Sondage auprès d'utilisateurs d'Internet au sujet de la cybersécurité

Rapport final

Préparé pour Sécurité publique Canada

Fournisseur : LES ASSOCIÉS DE RECHERCHE EKOS INC.
No de contrat : OD160192340/001/CY
Valeur de l'entente : 122 983,55 $, taxes incluses
Date du contrat : 13 août 2018
Date de livraison : 30 septembre 2018

No d'inscription : ROP 032-18
Pour obtenir de plus amples renseignements sur le présent rapport, veuillez communiquer avec Sécurité publique Canada à ps.communications-communications.sp@canada.ca

This report is also available in English

Sondage auprès d'utilisateurs d'Internet au sujet de la cybersécurité

Rapport final

Préparé pour Sécurité publique Canada
Nom du fournisseur : LES ASSOCIÉS DE RECHERCHE EKOS INC.
Date : 30 septembre 2018

Ce rapport de recherche sur l'opinion publique présente les résultats d'un sondage en ligne mené par les Associés de recherche EKOS Inc. pour le compte de Sécurité publique Canada. L'étude de recherche a été menée auprès de 2 072 Canadiens du 21 août au 5 septembre 2018.

This report is also available in English under the title: Survey of Internet Users Regarding Cyber Security.

Cette publication ne peut être reproduite qu'à des fins non commerciales. Une autorisation écrite préalable doit d'abord être obtenue de Sécurité publique Canada. Pour obtenir de plus amples renseignements sur le présent rapport, veuillez communiquer avec Sécurité publique Canada à : ps.communications-communications.sp@canada.ca

ou à :
Secteur des communications
Sécurité publique Canada
269, avenue Laurier O.
Ottawa ON K1A 0S5

Numéro de catalogue :
PS4-245/2018F-PDF

Numéro international normalisé du livre (ISBN) :
978-0-660-27888-9

Publications connexes (numéro d'enregistrement : POR 130-16)

Numéro de catalogue PS4-245/2018E-PDF (Rapport final, anglais)
ISBN 978-0-660-27887-2

© Sa Majesté la Reine du chef du Canada, représentée par le ministre des Travaux publics et des Services gouvernementaux, 2018

LES ASSOCIÉS DE RECHERCHE EKOS

Contact : Susan Galley

Bureau d'Ottawa
359, rue Kent, bureau 300
Ottawa, Ontario
K2P 0R6
Tél. : (613) 235 7215
Télécopieur : (613) 235 8498
Courriel : pobox@ekos.com

www.ekos.com

TABLES DES MATIÈRES

Liste des tableaux vii
Liste des graphiques vii
Sommaire ix
1. Introduction 1
1.1 Contexte et objectifs de l'étude 1
1.1 Méthodologie 1
2. Utilisation d'appareils et d'Internet 7
2.1 Appareils dotés d'une connexion Internet utilisées 7
2.2 Endroits où accéder à Internet 9
2.3 Ampleur des activités en ligne 11
2.4 Activités en ligne 12
2.5 Moyens utilisés pour mener des transactions en ligne 14
2.6 Fréquence des activités en ligne risquées 16
2.7 Stockage d'information 18
3. Niveau de préoccupation et d'importance 19
3.1 Niveau de préoccupation – Menaces en ligne 19
3.2 Importance de se protéger contre les menaces en ligne 20
3.3 Omniprésence perçue des menaces en ligne 22
3.4 Probabilité perçue des menaces en ligne 23
3.5 Cryptomonnaie 24
4. Connaissance 27
4.1 Connaissance des menaces en ligne 27
4.2 Connaissance de mesures de précaution 29
4.3 Cerner les sites Web sûrs 32
5. Attitudes 35
5.1 Attitudes au sujet des menaces en ligne 35
6. Mesures de précaution 37
6.1 Fréquence déclarée des mesures de précaution 37
6.2 Types de mesures de précaution adoptées (protection des appareils) 38
6.3 Types de mesures de précaution prises (menaces en ligne) 40
6.4 Recours à un logiciel antivirus 41
6.5 Raisons de ne pas avoir de logiciel antivirus 44
6.6 Fréquence du changement des mots de passe en ligne 45
7. Fréquence à laquelle les gens sont des victimes 49
7.1 Fréquence et effets des attaques informatiques 49
7.2 Fréquence et conséquences des pertes financières 51
7.3 Fréquence et conséquences des vols d'identité 53
8. Information et responsabilités 59
8.1 Information recherchée 59
8.2 Attitudes – protection contre les risques en ligne 62
8.3 Organisations dignes de confiance pour l'obtention d'information 63

8.4 Organisations impartiales pour l'obtention de l'information 65
8.5 Comprendre les « Fausses nouvelles » 66
8.6 Responsabilité en ce qui concerne la sécurité des appareils 69
9. Préoccupations des parents 71
9.1 Préoccupations chez les parents 71
9.2 Raisons de ne pas être préoccupés 72
10. Expériences d'entreprises 75
10.1 Responsabilités du service des TI 75
10.2 Préoccupation par rapport aux interruptions 76
10.3 Mesures de protection contre les menaces en ligne 78
10.4 Renseignements utiles 81
11. Résultats des groupes de discussion 85
11.1 Connaissance d'enjeux de sécurité 85
11.2 Confiance dans la capacité de se protéger 85
11.3 Mesures prises pour atténuer les risques 86
11.4 À quel point la menace en ligne est-elle réelle? 87
11.5 Obstacles à la prise de mesures 88
11.6 Caractère adéquat de l'information 89
11.7 Fiabilité perçue de l'information 90
11.8 Responsabilité des partenaires 91
11.9 Rôle du gouvernement 92
11.10 Mise à l'essai du site Web 93
11.11 Infographie 97
11.12 Publication Facebook 100

ANNEXE A : Questionnaire du sondage
ANNEXE B : Scénario de recrutement pour les groupes de discussion
ANNEXE C : Guide du modérateur pour les groupes de discussion
ANNEXE D : Tableaux détaillés (sous pli séparé)

LISTE DES TABLEAUX

Tableau 1 : Tableau démographique
Tableau 2 : Fréquence du changement des mots de passe

LISTE DES GRAPHIQUES

Graphique 1 : Appareils servant à accéder à Internet
Graphique 2 : Endroits où accéder à Internet
Graphique 3 : Sécuriser le réseau sans fil ménager
Graphique 4 : Ampleur des activités en ligne
Graphique 5ab : Activités en ligne
Graphique 6 : Moyens utilisés pour mener des transactions en ligne
Graphique 7 : Fréquence des activités en ligne risquées
Graphique 8 : Stockage d'information
Graphique 9 : Niveau de préoccupation – Menaces en ligne
Graphique 10 : Importance de se protéger contre les menaces en ligne
Graphique 11 : Omniprésence perçue des menaces en ligne
Graphique 12 : Probabilité perçue des menaces en ligne
Graphique 13 : Raisons d'écarter la possibilité de menaces en ligne
Graphique 14 : Bonne connaissance des cryptomonnaies
Graphique 15 : Utilisation de cryptomonnaies
Graphique 16 : Connaissance des menaces en ligne
Graphique 17 : Connaissance des mesures de précaution
Graphique 18 : Appareils potentiellement en danger
Graphique 19 : Cerner les sites Web sûrs
Graphique 20 : Attitudes au sujet des menaces en ligne
Graphique 21 : Fréquence déclarée des mesures de précaution
Graphique 22 : Types de mesures de précaution adoptées (protection des appareils)
Graphique 23 : Types de mesures adoptées (menaces en ligne)
Graphique 24 : Recours à un logiciel antivirus
Graphique 25 : Choix du moment des mises à jour
Graphique 26ab : Raisons de ne pas avoir de logiciel antivirus
Graphique 27 : Pratiques sécuritaires

Graphique 28 : Probabilité de prendre des mesures contre les menaces en ligne par rapport aux menaces en personne
Graphique 29 : Fréquence des attaques informatiques
Graphique 30 : Incidence des attaques informatiques
Graphique 31 : Fréquence des pertes financières
Graphique 32 : Conséquences des pertes financières
Graphique 33 : Fréquence des vols d'identité
Graphique 34 : Conséquences des vols d'identité
Graphique 35 : Modifications de mots de passe – Médias sociaux
Graphique 36 : Modifications de mots de passe – Magasinage en ligne
Graphique 37 : Modifications de mots de passe – Courriels
Graphique 38 : Information recherchée
Graphique 39 : Sources d'information
Graphique 40 : Attitudes – Protection contre les menaces en ligne
Graphique 41 : Organisations dignes de confiance pour l'obtention d'information
Graphique 42 : Organisations impartiales pour l'obtention de l'information
Graphique 43 : Fausses nouvelles
Graphique 44 : Sources aidant à reconnaître une fausse nouvelle
Graphique 45 : Responsabilités en ce qui concerne la sécurité des appareils
Graphique 46 : Préoccupations chez les parents
Graphique 47 : Raisons de ne pas être préoccupés
Graphique 48 : Répondants du sondage
Graphique 49 : Niveau de préoccupation dans les entreprises
Graphique 50 : Raison de l'absence de préoccupation
Graphique 51 : Mesures prises par des entreprises
Graphique 52 ab : Instructions de sécurité précises à l'intention des employés
Graphique 53 ab : Renseignements requis

SOMMAIRE

L'utilisation de technologies faisant appel à Internet est très répandue à l'échelle du Canada. Sécurité publique Canada estime prioritaire d'informer la population d'enjeux liés à la sécurité et à la sûreté, et d'aider les Canadiens à se protéger contre les cybermenaces. Le sondage dont il est question dans le présent rapport a permis de réunir des données quantitatives au sujet des connaissances, des attitudes et des comportements de Canadiens qui utilisent Internet afin d'éclairer les futures initiatives d'élaboration de communications et de politiques. Les entrevues se sont déroulées auprès de 2 027 adultes canadiens de partout au pays qui utilisent Internet. Les cas étudiés proviennent d'une sélection effectuée au hasard parmi les membres du panel Prob*it*, un groupe de ménages canadiens recrutés aléatoirement au moyen de la méthode de composition aléatoire (CA) qui sert dans les démarches d'échantillonnage standard de sondages téléphoniques.

Une série de huit groupes de discussion a également eu lieu à l'échelle du pays afin de discuter de la connaissance des risques de sécurité en ligne, des types de mesures à prendre et des besoins en information.

Utilisation d'Internet

Les résultats du sondage confirment que les Canadiens recourent à divers appareils pour accéder tous les jours à Internet, non seulement les ordinateurs de bureau et les ordinateurs portables (93 p. cent), mais aussi les téléphones intelligents (76 p. cent), les tablettes et appareils de lecture (58 p. cent), les télévisions intelligentes (27 p. cent), les services de diffusion (25 p. cent), les consoles de jeux vidéos (21 p. cent) de même que d'autres appareils. Presque tout le monde y a accès à la maison et près de neuf répondants sur dix ont un réseau sans fil sécurisé à la maison. En moyenne, les Canadiens passent cinq heures par jour en ligne.

