à rechercher (36 %, contre 42 % en 2024), des conseils ou ressources sur le type de logiciel ou de matériel permettant de sécuriser les réseaux (35 %), et les pratiques exemplaires sécuritaires en

informatique en nuage (35 %). La liste complète des informations jugées utiles par les répondants se trouve dans le tableau ci-dessous.

Diagramme 39 : Renseignements sur les cybermenaces dont les entreprises pourraient tirer profit

	2026 (n=300)	2024 (n=301)	2022 (n=301)	2020 (n=360)	2018 (n=533)
Directives pour réagir à une cyberattaque	36 %	44 %	50 %	40 %	46 %
Liste de types de menaces qui existent et signaux à rechercher	36 %	42 %	49 %	41 %	47 %
Pratiques exemplaires sécuritaires en informatique en nuage	35 %	34 %	43 %	36 %	35 %
Conseils et ressources pour le type de logiciel ou matériel permettant de sécuriser des réseaux	35 %	33 %	41 %	29 %	36 %
Mesures pour protéger les appareils mobiles dans un lieu public	32 %	38 %	44 %	39 %	40 %
Directives pour mettre en place des règles relatives à la politique d'utilisation sécuritaire des courriels	32 %	35 %	40 %	28 %	39 %
Ressources sur la façon de crypter des ordinateurs, portables et dispositifs de stockage	31 %	33 %	41 %	34 %	37 %
Pratiques exemplaires sur la façon pour les employés de gérer les mots de passe	30 %	32 %	44 %	29 %	37 %
Conseils pour communiquer aux employé(e)s l'importance de suivre des politiques de cybersécurité	30 %	28 %	35 %	25 %	32 %
Directives sur l'utilisation de dispositifs personnels au travail	30 %	27 %	42 %	31 %	40 %
Pratiques exemplaires pour une politique d'utilisation d'Internet claire	30 %	26 %	38 %	27 %	37 %
Mesures pour gérer les renseignements liés au travail que possèdent les employés qui quittent l'organisation	29 %	27 %	33 %	22 %	33 %
Pratiques exemplaires pour l'utilisation de dispositifs de stockage	28 %	31 %	39 %	34 %	40 %
Directives sur la façon d'établir une politique en matière de médias sociaux	22 %	22 %	28 %	26 %	37 %
Autre	3 %	3 %	4 %	3 %	4 %
Aucune de ces mesures	*7 %*	*5 %*	*5 %*	*9 %*	*8 %*
Ne sait pas	*21 %*	*12 %*	*11 %*	*13 %*	*12 %*

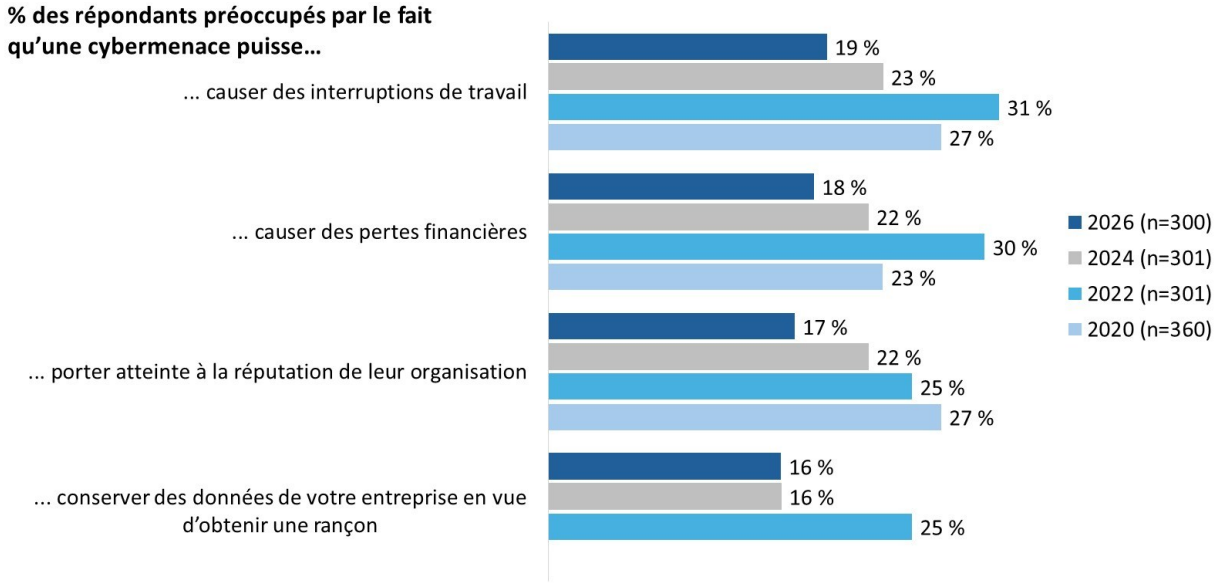
QBUS3. De quels types de renseignements parmi les suivants croyez-vous que votre organisation tirerait profit pour se protéger contre les cybermenaces? Base de référence : répondants qui sont des entreprises. [Plusieurs réponses acceptées].