Les Canadiens utilisent Internet pour mener un large éventail d'activités, presque tout le monde y ayant recours pour consulter des courriers électroniques et pour naviguer dans des sites Web. Les Canadiens se servent aussi couramment d'Internet pour effectuer des transactions financières, pour suivre les actualités, pour visionner des vidéos et des films, pour faire des achats, pour recourir à des sites de réseautage comme Facebook ou Twitter, ou encore pour consulter des services d'information du gouvernement. Le courrier électronique constitue la source de risques la plus répandue, 98 pourcent des Canadiens s'adonnant à ce type d'activité en ligne.

Niveau de préoccupation et de connaissance

Les Canadiens qui utilisent activement Internet sont très préoccupés à la perspective que quelqu'un obtienne et utilise leurs renseignements personnels sans leur autorisation lors des activités qu'ils mènent en ligne. Dans les faits, la moitié des Canadiens se disent très préoccupés par les menaces en ligne, tandis qu'en grande partie, les autres se disent modérément préoccupés. Plus de huit Canadiens sur dix reconnaissent l'importance de prendre des mesures pour protéger leurs renseignements personnels en ligne et leurs ordinateurs personnels. Une proportion semblable souligne l'importance de protéger leurs appareils mobiles contre les menaces en ligne.

Les Canadiens estiment que les menaces en ligne sont assez courantes de nos jours. En effet, 43 pour cent des répondants sont d'avis qu'il est très courant pour les Canadiens d'être touchés par ces menaces, tandis que plus de quatre personnes sur dix indiquent que les menaces en ligne sont moyennement fréquentes. En ce qui concerne leur sécurité personnelle en ligne, le tiers des répondants sont d'avis qu'ils sont susceptibles de faire l'objet d'une menace en ligne dans un avenir rapproché et un tiers de plus estiment que cette probabilité est modérée.

En majorité, les Canadiens qui mènent des activités en ligne sont au courant des dangers auxquels ils s'exposent sur le Web. Dans une proportion semblable aux niveaux de connaissance enregistrés en 2016, neuf Canadiens sur dix sont au courant de l'existence de logiciels espions ou de logiciels malveillants sur les appareils informatiques, de la possibilité d'être victime d'escroquerie ou de fraude en ligne, et des vols d'identité. Huit répondants sur dix sont également au courant des violations en matière de protection de la vie privée et des pertes. Un plus grand nombre de Canadiens (trois sur quatre) savent maintenant que leurs renseignements personnels peuvent être retenus en échange d'une rançon (une augmentation de douze points par rapport à 2016). Ils sont aussi conscients qu'ils peuvent perdre des fichiers ou de l'information, ou que leurs données personnelles peuvent être effacées, modifiées ou perdues. La quasi-totalité des Canadiens affirme connaître les mesures de précaution à prendre pour se protéger en ligne, notamment en ne divulguant pas leurs mots de passe, en n'ouvrant pas les pièces jointes des messages électroniques provenant de quelqu'un qu'ils ne connaissent pas, en réduisant les renseignements personnels qu'ils partagent en ligne et en utilisant des logiciels antivirus ou anti-espion. Presque tous savent aussi que leur portable ou leur ordinateur peut faire l'objet d'une menace en ligne, tandis que huit sur dix savent que les menaces en ligne peuvent toucher aussi leur téléphone intelligent, leur tablette ou leur liseuse. Cette proportion est toutefois nettement à la baisse en ce qui concerne la connaissance des risques susceptibles de toucher les appareils domestiques à commande vocale, les télévisions intelligentes ou les dispositifs prêt-à-porter.

Les résultats suggèrent que le niveau de connaissances des Canadiens à l'égard des cryptomonnaies est plutôt limité et que leur utilisation est rare. Un peu moins de la moitié des Canadiens croit posséder à tout le moins des connaissances limitées sur ces monnaies alternatives. Parmi ceux qui les connaissent, seule une personne sur dix en a utilisé.

Ampleur des mesures de protection adoptées

La plupart des Canadiens affirment être aussi prudents ou même plus prudents quand vient le temps de se protéger contre les menaces en ligne que contre les menaces du monde réel. Ils nomment un vaste répertoire de mesures de précaution qu'ils adoptent pour protéger leurs appareils et leurs renseignements personnels en ligne, y compris au moins deux tiers des répondants qui téléchargent uniquement des fichiers de sources fiables, veillent à ce que leur logiciel antivirus soit à jour, verrouillent leurs appareils avec un mot de passe, protègent à l'aide d'un mot de passe leur réseau sans fil, et de façon générale, font preuve de prudence avec les sources inconnues.

Dans une proportion de neuf sur dix environ, les Canadiens disent éviter de partager leurs mots de passe, huit sur dix utilisant des mots de passe complexes ou faisant preuve de prudence lorsqu'ils communiquent de l'information comme leur vrai nom, leur adresse ou leur numéro de téléphone, ou lorsqu'ils donnent suite à des demandes de sources inconnues. Environ neuf répondants sur dix utilisent un logiciel antivirus sur leurs ordinateurs. Au nombre des autres mesures de précaution adoptées moins souvent figurent la modification des mots de passe par défaut, la consultation des politiques sur la protection de la vie privée, le recours à divers comptes de courriels au moyen d'un pseudonyme, la non-utilisation d'un compte d'administrateur pour accéder au Web et l'utilisation de logiciels de chiffrement. Il y a une augmentation considérable du nombre de gens qui disent utiliser l'authentification à deux étapes et la protection biométrique, proportion qui est passée d'un Canadien sur quatre en 2016 à un Canadien sur trois à l'heure actuelle.

Néanmoins, plusieurs comportements risqués sont très répandus. Près de la moitié des Canadiens disent utiliser le même mot de passe pour plusieurs comptes, alors que quatre personnes sur dix permettent à leurs navigateurs de conserver leurs mots de passe. En outre, entre trois et quatre Canadiens sur dix ne changent jamais leurs mots de passe ou attendent quelques années avant de le faire dans le cas des médias sociaux, des sites de magasinage et des comptes de messagerie. Les jeunes Canadiens (25 ans ou moins) sont plus enclins que les Canadiens plus âgés à modifier les mots de passe de leurs comptes de médias sociaux lorsqu'ils entendent parler d'une brèche de sécurité.

Même si un Canadien sur dix déclare avoir moins tendance à prendre des mesures de précaution contre les menaces en ligne que contre celles en personne, trois personnes sur dix sont plus susceptibles de faire preuve de prudence dans le monde numérique que dans le monde réel (alors que six répondants sur dix déclarent faire tout aussi attention).

Fréquence de la victimisation

La fréquence de la victimisation dans les attaques en ligne semble être à la hausse. Plus de la moitié des Canadiens (56 p. cent) font état d'un incident de virus, de logiciel malveillant ou de logiciel espion sur le ou les ordinateurs dont ils se servent pour accéder à Internet à des fins personnelles. Les résultats indiquent que ces attaques entraînent des conséquences au moins modérées pour plus de la moitié de personnes touchées. Le cinquième de ces personnes évoquent même un impact important. Entre cinq et douze pour cent des répondants ont subi un vol d'identité et des pertes financières à la suite d'activités menées en ligne.

Besoin d'information

Les Canadiens cherchent à obtenir une vaste gamme de renseignements au sujet des menaces en ligne, y compris des façons de protéger les appareils au moyen d'un logiciel antivirus (48 p. cent), les moyens de sécuriser les réseaux à la maison (38 p. cent) ou les moyens de reconnaître des escroqueries par courrier électronique (38 p. cent). Trois répondants sur dix recherchent de l'information sur la façon de protéger les fichiers de leurs appareils et ordinateurs (30 p. cent), alors que le quart recherche des renseignements sur le réseautage social sécuritaire. L'utilisation d'un réseau sans fil public, les conditions générales associées à la cybersécurité et la cyberintimidation sont également l'objet de recherches d'environ une personne sur six. La plupart des répondants cherchent à obtenir cette information avec un moteur de recherche (deux sur trois) ou sur le site Web d'un fournisseur (quatre sur dix). Environ le tiers du temps, ils consultent des sites Web de gouvernements, ou encore des amis ou des membres de leur famille. Les résultats donnent à penser que les répondants cherchent davantage à obtenir de l'information de façon proactive que pour régler un problème déjà survenu. Cette observation révèle une volonté de prendre des mesures pour faire des démarches, pour autant que l'information nécessaire soit disponible. Cela se confirme dans les groupes de discussion, où de nombreux participants disent s'intéresser à un site Web contenant d'une part des renseignements centralisés sur les risques de sécurité en général et sur les nouveaux risques, et d'autre part des comportements qui améliorent le niveau de protection.

Les deux tiers des Canadiens estiment qu'ils peuvent se protéger en ligne tant qu'ils disposent de renseignements de base dignes de confiance au sujet des mesures à prendre. Cette observation donne à penser que des renseignements concrets sont nécessaires, surtout pour les personnes moins renseignées ou moins confiantes. Six répondants sur dix estiment posséder assez

d'information sur les mesures à prendre pour se protéger contre les menaces en ligne. En revanche, le quart des Canadiens ne partage pas cet avis. De même, les avis des Canadiens sont partagés en ce qui concerne la question de savoir s'ils estiment disposer d'assez de renseignements pour savoir de quelle façon les nouvelles technologies sont susceptibles d'exercer une influence sur leur vie privée. En effet, la moitié des répondants sont d'accord avec cet énoncé, tandis que le tiers est en désaccord.

Les Canadiens sont perplexes en ce qui a trait au niveau de confiance qu'ils ressentent à l'égard de la fiabilité technique et de la neutralité des renseignements sur les menaces en ligne d'un éventail de sources. Environ la moitié des Canadiens se fie aux organismes d'application de la loi, aux gouvernements et aux entreprises de logiciels de sécurité. Ils sont un peu moins nombreux à estimer que les fournisseurs de services Internet sont dignes de confiance en ce qui concerne la communication de renseignements actuels et fiables sur des menaces en ligne. Lorsque nous les avons invités à indiquer la source qui leur inspire le plus confiance pour obtenir de l'information impartiale au sujet des menaces en ligne, le gouvernement et les organismes d'application de la loi figurent de nouveau en tête de liste, la moitié des répondants disant se fier à ces groupes. Les organismes sans but lucratif occupent le troisième rang, alors que les institutions financières, les amis et la famille, les fournisseurs privés et les entreprises de logiciels de sécurité ont chacun la confiance du quart des Canadiens.

La plupart des Canadiens croient qu'il est de la responsabilité des propriétaires d'appareils personnels ayant accès à Internet de veiller à ce qu'ils soient sécurisés et sécuritaires. Encore une fois, cette observation donne à penser que les Canadiens sont disposés à passer à l'action, pour autant qu'ils reçoivent l'information dont ils ont besoin.

Les Canadiens ont diverses interprétations lorsque vient le temps de décrire ce qu'est une « fausse nouvelle ». Environ quatre personnes sur dix les interprètent comme des renseignements qui sont utilisés à tort pour façonner des opinions ou des faits, tandis que trois sur dix croient qu'il s'agit d'information issue d'une source partiale. Il n'y a pas de consensus en ce qui concerne la responsabilité d'aider les Canadiens à reconnaître les fausses nouvelles, bien qu'une majorité relative croie que le gouvernement devrait jouer un rôle prépondérant.