Les préoccupations concernant les cybermenaces ont diminué d'une année à l'autre

Lorsqu'ils réfléchissaient aux activités courantes de leur entreprise, environ deux propriétaires et gestionnaires sur dix exprimaient des inquiétudes concernant les interruptions de travail (19 %), les pertes financières (18 %) et les atteintes à la réputation (17 %). Seize pour cent craignaient que les données de leur entreprise soient conservées en vue d'obtenir une rançon.

Depuis 2022, les préoccupations ont diminué sur presque tous les plans. La préoccupation concernant la conservation de données des entreprises en vue d'une rançon, qui est restée stable à 16 % depuis 2024, est l'exception.

Diagramme 40 : Niveau de préoccupation concernant les répercussions des 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...? Base de référence : répondants qui sont des entreprises.

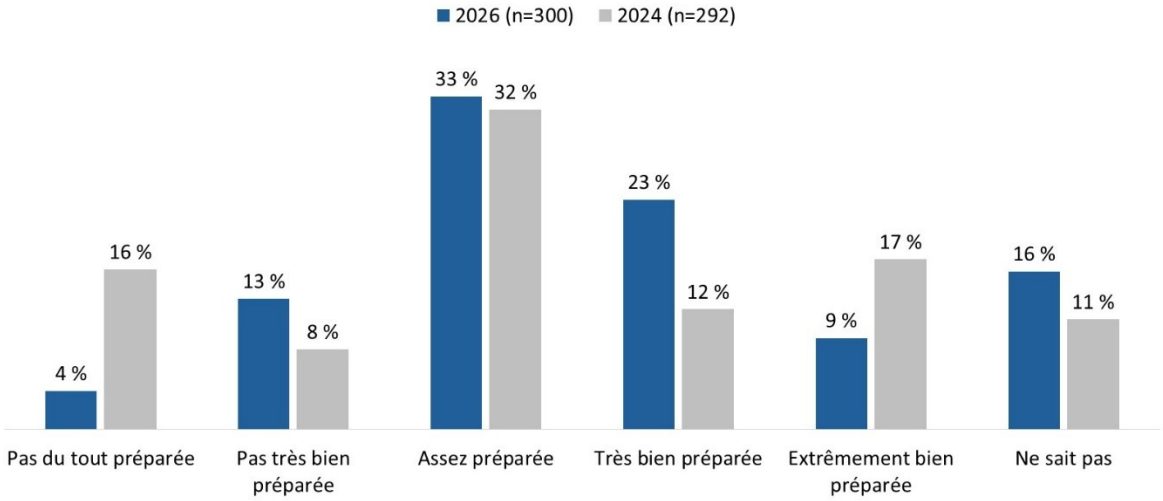
Les deux tiers des entreprises sont au moins en partie préparés à se défendre contre les attaques par rançongiciel

La majorité des propriétaires et gestionnaires d'entreprise affirment que leur entreprise est au moins en partie préparée à se défendre contre les attaques par rançongiciel; 33 % se sentent assez préparés, 23 % se disent très bien préparés et 9 %, extrêmement bien préparés. Environ deux répondants sur dix (17 %) déclarent que leur entreprise n'est pas préparée, tandis que 16 % ne savent pas comment évaluer l'état de préparation de leur organisation.

Au fil du temps, les perceptions de l'état de préparation sont demeurées stables.[2]

[2] L'échelle a été modifiée en 2026 pour comporter 5 points (au lieu de 7). Les données de 2024 ont été comprimées afin de correspondre à celles de 2026. Les différences observées au fil du temps ne sont pas significatives sur le plan statistique.