Préoccupations chez les parents

Les résultats donnent à penser que même si de nombreux parents estiment posséder l'information dont ils ont besoin pour protéger leurs enfants en ligne, une minorité considérable ne croit pas que c'est le cas. Par exemple, tandis que plus de la moitié des personnes interrogées estiment posséder l'information nécessaire pour aider leur enfant à naviguer en ligne, le quart d'entre elles ne partagent pas cet avis. Quatre répondants sur dix sont aussi d'accord pour dire qu'ils ne parviennent pas à suivre l'évolution des jeux, des applications et des autres technologies que les

jeunes utilisent. La moitié environ affirme se préoccuper de questions entourant la protection des renseignements personnels de leurs enfants, de même que des risques de cyberintimidation et de harcèlement en ligne. Dans de moindres proportions (entre deux et quatre sur dix), les gens se préoccupent des implications juridiques du partage d'images et de fichiers. Les parents qui ne sont pas préoccupés par l'exposition de leurs enfants à ces menaces affirment avoir déjà abordé ces questions avec leurs enfants, disent que leurs enfants ne sont pas souvent en ligne (plus fréquents chez les parents de jeunes enfants), croient que leurs enfants reçoivent suffisamment d'information à l'école ou se fient à leurs enfants pour agir de façon appropriée.

Préoccupations dans les entreprises

Même si l'étude s'inspire d'un sondage réalisé auprès de la population en général, nous en avons profité pour interroger les personnes qui sont des travailleurs autonomes ou des dirigeants dans une PME (moins de 250 employés) au sujet des pratiques de leur entreprise en matière de TI et de leurs niveaux de préoccupation relativement à des questions de protection en ligne. Au total, 533 entreprises sont représentées. Bien que le quart de ces répondants se dise très préoccupé, la moitié d'entre eux est moyennement préoccupée et le cinquième affirme ne pas être préoccupé du tout par les possibilités d'interruptions de travail ou de pertes financières découlant de menaces en ligne. Au nombre des personnes non préoccupées, cette attitude tient habituellement au fait qu'elles estiment que le risque est très faible ou qu'elles ont fait des recherches et pris de mesures pour protéger leur entreprise.

Les résultats révèlent qu'il y a autant matière à amélioration dans le domaine de la protection contre les menaces en ligne dans les entreprises que chez les membres de la population, dans l'espace personnel. Entre cinq et sept employeurs sur dix exigent de leurs employés qu'ils protègent leurs appareils avec un mot de passe, qu'ils actualisent leur logiciel de sécurité, qu'ils utilisent un protocole d'identification de mot de passe, qu'ils fassent des copies de sécurité de leurs renseignements et qu'ils installent des filtres antipourriel. Dans la moitié des cas environ, les employés doivent télécharger du contenu provenant seulement de sources fiables, utiliser des mots de passe complexes et faire preuve de prudence lorsqu'ils cliquent sur une pièce jointe ou répondent à une invitation par courriel. Une moindre proportion d'employeurs demande à leurs employés de ne pas partager leurs mots de passe, de faire preuve de prudence lorsqu'ils répondent à des sollicitations d'étrangers et de changer les mots de passe par défaut. Les résultats révèlent aussi que les organisations sont avides de recevoir de plus amples renseignements au sujet d'une vaste gamme de sujets en vue de mieux cerner et gérer les risques associés aux menaces en ligne. Quatre répondants sur dix disent s'intéresser au fait de posséder une liste de menaces à rechercher, aux procédures à suivre pour réagir à une cyberattaque, aux mesures à prendre pour protéger les appareils mobiles dans un lieu public, aux pratiques exemplaires de stockage de données, aux directives relatives à l'utilisation d'appareils personnels

au travail, et aux directives d'élaboration de règlements et de politiques d'utilisation sécuritaire des courriels.

Segments de la population

Un certain nombre de tendances récurrentes se dégagent des résultats du sondage. Les Canadiens plus jeunes sont plus actifs en ligne et ont tendance à mieux connaître les enjeux relatifs aux menaces et à la sécurité en ligne. Les Canadiens plus âgés sont moins actifs en ligne, mais plus préoccupés par la sécurité. Ils sont habituellement plus disposés à rechercher des renseignements et des conseils au sujet de la façon de se protéger en ligne. Habituellement, le fossé générationnel apparaît chez les plus jeunes membres de la génération des baby-boomers (il y a de grandes différences dans les résultats entre les moins de 55 ans et les 45 ans et plus). La situation socioéconomique permet aussi d'établir une importante démarcation. En effet, les personnes dont le niveau de scolarité est supérieur font souvent état d'un plus grand nombre d'activités en ligne ou de connaissances sur ces enjeux. Les résidents du Québec, qui font état de moindres niveaux de connaissances au sujet des menaces en ligne et de la sécurité, et de moindres préoccupations au sujet des menaces possibles, affirment aussi adopter un moins grand nombre de mesures de protection.

La valeur totale du projet de sondage d'opinion publique est de 122 983,55 dollars (TVH incluse).

Nom du fournisseur : Les Associés de recherche EKOS
No de contrat – TPSGC : OD160192340/001/CY
Date d'attribution du contrat : 13 août 2018
Pour obtenir de plus amples renseignements sur cette étude, veuillez envoyer un courriel à ps.communications-communications.sp@canada.ca.

CERTIFICATION DE NEUTRALITÉ POLITIQUE

La présente certification s'appliquera au rapport définitif envoyé au chargé de projet.

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

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

Signé par :

Susan Galley (vice-présidente)

1. INTRODUCTION

1.1 CONTEXTE ET OBJECTIFS DE L'ÉTUDE

En leur qualité de plus grands utilisateurs d'Internet au monde, il importe que les Canadiens comprennent bien les enjeux de cybersécurité et qu'ils s'engagent pleinement dans un processus à cet égard, ce qui englobe d'une part la capacité à reconnaître les menaces en ligne, les mesures à prendre pour combattre ces risques et les sources d'informations fiables sur les façons de naviguer en toute sécurité, et d'autre part un engagement à adopter des mesures de protection de l'identité et de protection des appareils permettant d'accéder à Internet. Voilà pourquoi la Stratégie de cybersécurité du Canada évalue les connaissances et l'engagement de la population en matière de cybersécurité, de même que la mise en œuvre de la campagne de sensibilisation Pensez cybersécurité, dont l'objectif est de favoriser les connaissances générales et la compréhension de la population dans ce domaine.

Les objectifs de la recherche sont les suivants :

- Évaluer le rendement de la campagne de sensibilisation du public et contribuer à l'identification des changements dans les connaissances, les comportements et les attitudes.
- Assurer le suivi du ou des publics cibles particuliers que doit viser la campagne de sensibilisation.
- Cerner les facteurs de motivation et les obstacles au changement des comportements (pour les gens qui ont pris des mesures, ce qui les a poussés à agir; pour ceux qui ne l'ont pas fait, pourquoi pas?) et en assurer le suivi.
- Cerner les meilleures façons de communiquer ces renseignements et en assurer le suivi.
- Assurer le suivi des attentes du public en ce qui a trait à la participation des gouvernements provinciaux et fédéral, d'administrations municipales, et d'organismes non gouvernementaux.

1.1 MÉTHODOLOGIE

a) Sondage

L'échantillon se compose de 2 072 entretiens réalisés avec des Canadiens âgés de 18 ans ou plus qui utilisent régulièrement Internet, y compris plus de 300 entrevues avec des jeunes âgés de 16 à 24 ans, et 300 Canadiens qui occupent un poste de direction dans une PME comptant entre un et cent employés. Dans un premier temps, l'échantillon réunissait une sélection

aléatoire de membres du panel Prob*it* de partout au pays. Les panellistes de Prob*it* ont été sélectionnés pour former une base de sondage hybride recruté sur des téléphones cellulaires et des lignes terrestres à l'aide d'un système à composition aléatoire. Il s'agit de la même base de sondage et du même processus d'échantillonnage utilisés pour mener des enquêtes au téléphone, considérés comme représentatifs de la population. Une fois sélectionnées, nous avons communiqué avec eux par téléphone et les avons recrutés en leur demandant de créer un profil de base (c.-à-d. en répondant au questionnaire de base du sondage), qui comprenait un éventail de renseignements démographiques les décrivant. Nous leur demandions également s'ils souhaitaient répondre au sondage au téléphone ou en ligne. Tous les membres de l'échantillon étaient admissibles à une participation, y compris ceux qui ne possèdent qu'un téléphone cellulaire, ceux qui n'ont pas accès à Internet et ceux qui préféraient simplement répondre au téléphone plutôt qu'en ligne. Ce panel se compose d'un échantillon totalement représentatif de la population canadienne à partir duquel il est possible de sélectionner des échantillons aléatoires et de recueillir des données d'une façon plus délibérée et en temps plus opportun que ce qui serait possible dans un sondage téléphonique traditionnel. Ce panel de plus de 95 000 membres peut être tenu comme représentatif de la population canadienne (c'est-à-dire qu'une population cible donnée comprise dans notre panel correspond de très près à l'ensemble de la population), et il est donc possible de lui attribuer une marge d'erreur.

En particulier, dans le cadre du sondage, un échantillon de 16 178 personnes a été créé à partir du volet en ligne seulement du panel Prob*it,* en vue de la réalisation des sondages en ligne seulement, étant donné qu'il s'agissait de la portion précise de la population canadienne qui était ciblée par la campagne de communications. Le taux de participation s'est établi à 15 pour cent[1]. L'échantillon du sondage final, en vertu duquel 2 072 sondages ont été achevés, présente un niveau de précision de +/- 2,2 pour cent pour l'échantillon dans son ensemble et de +/- 3 à 6 pour cent pour la plupart des sous-groupes pouvant être isolés dans l'analyse (y compris l'ensemble des régions, des groupes d'âge, des niveaux de scolarité et des niveaux de revenu).

Le prétest a mené à 16 entretiens en anglais et à 10 en français. Des questions supplémentaires ont été intégrées à la version du prétest du questionnaire pour recueillir les impressions des répondants sur la durée, le rythme, la clarté des libellés et d'autres aspects. Des changements mineurs ont été apportés à la suite des essais, bien que quelques questions aient été enlevées pour réduire la durée du sondage.

Le sondage, qui s'est déroulé entre le 21 août et le 5 septembre 2018, faisait appel à un questionnaire bilingue hébergé sur un serveur Web sécurisé sous le contrôle des Associés de recherche EKOS. Le courriel d'invitation comprenait une description et une explication de l'objectif

[1] Parmi l'échantillon de 16 178 cas, 596 se sont avérés non distribuables (échantillon valide de 15 582 cas) et 260 cas ont été supprimés parce qu'ils étaient considérés comme hors du domaine.

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

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

Le tableau suivant présente le profil de l'échantillon. Le tableau comprend la distribution non pondérée de caractéristiques démographiques liées à la région, au genre et à l'âge (utilisées dans la pondération des données), ainsi que la distribution pondérée relativement à la présence d'enfants à la maison, à l'âge des enfants, au fait que les répondants soient nés ou non au Canada, à la composition actuelle des ménages, au niveau de scolarité, au revenu annuel du ménage et à la langue maternelle.

Tableau 1 : Tableau démographique

Tableau 1a : Province/Territoire (non pondérés)

---	Total
n=	*2072*
Colombie-Britannique et Yukon	13 %
Alberta et Territoires-du-Nord-Ouest	10 %
Saskatchewan et Manitoba	6 %
Ontario	33 %
Québec et Nunavut	23 %
Atlantique	10 %

Tableau 1b : Sexe (non pondéré)

---	Total
Homme	48 %
Femme	52 %

Tableau 1c : Âge (non pondéré)

---	Total
16-24	15 %
25-34	11 %
35-44	17 %
45-54	20 %
55-64	20 %
65 et +	15 %

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

---	Total
n=	*2072*
Oui	26 %
Non	74 %
Je préfère ne pas répondre	0 %

Tableau 1e : Âge des enfants à la maison

---	Total
n=	*2072*
Moins de 6 ans	22 %
6 à 11	23 %
11 à 15	27 %
16 ans ou plus	17 %
Je préfère ne pas répondre	11 %

Tableau 1f : Né(e) au Canada

---	Total
n=	2072
Oui	86 %
Non	13 %
Je préfère ne pas répondre	1 %

Tableau 1g : Niveau de scolarité atteint

---	Total
n=	2072
École secondaire ou moins	12 %
Un peu d'études postsecondaires	12 %
Certificat ou diplôme d'un établissement collégial ou d'une école de métiers	27 %
Diplôme d'études de premier cycle	29 %
Diplôme d'études supérieures ou professionnel	19 %
Je préfère ne pas répondre	1 %

Tableau 1h : Revenu annuel du ménage

---	Total
n=	2072
Moins de 20 000 $	6 %
Entre 20 000 $ et 39 999 $	11 %
Entre 40 000 $ et 59 999 $	14 %
Entre 60 000 $ et 79 999 $	13 %
Entre 80 000 $ et 99 999 $	13 %
Entre 100 000 $ et 149 999 $	17 %
150 000 $ ou plus.	12 %
Je ne sais pas/Pas de réponse	14 %

Table 1i : Langue maternelle

---	Total
n=	2072
Anglais	73 %
Français	20 %
Autre	7 %
Je préfère ne pas répondre	1 %

La comparaison de chaque échantillon non pondéré avec les données du recensement de 2016 de Statistique Canada laisse entrevoir des sources semblables de biais systématique dans chaque sondage, conformément au modèle qui se dégage de la plupart des sondages à l'intention du grand public. Les membres des échantillons des sondages sont un peu plus scolarisés que ce que l'on retrouve dans l'ensemble de la population puisque 48 pour cent disent avoir un diplôme universitaire contre 25 pour cent dans la population générale. Les ménages comprenant des enfants de moins de 18 ans sont également sous-représentés dans chaque échantillon (26 p. cent, comparativement à 35 p. cent dans la population). Les Canadiens

nés à l'extérieur du pays sont également sous-représentés dans chaque sondage (13 p. cent dans l'étude préliminaire et dans le sondage de post-campagne, par rapport à 27 p. cent dans la population). Comme décrit précédemment, chaque échantillon a été pondéré en fonction de l'âge, du sexe et de la région.

b) Groupes de discussion

Pour mieux saisir le contexte et mieux comprendre les résultats du sondage et recueillir des réactions par rapport au site Web PensezCybersecurite, huit groupes de discussion ont été tenus dans quatre villes canadiennes, soit Montréal (2), Toronto (2), Calgary (2) et Halifax (2). Dans chaque ville, une séance a réuni des membres du grand public issus de tous les groupes d'âge. À Montréal et à Toronto, la deuxième séance rassemblait des gens âgés de moins de 30 ans. À Calgary et à Halifax, elle regroupait des propriétaires ou des employés de petites et moyennes entreprises (c.-à-d., des organisations comptant moins de cent employés). Les deux groupes de Montréal ont eu lieu en français. Tous les autres groupes se tenaient en anglais. Un questionnaire de recrutement est disponible à l'annexe A. Des groupes ont été stratifiés pour assurer un équilibre hommes-femmes, et une diversité entre les divers groupes d'âge. En tout, 67 personnes ont pris part aux discussions. En consultation avec le client, EKOS a mis au point un scénario de recrutement pour les groupes de discussion (adjoint à l'annexe B). Les discussions traitaient du niveau de connaissance, des préoccupations et des mesures prises pour atténuer les risques que présentent les menaces en ligne, ainsi que des sources d'information utilisées, et du besoin d'information à ce sujet. Des réactions ont également été recueillies par rapport à la page d'accueil du site Web, à une annonce infographique et à une annonce sur Facebook.

Tous les groupes de discussions duraient 90 minutes. Les discussions avaient lieu dans des installations professionnelles de groupes de discussion. Des rafraîchissements étaient fournis et les participants recevaient 85 dollars en contrepartie de leur participation. Les enregistrements vidéo ou audio, les notes des enquêteurs et les observations tirées sont à la base de l'analyse et du rapport sur les résultats.

Lors de la lecture du présent rapport, il ne faut pas perdre de vue que les constatations issues des groupes de discussion sont de nature qualitative et qu'elles sont davantage conçues pour fournir un contexte élargi que pour mesurer des pourcentages de la population cible. Ces résultats ne sont pas conçus pour estimer la proportion numérique ou le nombre de personnes de la population qui a une opinion particulière, car ils ne sont pas prévisibles statistiquement parlant.

2. Utilisation d'appareils et d'Internet

La présente section établit les niveaux d'utilisation et de sophistication des Canadiens lorsqu'ils sont en ligne. Elle examine également leur utilisation de l'ordinateur et d'autres appareils permettant d'accéder à Internet, la fréquence de leur utilisation et leurs compétences avec les ordinateurs et d'autres technologies, de même que leur niveau d'activités en ligne. Les Canadiens, très actifs en ligne, utilisent un éventail de plus en plus vaste d'appareils et, en général, un haut niveau de sophistication technologique.

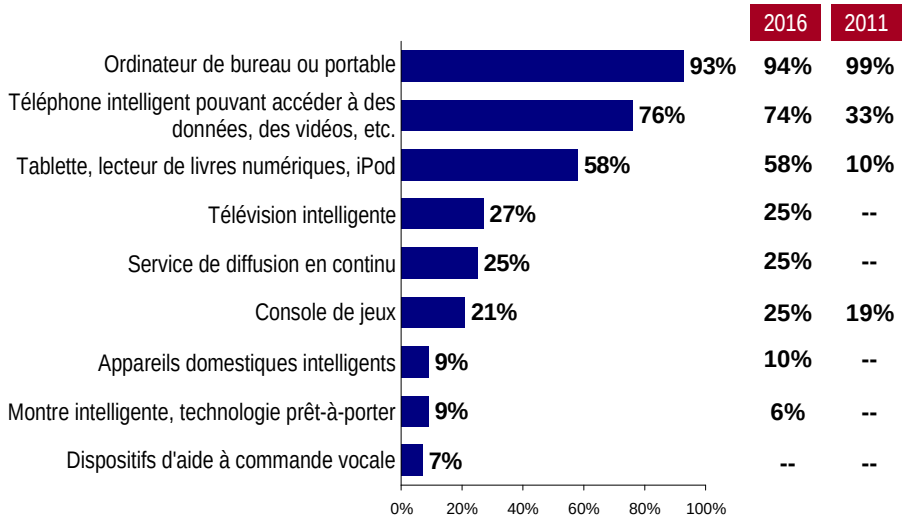
2.1 Appareils dotés d'une connexion Internet utilisées

En harmonie avec les résultats de 2016, presque tous les Canadiens (93 p. cent) qui sont en ligne utilisent des ordinateurs portables et de bureau pour accéder à Internet à des fins personnelles. Les trois quarts de ces Canadiens (76 p. cent) ont recours à un téléphone intelligent capable d'accéder à des données. Ce résultat correspond à celui obtenu en 2016, mais témoigne d'une forte augmentation depuis 2011, alors que le tiers (33 p. cent) des répondants affirmait utiliser un téléphone intelligent, comme un iPhone ou un BlackBerry, pour accéder à Internet à des fins personnelles[2]. Plus de la moitié des Canadiens (58 p. cent) utilise des tablettes (y compris des iPod et des liseuses) pour accéder à Internet (en harmonie avec les résultats de 2016, mais à la hausse de plus de cinq points par rapport à 2011). Le quart a recours à une télévision intelligente (27 p. cent), à un service de diffusion en continu (25 p. cent), à une console de jeux vidéos, comme PlayStation de Sony ou Xbox de Microsoft (21 p. cent, une légère baisse par rapport aux 25 p. cent de 2011). Un répondant sur dix utilise un appareil domestique intelligent (9 p. cent) ou a recours à une montre intelligente ou à une autre technologie prêt-à-porter (9 p. cent). Sept pour cent utilisent des appareils à reconnaissance vocale.

[2] Dix pour cent de plus affirmaient recourir à un téléphone cellulaire assorti d'un accès Internet de base en 2011. Cette catégorie n'était pas offerte en 2016.

Graphique 1 : Appareils servant à accéder à Internet

« De quels appareils vous servez-vous pour accéder à internet à des fins personnelles? »