Diagramme 41 : État de préparation pour se défendre contre les attaques par rançongiciel



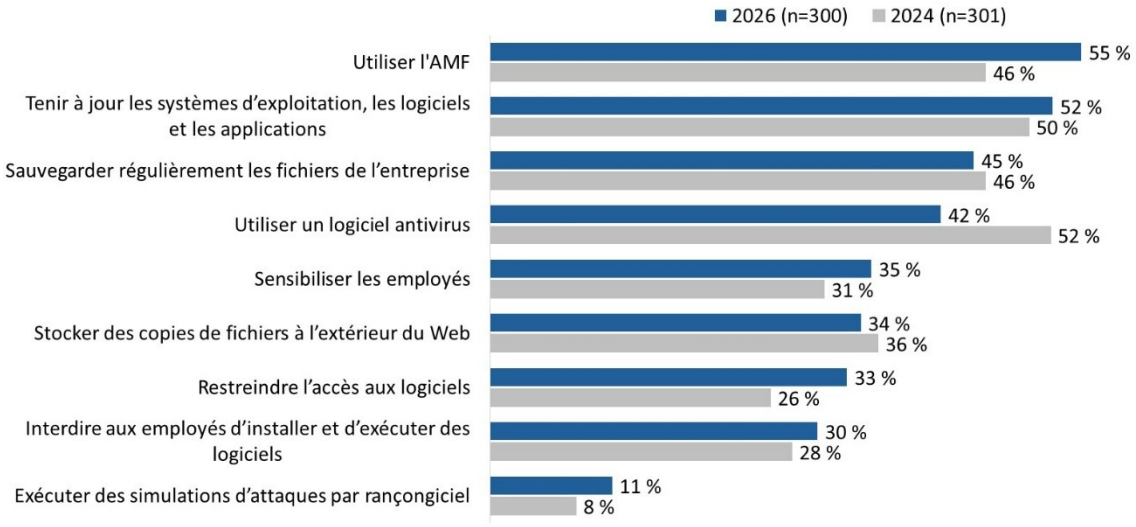
QBUS5. Selon vous, dans quelle mesure votre entreprise est-elle préparée actuellement pour se défendre contre des attaques par rançongiciel? Base de référence : répondants qui sont des entreprises.

Environ la moitié des entreprises se servent de l'AMF et effectuent les mises à jour de leurs systèmes

Environ la moitié des propriétaires et gestionnaires d'entreprise ont déclaré que leur entreprise utilise l'AMF (55 %, contre 46 % en 2024) et tient à jour les systèmes d'exploitation, les logiciels et les applications (52 %). Quarante-cinq pour cent des répondants sauvegardent régulièrement les fichiers de l'entreprise, tandis qu'un nombre légèrement inférieur utilise des logiciels antivirus (42 %, contre 52 %).

De plus, environ un tiers des répondants sensibilisent leurs employés (35 %), stockent des copies de fichiers à l'extérieur du Web (34 %) et restreignent l'accès aux logiciels (33 %). Trois personnes sur dix (30 %) interdisent aux employés de procéder à l'installation ou à l'exécution de logiciels. Très peu de répondants (11 %) réalisent des simulations d'attaques par rançongiciel. Près d'un quart (23 %) des propriétaires et gestionnaires d'entreprise ne savent pas si leur entreprise a fait quelque chose pour se protéger contre les attaques par rançongiciel.

Diagramme 42 : Mesures mises en œuvre par les entreprises pour se protéger contre les attaques par rançongiciel

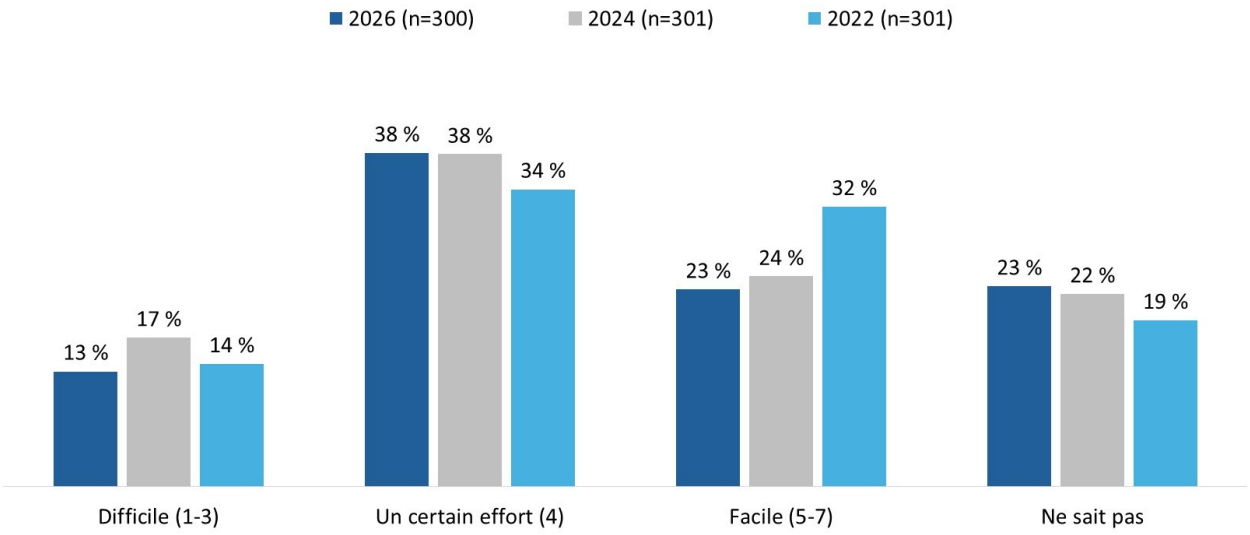


QBUS6. Qu'a fait, s'il y a lieu, votre entreprise pour se protéger contre les attaques par rançongiciel? Base de référence : répondants qui sont des entreprises. [Plusieurs réponses acceptées].

Se remettre d'une attaque par rançongiciel exigerait des efforts pour la plupart des entreprises

La moitié des propriétaires et gestionnaires d'entreprise affirment qu'il faudrait un certain effort (38 %) pour que leur entreprise se remette d'une attaque par rançongiciel, ou indiquent que cette dernière s'en remettrait difficilement (13 %). Environ un quart des répondants estiment qu'il serait facile pour leur entreprise de s'en remettre (23 %) ou ne le savent pas (23 %).

Diagramme 43 : Capacité de 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.

Profil des répondants au sondage

Les tableaux ci-dessous présentent le profil des répondants au sondage (à l'aide de données pondérées). Au total, 81 % des sondages ont été réalisés en anglais et 19 % en français.

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

Âge	**%**
18 à 24 ans	10 %
25 à 34 ans	17 %
35 à 44 ans	16 %
45 à 54 ans	16 %
55 à 64 ans	18 %
65 ans ou plus	24 %

Génération	**%**
Génération Z : 1997 à 2008	17 %
Milléniaux : 1981 à 1996	28 %
Génération X : 1965 à 1980	28 %
Baby-boomers : 1946 à 1964	25 %
Génération silencieuse : 1928 à 1945	3 %

Genre	**%**
Homme	47 %
Femme	49 %
Autre genre	1 %
Préfère ne pas répondre	2 %

Études	%
École primaire ou moins	2 %
École secondaire	14 %
Collège, école technique ou de métier	32 %
Programme universitaire de premier cycle	7 %
Programme universitaire de 2e ou 3e cycle, ou professionnel	50 %
Préfère ne pas répondre	2 %

Statut d'emploi	%
Emploi à temps plein	47 %
Emploi à temps partiel	7 %
Travail autonome	13 %
Sans emploi, mais à la recherche de travail	4 %
Aux études à temps plein	7 %
À la retraite	17 %
À l'extérieur de la population active	3 %
Autre	2 %
Préfère ne pas répondre	1 %

Revenu du ménage	%
Moins de 20 000 $	5 %
De 20 000 $ à moins de 40 000 $	8 %
De 40 000 $ à moins de 60 000 $	10 %
De 60 000 $ à moins de 80 000 $	10 %
De 80 000 $ à moins de 100 000 $	14 %
De 100 000 $ à moins de 150 000 $	20 %
150 000 $ et plus	20 %
Préfère ne pas répondre	13 %