Les Associés de recherche EKOS

n=2072

Sondage de SP sur la cybersécurité, 2018

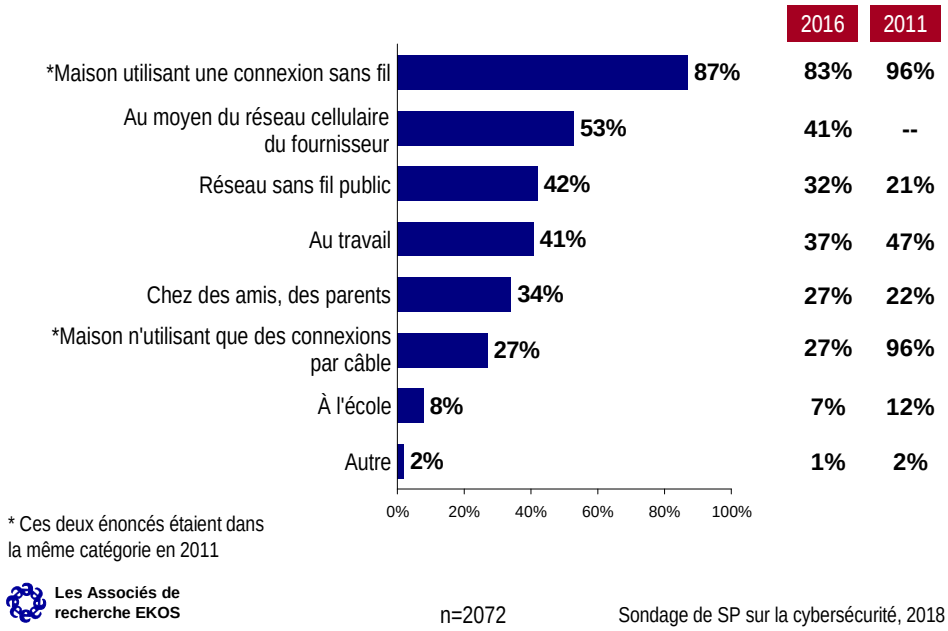
- Les répondants âgés de moins de 25 ans sont moins enclins que ceux des autres groupes d'âge à utiliser des ordinateurs de bureau ou des portables, des tablettes, des liseuses ou des iPod. Les Canadiens plus jeunes (55 ans ou moins) sont plus susceptibles d'utiliser des téléphones intelligents et des consoles de jeux vidéos pour accéder à Internet. Les Canadiens âgés de 25 à 44 ans sont plus enclins que ceux des autres groupes d'âge à utiliser des services de diffusion en continu tandis que ceux âgés de 35 à 44 ans ont plus tendance à avoir recours à des télévisions intelligentes.
- Les répondants de la Colombie-Britannique et des Prairies sont plus enclins que les Canadiens des autres régions à utiliser les téléphones intelligents pour accéder à Internet à des fins personnelles. Les résidents du Québec sont moins enclins à utiliser une télévision intelligente, un service de diffusion en continu ou une console de jeux vidéo.
- Les hommes ont plus tendance que les femmes à mentionner l'utilisation d'une télévision intelligente, d'un service de diffusion en continu et d'une console de jeux vidéo.
- Les répondants ayant fait des études universitaires et les répondants ayant un revenu plus élevé sont généralement plus susceptibles de recourir à tous les appareils.

2.2 ENDROITS OÙ ACCÉDER À INTERNET

La vaste majorité des ménages de l'échantillon qui ont Internet à la maison utilise un réseau sans fil (87 p. cent, une légère hausse par rapport aux 83 p. cent de 2016), alors que le quart (27 p. cent) a recours à une connexion par câble seulement (la même proportion qu'en 2016). Les Canadiens accèdent à Internet par le biais d'autres moyens, notamment par le biais de leur réseau cellulaire (53 p. cent, en hausse par rapport à 41 p. cent), de réseaux sans fil publics (42 p. cent, en hausse par rapport à 32 p. cent) ou du réseau de leur travail (41 p. cent, en légère hausse par rapport à 37 p. cent). Le tiers (34 p. cent, une hausse par rapport à 27 p. cent) des répondants accèdent à Internet chez des amis ou des parents. Une personne sur dix (8 pour cent) affirme accéder à Internet à l'école, mais cette proportion gonfle à 54 pour cent chez les répondants de moins de 25 ans (par rapport à 39 p. cent en 2016).

Graphique 2 : Endroits où accéder à Internet

« Où accédez-vous normalement à internet? »

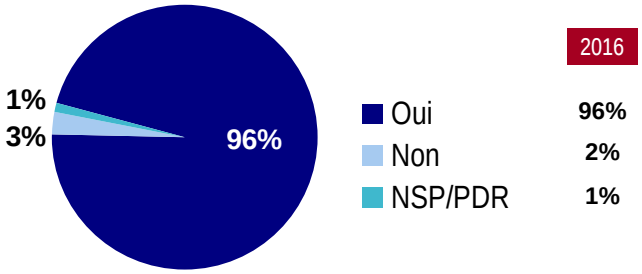


- Les Canadiens âgés (65 ans ou plus) sont plus susceptibles que les Canadiens plus jeunes d'accéder principalement à Internet à la maison au moyen d'une connexion par câble seulement. Ceux âgés de 25 à 54 ans ont plus tendance à accéder à Internet à la maison ou au travail à l'aide d'un réseau sans fil. Les moins de 45 ans sont plus susceptibles d'utiliser le réseau cellulaire de leur fournisseur, un réseau sans fil public ou la connexion d'un ami ou d'un membre de leur famille.
- Les hommes sont plus susceptibles que les femmes d'accéder à Internet à la maison au moyen d'une connexion sans fil, du réseau de leur lieu de travail ou de leur réseau cellulaire.
- Les Canadiens faisant état de plus hauts niveaux de scolarité et de revenu sont plus enclins à accéder à Internet à la maison au moyen d'une connexion sans fil, d'accéder à Internet au travail ou de recourir au réseau cellulaire de leur fournisseur.

Les Canadiens semblent prendre des mesures de précaution pour protéger le réseau sans fil de leur maison. Parmi les Canadiens qui ont un réseau sans fil à la maison, la quasi-totalité (96 p. cent) sécurise son réseau avec un mot de passe, comparativement à seulement trois pour cent qui ne le font pas. Ces résultats sont en harmonie avec ceux de 2016.

Graphique 3 : Sécuriser le réseau sans fil ménager

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



Les Associés de recherche EKOS n=1801 Sondage de SP sur la cybersécurité, 2018

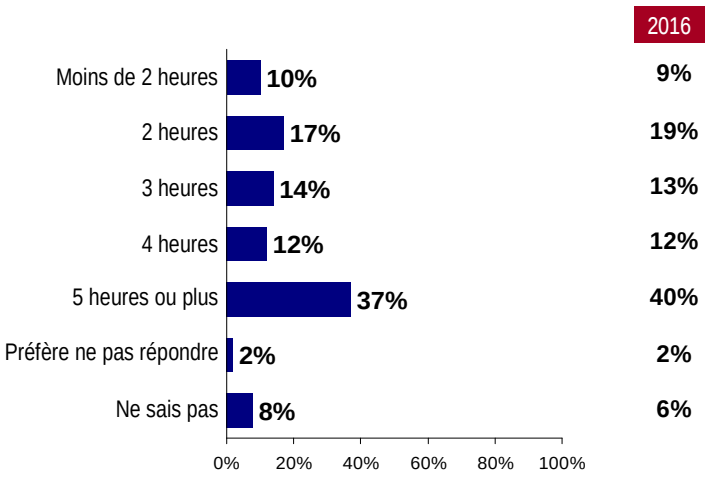
- Les répondants âgés de plus de 65 ans sont un peu moins enclins à recourir à un mot de passe (sept pour cent n'en utilisent pas).

2.3 AMPLEUR DES ACTIVITÉS EN LIGNE

En moyenne, les Canadiens passent 4,9 heures par jour en ligne. Environ deux personnes sur cinq (37 p. cent) affirment passer au moins cinq heures en ligne tous les jours. Le dixième des Canadiens seulement (10 p. cent) passent moins de deux heures en ligne tous les jours. Un répondant sur six (17 p. cent) passe deux heures par jour en ligne, 14 pour cent passent trois heures par jour en ligne et 12 pour cent passent quatre heures par jour en ligne.

Graphique 4 : Ampleur des activités en ligne

« Combien d'heures par jour passez-vous en ligne? »



Les Associés de recherche EKOS

n=2072

Sondage de SP sur la cybersécurité, 2018

- Les Canadiens plus jeunes passent beaucoup plus de temps en ligne que les Canadiens plus âgés. Les Canadiens de moins de 25 ans passent en moyenne 7,2 heures en ligne tous les jours et ceux qui ont 25 à 34 ans passent en moyenne 6,5 heures en ligne. Les Canadiens de 55 à 64 ans passent 4,1 heures en ligne, tandis que les personnes âgées de 65 ans et plus passent un peu moins de temps en ligne, soit 3,3 heures en moyenne tous les jours.

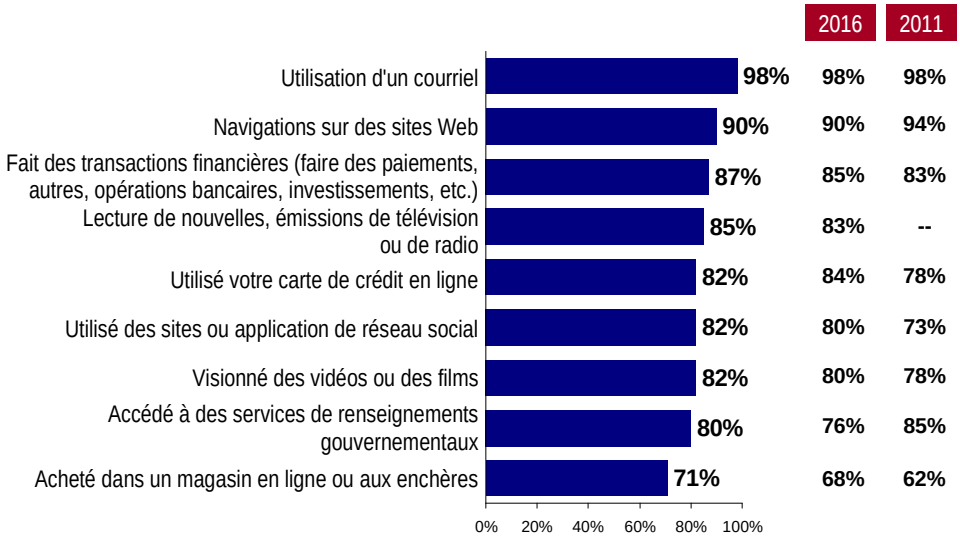
2.4 ACTIVITÉS EN LIGNE

Bien que les moyens d'accéder à Internet aient quelque peu changé au cours des deux dernières années, les activités en ligne demeurent relativement les mêmes. Les Canadiens recourent à Internet pour faire un vaste éventail d'activités, signalant cinq ou six activités principales. Les courriers électroniques constituent l'activité la plus courante chez les Canadiens, qui soutiennent à 98 pour cent utiliser Internet pour se servir de la messagerie électronique. Neuf personnes sur dix (90 p. cent) signalent naviguer dans des sites Web ou fureter sur Internet en général. Plus de huit Canadiens sur dix font des transactions financières (87 p. cent), prennent connaissance de nouvelles, visionnent du contenu télé ou écoutent la radio (85 p. cent), utilisent une carte de crédit en ligne (82 p. cent), accèdent à des médias sociaux (82 p. cent) ou regardent des vidéos ou des films (82 p. cent). Huit Canadiens sur dix (80 p. cent) consultent des renseignements sur des services gouvernementaux (une légère hausse par rapport aux 76 p. cent de 2016), alors que sept répondants sur dix (71 p. cent) font du magasinage en ligne.

Six Canadiens sur dix téléchargent des logiciels (62 p. cent), téléchargent ou écoutent en continu de la musique ou des fichiers balados (61 p. cent, une hausse de dix points en comparaison avec 2016) ou font des appels téléphoniques ou vidéos (58 p. cent). Environ la moitié des répondants joue à des jeux en ligne (51 p. cent) ou participe à des concours en ligne (47 p. cent). Quelque quatre personnes sur dix envoient des demandes d'emploi (40 p. cent), participent à des blogues ou à des discussions en ligne (38 p. cent), achètent des cours de formation en ligne (36 p. cent) ou utilisent des services offerts par le biais d'applications (35 p. cent, une hausse par rapport aux 27 p. cent de 2016).