Parent	%
Oui	35 %
Non	64 %
Préfère ne pas répondre	1 %

Âge des enfants	%
Moins de 5 ans	26 %
5 à 8 ans	28 %
9 à 12 ans	30 %
13 à 15 ans	30 %
16 à 17 ans	29 %

Fréquence de l'utilisation d'Internet	%
Quelques fois par semaine	<0,5 %
Quelques fois par jour	23 %
Je suis toujours branché(e)	77 %

Niveau de connaissances sur la sécurité en ligne	%
Avancé	20 %
Intermédiaire	46 %
Base	29 %
Novice/débutant	3 %
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 de 15 minutes a été mené auprès de 2 330 Canadiens et Canadiennes de 18 ans et plus qui utilisent Internet au moins quelques fois par mois. Les résultats globaux peuvent être considérés comme exacts dans ±2,1 %, 19 fois sur 20.
- 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 600 ménages avec enfants de moins de 18 ans (sous-échantillon de parents). En tout, 300 propriétaires et gestionnaires/superviseurs d'entreprise et 846 parents ont répondu au sondage. Les marges d'erreur sont plus grandes pour les résultats des sous-groupes de l'échantillon complet.
- 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 5 janvier 2026 auprès de 30 personnes. Quatorze sondages ont été réalisés en français et les autres l'ont été en anglais. La durée médiane du sondage était de 16,8 minutes. Le 9 janvier, des modifications ont été apportées au questionnaire afin d'en réduire la longueur (la durée cible était de 15 minutes). Des questions ont été supprimées et le libellé d'une question a été modifié. Par conséquent, les données du prétest n'ont pas été intégrées aux données du sondage final.
- Le travail sur le terrain a commencé le 9 janvier et s'est terminé le 29 janvier 2026.
- 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, 20 601 panélistes ont été recrutés pour participer à l'étude et 2 330 d'entre eux ont répondu au sondage. Le taux de participation s'élève donc à 14,2 %.

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 %	6 %
Québec	23 %	20 %
Ontario	39 %	41 %
Saskatchewan et Manitoba	6 %	7 %
Alberta	11 %	11 %
Colombie-Britannique et territoires	14 %	15 %

Âge	% pondérées	% non pondérées
18 à 24 ans	10 %	9 %
25 à 34 ans	17 %	17 %
35 à 44 ans	16 %	19 %
45 à 54 ans	16 %	18 %
55 à 64 ans	18 %	14 %
65 ans et plus	24 %	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 du sondage

Nous vous remercions d'avoir accepté de participer à ce court sondage mené par Phoenix SPI pour le 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 [INSERT]. 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 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]
01. Moins de quelques fois par mois [REMERCIER ET METTRE FIN AU SONDAGE]
02. Quelques fois par mois [REMERCIER ET METTRE FIN AU SONDAGE]
03. Une fois par semaine
04. Quelques fois par semaine
05. Quelques fois par jour
06. J'y suis toujours connecté(e) [PASSER À S6]

S5. [SI S4=03-05] 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 [REMERCIER ET METTRE FIN AU SONDAGE]
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 (30 heures par semaine ou plus)
02. Employé(e) à temps partiel (moins de 30 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]
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]
[ALTERNER L'ORDRE DES ÉNONCÉS]
a) Je trouve ça facile d'être en sécurité quand je suis en ligne.
b) Je suppose que tous mes appareils sont automatiquement sécurisés.
c) Me protéger complètement en ligne coûte cher.
d) Je ne comprends pas pourquoi je devrais mieux me protéger, car mes renseignements sont déjà en ligne.
e) Je m'inquiète à l'idée d'être victime d'un cybercrime.
f) 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]
g) Les membres de ma famille comptent sur moi pour assurer leur 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]
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]
[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 vos 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).

*Ajouter la description suivante : Le hameçonnage est une tentative, par des arnaqueurs, de se faire passer pour une organisation de confiance afin d'inciter les gens à fournir des renseignements personnels ou financiers. Les arnaqueurs se servent souvent de courriels, de messages texte ou de messages directs pour obtenir notamment des mots de passe ou des renseignements bancaires.