Graphique 5a : Activités en ligne

« Lesquelles des activités suivantes avez-vous faites sur internet dans la dernière année? »

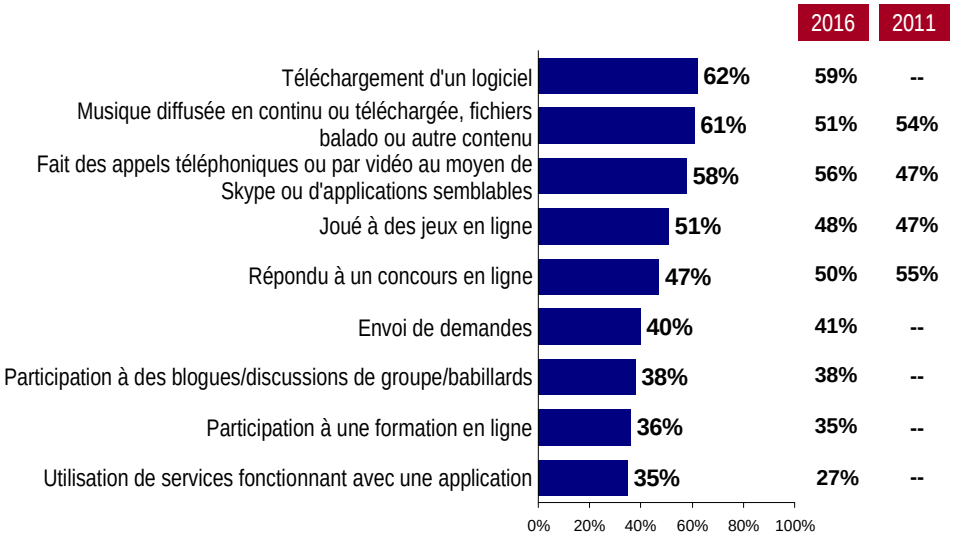


Les Associés de recherche EKOS

Sondage de SP sur la cybersécurité, 2018

Graphique 5b : Activités en ligne

« Lesquelles des activités suivantes avez-vous faites sur internet dans la dernière année? »



Les Associés de recherche EKOS

n=2072

Sondage de SP sur la cybersécurité, 2018

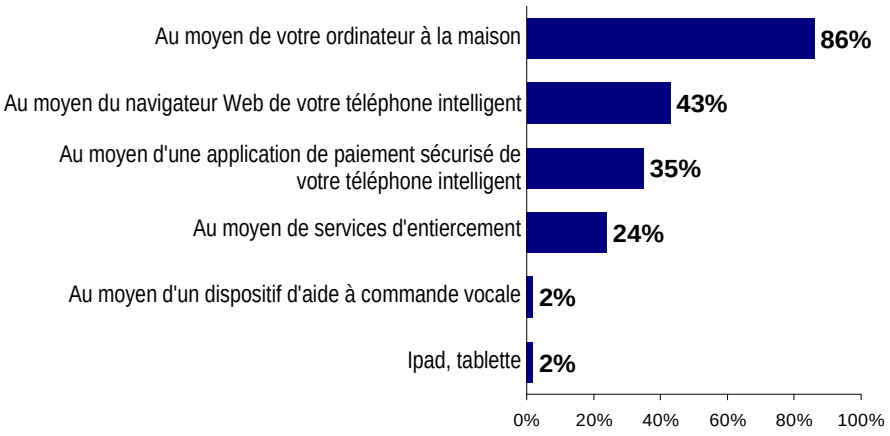
- Un net fossé générationnel divise les personnes plus susceptibles d'utiliser Internet pour mener ces activités et celles qui ne le sont pas. Les Canadiens de 55 ans ou plus sont les moins susceptibles d'utiliser Internet pour mener la plupart de ces activités, exception faite du courrier électronique. Pour la plupart des activités, l'utilisation d'Internet est plus répandue chez les Canadiens de 55 ans ou moins. Ceux âgés de 25 ans ou moins sont moins enclins à utiliser Internet à des fins commerciales (transactions bancaires, utilisation d'une carte de crédit, magasinage), pour naviguer sur des sites Web, pour accéder à des services gouvernementaux, pour lire les nouvelles, regarder la télévision et pour écouter la radio.
- Les hommes montrent une plus forte propension à faire du magasinage en ligne, à visionner des vidéos, à télécharger des logiciels, à télécharger ou à écouter de la musique en continu, à utiliser des services par le biais d'applications, à participer à des discussions ou à suivre des cours. Les femmes sont légèrement plus enclines à utiliser des sites de médias sociaux.
- Les personnes dont les niveaux de revenu et de scolarité sont plus élevés sont plus susceptibles d'utiliser Internet pour mener la plupart de ces activités, exception faite du courrier électronique, des jeux en ligne et des concours en ligne.
- Les résidents du Québec ont plus tendance à participer à des concours en ligne, mais sont moins susceptibles de faire la plupart des autres activités testées, à l'exception du courrier électronique, des transactions financières, des médias sociaux, des jeux en ligne et de l'envoi de demande d'emploi.

2.5 MOYENS UTILISÉS POUR MENER DES TRANSACTIONS EN LIGNE

Nous avons demandé aux répondants qui disent avoir effectué des transactions financières en ligne au cours de la dernière année de nommer les moyens qu'ils utilisent. La vaste majorité d'entre eux (86 p. cent) effectuent ces transactions à partir d'un ordinateur à la maison. Environ quatre répondants sur dix utilisent leur téléphone intelligent, soit par le biais d'un navigateur (43 p. cent) soit à l'aide d'une application de paiements sécurisés (35 p. cent). Le quart (24 p. cent) se fie à des services entiercés comme PayPal. Quelques-uns ont également recours à des appareils à reconnaissance vocale (2 p. cent) ou à un iPad ou tablette (2 p. cent).

Graphique 6 : Moyens utilisés pour mener des transactions en ligne

« Comment procédez-vous habituellement pour faire ces transactions? »



Les Associés de recherche EKOS

n=1775; procèdent à des transactions financières

Sondage de SP sur la cybersécurité, 2018

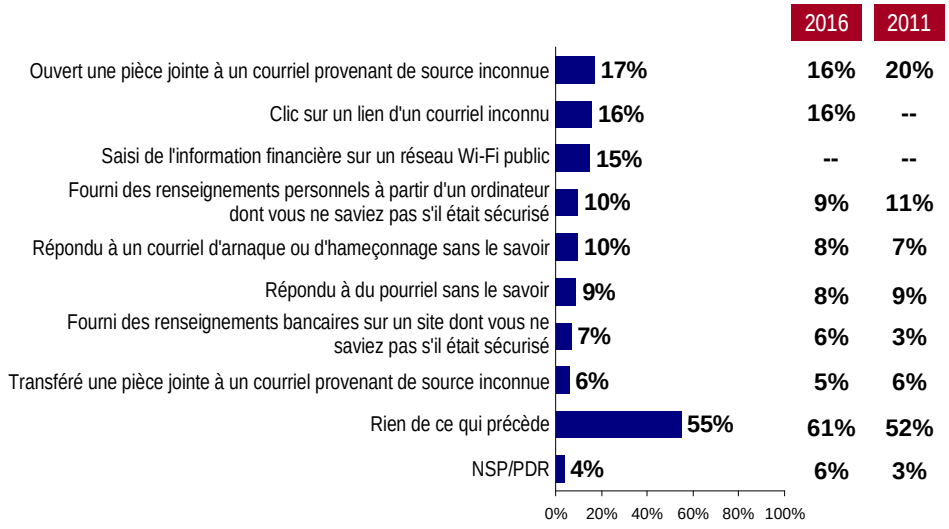
- Les Canadiens âgés de 65 ans et plus sont plus susceptibles d'effectuer leurs transactions à partir d'un ordinateur à la maison. Ceux âgés de moins de 45 ans ont beaucoup plus tendance à recourir aux téléphones intelligents et aux services entiercés.
- Les hommes sont un peu plus enclins à utiliser chacun des moyens testés.
- Les gens qui ont fait des études universitaires ont un peu plus tendance à utiliser un ordinateur à la maison ou une application sécurisée sur un téléphone intelligent, alors que ceux qui ont un diplôme d'études secondaires sont visiblement moins enclins à utiliser un téléphone intelligent, tout le contraire des gens qui ont un revenu plus élevé.

2.6 FRÉQUENCE DES ACTIVITÉS EN LIGNE RISQUÉES

Les résultats donnent à penser qu'une minorité considérable de Canadiens adoptent des comportements risqués en ligne. Un peu plus de la moitié (55 p. cent) déclare n'avoir fait aucune des activités à risque cernées, une légère baisse par rapport aux 61 pour cent de 2016. Un Canadien sur six a ouvert la pièce jointe d'un courriel provenant d'une source inconnue (17 p. cent), a cliqué sur le lien d'un courriel inconnu (16 p. cent) ou a saisi des renseignements financiers en utilisant un réseau sans fil public (15 p. cent). Un Canadien sur dix a saisi des renseignements personnels sur un ordinateur qu'ils ne connaissaient pas (10 p. cent), a répondu à un courriel d'hameçonnage sans le savoir (10 p. cent), a répondu à un pourriel sans le savoir (9 p. cent), a saisi des renseignements bancaires dans un site méconnu (7 p. cent) ou a transféré une pièce jointe à un courriel de source inconnue (6 p. cent). Ces résultats sont généralement en harmonie avec ceux de 2016.

Graphique 7 : Fréquence des activités en ligne risquées

« À votre connaissance, avez-vous déjà fait l'une ou l'autre des choses suivantes? »



Les Associés de recherche EKOS

n=2072

Sondage de SP sur la cybersécurité, 2018

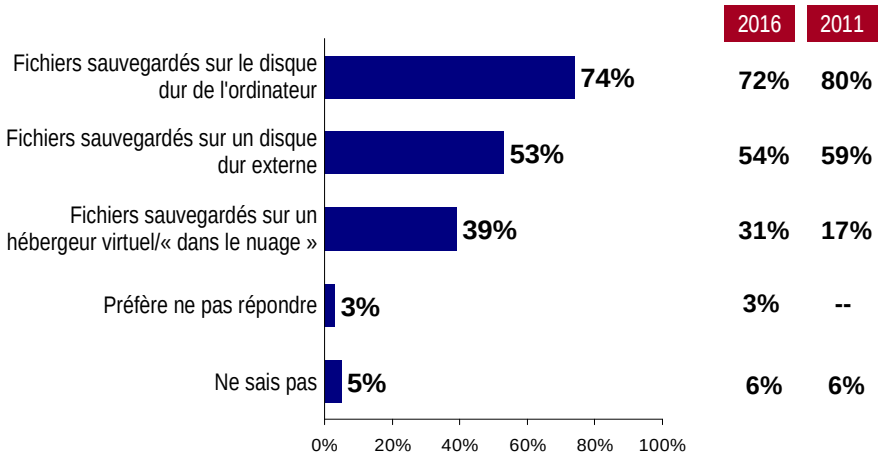
- Les personnes de moins de 25 ans sont plus susceptibles d'avoir ouvert la pièce jointe d'un courriel provenant d'une source inconnue, d'avoir cliqué sur un lien provenant d'une source inconnue ou d'avoir transféré une pièce jointe à un courriel de source inconnue. Les personnes de moins de 35 ans sont plus enclines à avoir saisi des renseignements personnels sur un ordinateur méconnu ou d'avoir saisi des renseignements bancaires sur un site dont elles ne savaient pas s'il était sécurisé. Ceux âgés de moins de 45 ans sont plus enclins à avoir saisi des renseignements financiers sur un réseau sans fil public.
- Les Canadiens qui possèdent un diplôme universitaire ont plus tendance à saisir des renseignements financiers en utilisant un réseau sans fil public ou à saisir des informations personnelles à partir d'un ordinateur méconnu. Les gens dont le revenu du ménage est de 80 000 dollars ou plus sont plus susceptibles d'avoir saisi des renseignements financiers sur un réseau sans fil public.

2.7 STOCKAGE D'INFORMATION

La plupart des Canadiens (74 p. cent, en harmonie avec les résultats de 2016) continuent d'utiliser le disque dur de leur ordinateur pour sauvegarder leurs données à des fins personnelles. Environ la moitié (53 p. cent) sauvegarde des fichiers sur un disque dur externe. Quatre sur dix (39 p. cent) sauvegardent des fichiers sur un serveur virtuel, une augmentation de huit points par rapport à 2016. Cinq pour cent des répondants ne savent pas trop comment ils sauvegardent leurs données et trois pour cent préfèrent ne pas répondre.

Graphique 8 : Stockage d'information

« En ce qui concerne le stockage de l'information à des fins personnelles, est-ce que vous sauvegardez vos données sur le disque dur de votre ordinateur, sur un disque dur externe ou sur un hébergeur virtuel? »



Les Associés de recherche EKOS

n=2072

Sondage de SP sur la cybersécurité, 2018

- La scolarité, l'âge, le revenu et le sexe constituent de fortes variables qui expliquent le recours à l'une ou l'autre des options de stockage d'information signalées ci-dessus. Les Canadiens âgés de 25 à 54 ans sont plus susceptibles que les répondants des autres groupes d'âge d'utiliser l'une ou l'autre des options de stockage d'information. Les hommes ont plus tendance que les femmes à utiliser des disques durs d'ordinateurs ou des disques durs externes. Les gens qui ont fait des études universitaires et ceux dont le revenu annuel du ménage est d'au moins 80 000 dollars sont plus susceptibles d'utiliser toutes les options de stockage de données mentionnées.

3. Niveau de préoccupation et d'importance

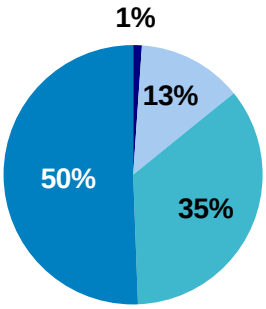
La présente section aborde les perceptions qu'ont les Canadiens quant au problème que constituent les menaces en ligne. Elle examine l'ampleur perçue des risques, y compris la gravité des conséquences, de même que les préoccupations globales face aux risques en ligne. Les résultats révèlent que les Canadiens qui effectuent des activités en ligne comprennent les risques et problèmes qui sont associés à l'utilisation d'Internet, et jugent nécessaire de recourir à des mesures de protection pour assurer leur cybersécurité. Cela dit, certaines données démontrent aussi que plusieurs Canadiens se sentent, eux et leur famille, à l'abri de ces menaces.

3.1 Niveau de préoccupation – Menaces en ligne

Les Canadiens qui utilisent activement Internet sont toujours très préoccupés à la perspective que quelqu'un obtienne et utilise leurs renseignements personnels sans leur autorisation après avoir mené des activités en ligne. La moitié des répondants (50 p. cent) se dit très préoccupée par les menaces en ligne, alors que le tiers (35 p. cent) se dit plutôt préoccupé. Très peu d'entre eux (1 p. cent) affirment ne pas être préoccupés du tout par la possibilité que quelqu'un obtienne de façon frauduleuse leurs renseignements personnels en ligne.

Graphique 9 : Niveau de préoccupation – Menaces en ligne

« Les Canadiennes et Canadiens ont exprimé diverses opinions relativement à leur capacité de protéger leurs renseignements personnels lorsqu'ils sont en ligne. Certains d'entre eux sont très préoccupés, d'autres ne le sont pas. À quel point êtes-vous préoccupé(e) par la possibilité que quelqu'un obtienne de manière frauduleuse vos renseignements personnels en ligne et les utilise pour mener des activités illégales? »



	2016	2011
Pas du tout	1%	1%
Pas tellement	14%	17%
Assez	35%	36%
Très	49%	45%

Les Associés de recherche EKOS

n=2072

Sondage de SP sur la cybersécurité, 2018

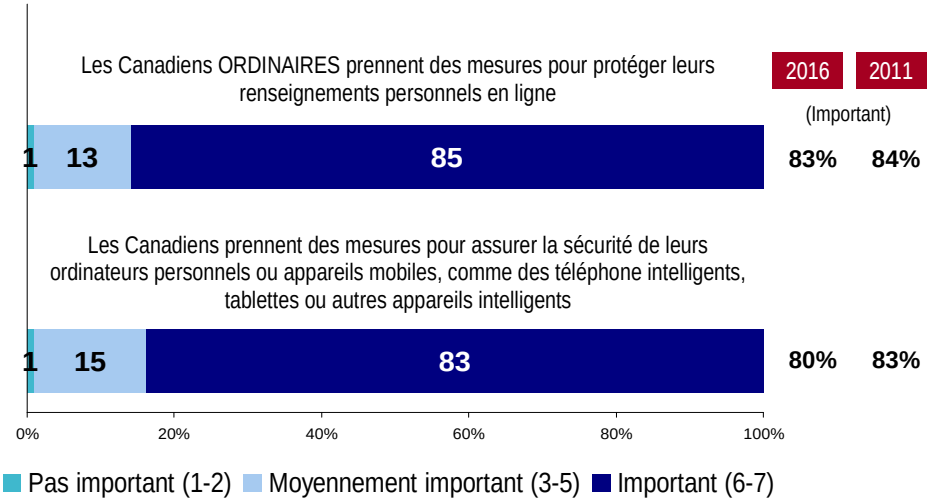
- Les Canadiens âgés (55 ans et plus) sont plus susceptibles d'être très préoccupés par les menaces en ligne.
- Les résidents du Québec et des Prairies sont moins enclins à se dire très préoccupés.

3.2 IMPORTANCE DE SE PROTÉGER CONTRE LES MENACES EN LIGNE

Les Canadiens continuent de croire qu'il est important de se protéger contre les menaces en ligne. En harmonie avec les niveaux de préoccupation enregistrés en 2011 et en 2016, plus de huit répondants sur dix déclarent qu'il est important de prendre des mesures pour protéger ses renseignements personnels en ligne (85 p. cent) ou pour protéger leurs ordinateurs domestiques ou appareils mobiles (83 p. cent).

Graphique 10 : Importance de se protéger contre les menaces en ligne

« Quelle importance pensez-vous de chacun des énoncés suivants…? »



Les Associés de recherche EKOS

n=1991

Sondage de SP sur la cybersécurité, 2018

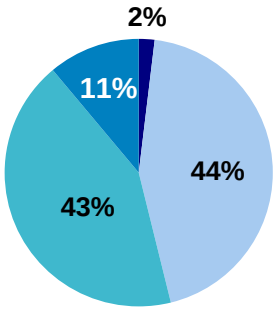
- L'importance perçue de prendre des mesures pour protéger la sécurité de leurs ordinateurs domestiques et appareils mobiles est plus marquée chez les Canadiens âgés de 45 ans et plus. Ceux âgés de moins de 25 ans sont moins enclins à affirmer qu'il est très important de prendre des mesures pour protéger leurs renseignements personnels.

3.3 OMNIPRÉSENCE PERÇUE DES MENACES EN LIGNE

Les Canadiens croient que les menaces en ligne sont de plus en plus omniprésentes. Quelque quatre répondants sur dix (43 p. cent) croient qu'il est fréquent que les Canadiens soient confrontés à des menaces en ligne, ce qui représente une hausse constante par rapport aux 28 pour cent de 2011. Environ la même proportion (44 p. cent) indique que les menaces en ligne sont moyennement fréquentes. Deux pour cent sont d'avis que les menaces en ligne ne sont pas fréquentes.

Graphique 11 : Omniprésence perçue des menaces en ligne

« À quel point est-ce courant que les Canadiens fassent l'objet de menaces en ligne? »



	2016	2011
Pas commun (1-2)	2%	2%
Moyennement commun (3-5)	47%	54%
Commun (6-7)	39%	28%
Ne sais pas	11%	--

Les Associés de recherche EKOS

n=2072

Sondage de SP sur la cybersécurité, 2018

- Les personnes âgées de 45 à 64 ans sont un peu plus enclines à affirmer que les menaces en ligne sont très fréquentes.

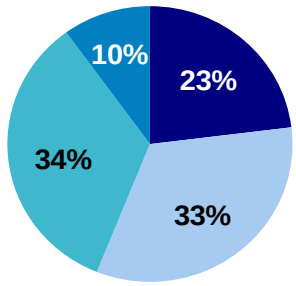
3.4 PROBABILITÉ PERÇUE DES MENACES EN LIGNE

En comparaison avec l'omniprésence perçue à l'égard des menaces en ligne en général, les Canadiens sont moins enclins à croire qu'eux ou un membre de leur famille sera touché. À l'instar des résultats de 2016, un répondant sur trois (34 p. cent) est d'avis qu'il est probable qu'il ait personnellement à composer avec une menace en ligne au cours de l'année à venir. Un autre tiers (33 p. cent) a l'impression que cette probabilité pour les deux prochaines années est modérée, et le quart (23 p. cent) croit que cette situation n'est pas probable.

Parmi ceux qui croient qu'une menace est improbable, la plupart affirment avoir cette opinion parce qu'ils prennent des mesures pour se protéger en ligne (73 p. cent) ou parce qu'ils n'adoptent pas de comportements risqués en ligne (67 p. cent), alors que deux sur cinq (42 p. cent) sont d'avis que les possibilités sont tout simplement très faibles. Une faible proportion (6 p. cent) pense que les menaces en ligne ne concernent que les entreprises et les gens qui ont beaucoup d'argent.