[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]
1-Pas du tout confiant(e)
2
3
4
5
6
7
8
9
10-Très confiant(e)

*Ajouter la description suivante : Le hameçonnage est une tentative, par des arnaqueurs, de se faire passer pour une organisation de confiance afin d'inciter les gens à fournir des renseignements personnels ou financiers. Les arnaqueurs se servent souvent de courriels, de messages texte ou de messages directs pour obtenir notamment des mots de passe ou des renseignements bancaires.

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? [Cyber24]
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]
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]
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]
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]
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] Savez-vous comment utiliser l'authentification multifactorielle (AMF)? **[CAB24]**

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]
[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 utiliser l'AMF.
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 utiliser l'AMF.
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.

QBEH12. Quelles mesures prenez-vous pour vérifier la légitimité d'un site web? **[CAB24]**
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? [Cyber24]
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]
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? [Cyber24]
Veuillez choisir toutes les réponses pertinentes

[ALTERNER L'ORDRE DES CHOIX DE RÉPONSE]
01. [NE PEUT ÊTRE SÉLECTIONNÉ AVEC LE CHOIX DE RÉPONSE 02] Mots de passe simples et faciles à mémoriser
02. [NE PEUT ÊTRE SÉLECTIONNÉ AVEC LE CHOIX DE RÉPONSE 01] Mots de passe complexes, avec une combinaison de lettres, de chiffres et de symboles
03. Phrase 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. Choisir une clé d'accès, lorsque c'est possible, au lieu d'un mot de passe (une clé d'accès est une méthode de connexion qui se sert de la biométrie enregistrée dans votre appareil, comme une empreinte digitale, la reconnaissance facile ou un NIP)
11. [ANCRAGE] Autre (veuillez préciser) :
12. [ANCRAGE] Rien de ce qui précède

13. [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]
« 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] Quelle est la principale raison pour laquelle vous utilisez rarement, voire jamais, des mots de passe uniques pour vos comptes en ligne? [CAB24]
[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]
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]
[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.

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... [Cyber24]
[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? [Cyber24]
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 semblent s'appliquer 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? [Cyber24]
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? [Cyber24]
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? [Cyber24]
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? [Cyber24]
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? **[Cyber24]**
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? [Cyber24]
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? [Cyber24]
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

QCCE1. Avez-vous subi personnellement une perte d'argent ou de données à cause d'arnaques en ligne? [CAB24-MODIFIÉE]
[ALTERNER L'ORDRE DES CHOIX DE RÉPONSE]
01. Oui
02. Non

QCCE1B. Est-ce que c'était à cause…[CAB24-MODIFIÉE]
Veuillez choisir toutes les réponses pertinentes
[ALTERNER L'ORDRE DES CHOIX DE RÉPONSE]
01. [MONTRER SI QCT16=07] D'une tentative d'hameçonnage (par courriel ou message texte).
02. D'une arnaque amoureuse en ligne [PASSER À QAI1]
03. D'un vol d'identité [PASSER À QAI1]
04. D'autre chose (veuillez préciser) [PASSER À QAI1]

Ajouter les descriptions suivantes :

- « 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 QCCE1B=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]
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]
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]
[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) :

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]
***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]
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? [Cyber24]
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? [Cyber24]
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? [Cyber24]

Veuillez choisir toutes les réponses pertinentes

[ALTERNER L'ORDRE DES CHOIX DE RÉPONSE]
01. Liste de types de menaces qui existent 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... [Cyber24]
[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]
01. Pas du tout préoccupé(e)
02. Pas très préoccupé(e)
03. Assez préoccupé(e)
04. Très préoccupé(e)
05. 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? [Cyber24]
01. Pas du tout préparé(e)
02. Pas très bien préparé(e)
03. Assez préparé(e)
04. Très bien préparé(e)
05. Extrêmement bien préparé(e)
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? [Cyber24]
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? [Cyber24]
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. [Cyber24]
[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? [Cyber24]
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? [Cyber24]
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? [Cyber24]
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? [Cyber24]
[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. Inférieur à un diplôme d'études secondaires ou l'équivalent
02. Diplôme d'études secondaires ou l'équivalent
03. Certificat ou diplôme d'apprenti inscrit ou d'une école de métiers
04. Certificat ou diplôme d'un collège, cégep ou d'un autre établissement non universitaire
05. Certificat ou diplôme universitaire inférieur au baccalauréat
06. Baccalauréat
07. Certificat ou diplôme universitaire supérieur au baccalauréat
08. 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 Canada. 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.