Graphique 12 : Probabilité perçue des menaces en ligne

« À quel point est-il probable que vous fassiez, vous-même ou un membre de votre famille, l'objet d'une menace en ligne au cours des 2 prochaines années? »



	2016	2011
Pas probable (1-3)	23%	21%
Moyennement probable (4)	34%	34%
Probable (5-7)	32%	33%
Ne sais pas	12%	12%

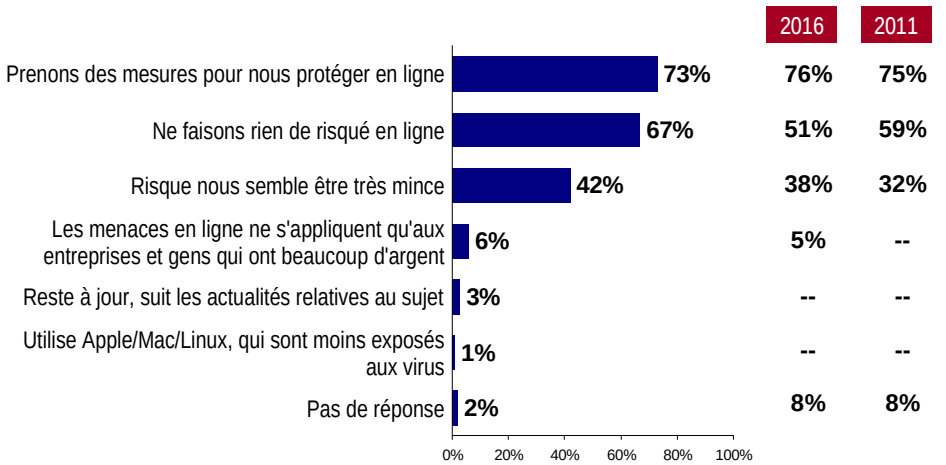
Les Associés de recherche EKOS

n=2072

Sondage de SP sur la cybersécurité, 2018

Graphique 13 : Raisons d'écarter la possibilité de menaces en ligne

« Pourquoi trouvez-vous improbable d'être, vous-même ou un membre de votre famille, affecté par une menace en ligne? »



Les Associés de recherche EKOS

n=492 (pas probable)

Sondage de SP sur la cybersécurité, 2018

- Les répondants âgés de moins de 35 ans sont plus susceptibles de croire qu'il est improbable qu'eux ou un membre de leur famille soient touchés par une menace en ligne.
- Les hommes ont un peu plus tendance que les femmes à se considérer, eux ou un membre de leur famille, comme la cible potentielle d'une menace au cours des deux prochaines années.

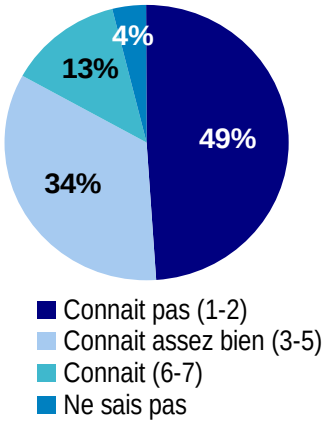
3.5 CRYPTOMONNAIE

Les résultats donnent à penser que les répondants possèdent des connaissances plutôt limitées des cryptomonnaies. La moitié des répondants (49 p. cent) affirme ne pas bien connaître ce moyen d'échange, alors que le tiers (34 p. cent) le connaît dans une certaine mesure. Seule une personne sur huit (13 p. cent) considère très bien connaître les cryptomonnaies.

Parmi ceux qui connaissent au moins dans une certaine mesure les cryptomonnaies, environ seulement une personne sur dix (12 p. cent) en a utilisé. La vaste majorité de ces répondants (86 p. cent) n'ont jamais acheté, échangé ou utilisé une cryptomonnaie.

Graphique 14 : Bonne connaissance des cryptomonnaies

« Dans quelle mesure connaissez-vous la pratique de l'acquisition de cryptomonnaie pour les achats ou le commerce en ligne? »



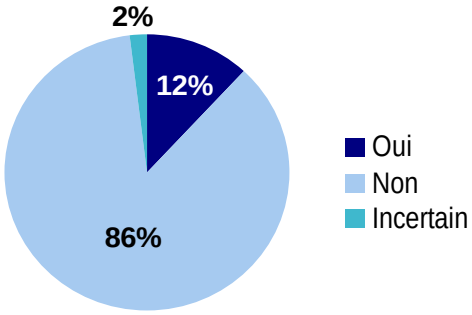
Les Associés de recherche EKOS

n=1036; demi échantillon

Sondage de SP sur la cybersécurité, 2018

Graphique 15 : Utilisation de cryptomonnaies

« Avez-vous déjà fait l'acquisition de cryptomonnaie pour vos achats ou activités en ligne? »



Les Associés de recherche EKOS

n=502; connait la cryptomonnaie (demi échantillon)

Sondage de SP sur la cybersécurité, 2018

- L’autoévaluation du niveau de connaissance des cryptomonnaies baisse constamment avec l’âge. L’utilisation de cryptomonnaies est beaucoup plus élevée chez les répondants âgés de moins de 35 ans, alors que ce type de devise est presque inconnu chez les 55 ans et plus.
- Comparativement aux femmes, les hommes sont plus enclins à déclarer connaître assez bien ou très bien les cryptomonnaies.
- Les gens qui ont fait des études universitaires sont plus susceptibles de considérer qu’ils possèdent au moins des connaissances moyennes à ce sujet.
- Le niveau de connaissance à l’égard des cryptomonnaies augmente progressivement avec le revenu du ménage.

4. CONNAISSANCE

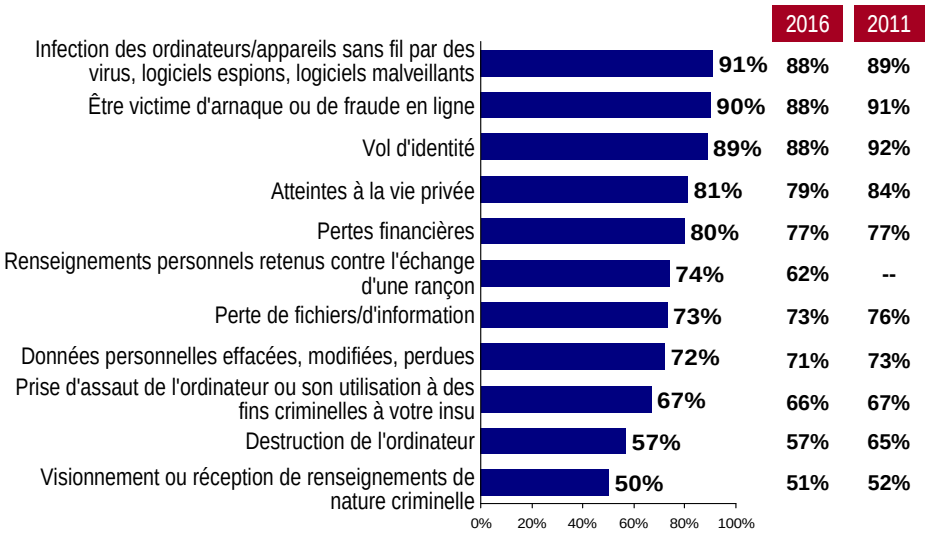
La présente section aborde le niveau de connaissance qu'ont les Canadiens qui utilisent Internet au sujet des risques en ligne et traite des mesures de précaution à prendre pour se protéger contre ces risques. Les Canadiens sont bien au courant de l'existence d'un éventail de risques en ligne, de même que de la variété de mesures de précaution qu'ils peuvent prendre. Par ailleurs, les moyens de déterminer si un site Web est sûr sont relativement peu connus.

4.1 CONNAISSANCE DES MENACES EN LIGNE

La plupart des Canadiens en ligne sont au courant des dangers auxquels ils sont exposés lorsqu'ils utilisent Internet. Dans une proportion semblable aux niveaux de connaissance enregistrés en 2016, neuf Canadiens sur dix sont au courant de l'existence de logiciels espions ou de logiciels malveillants sur les appareils informatiques (91 p. cent), ainsi que de la possibilité d'être victime d'escroquerie ou de fraude en ligne (90 p. cent) ou de vol d'identité (89 p. cent). Huit répondants sur dix connaissent également l'existence de violations de la vie privée (81 p. cent) et de pertes financières (80 p. cent). Près des trois quarts savent qu'une rançon peut être demandée en échange de renseignements personnels (74 p. cent, une augmentation de 12 points par rapport à 2016), ou qu'il est possible qu'ils perdent des fichiers ou des renseignements (73 p. cent), ou certaines de leurs données personnelles soient supprimées, modifiées ou perdues (72 p. cent). Les deux tiers savent qu'il est possible qu'un appareil soit contrôlé à leur insu ou utilisé pour perpétrer d'autres crimes (67 p. cent), alors que quelque six personnes sur dix savent que leur ordinateur peut être détruit (57 p. cent). La moitié (50 p. cent) savent qu'il est possible de voir et de recevoir de l'information de nature criminelle.

Graphique 16 : Connaissance des menaces en ligne

« Voici une liste de certains dangers auxquels on s'expose quand on se sert d'internet. Lesquels de ces dangers connaissiez-vous déjà? »



Les Associés de recherche EKOS

n=2072

Sondage de SP sur la cybersécurité, 2018

- Les Canadiens de 25 à 54 ans sont plus susceptibles que les autres d'affirmer qu'ils sont déjà au courant de chacune de ces menaces en ligne.
- Les résidents du Québec sont systématiquement plus enclins à déclarer qu'ils connaissent ces risques.
- Les hommes sont invariablement plus susceptibles d'affirmer qu'ils connaissent l'existence de ces menaces.
- Les répondants dont le niveau de revenu ou de scolarité est plus élevé sont constamment plus susceptibles d'indiquer qu'ils sont déjà au courant de chacune des menaces en ligne présentées.

4.2 CONNAISSANCE DE MESURES DE PRÉCAUTION

Les résultats mettent en évidence un haut niveau de connaissance au sujet des moyens de réduire les risques d'être confronté à une menace en ligne. Plus de neuf personnes sur dix disent connaître certaines mesures de précaution pouvant être prises, comme le fait de ne pas partager les mots de passe (95 p. cent), de ne pas ouvrir les pièces jointes de courriels provenant de personnes inconnues (94 p. cent), de limiter la quantité de renseignements personnels qu'ils partagent en ligne (94 p. cent) et d'utiliser des logiciels anti-espions et antivirus (93 p. cent). Neuf répondants sur dix disent savoir qu'il leur faut effectuer leurs transactions bancaires sur un ordinateur sécuritaire (92 p. cent), utiliser des mots de passe longs et complexes (91 p. cent), protéger leurs réseaux domestiques sans fil à l'aide d'un mot de passe (91 p. cent), utiliser différents mots de passe pour différents comptes et sites Web (90 p. cent), choisir avec soin les sites de magasinage en ligne (89 p. cent) et éviter d'utiliser des réseaux sans fil publics lorsqu'ils font du magasinage et qu'ils effectuent des transactions bancaires en ligne (89 p. cent, une légère hausse comparativement aux 83 p. cent de 2016). Une proportion un peu plus faible de répondants (86 p. cent) dit savoir comment utiliser des pare-feu et des mots de passe pour protéger leurs appareils. Le niveau de connaissance est plutôt en harmonie avec les résultats de 2011 et 2016, bien qu'il semble y avoir depuis 2011 une augmentation constante de l'utilisation de mots de passe plus longs et plus complexes, de la protection des réseaux sans fil domestiques par le biais d'un mot de passe, et de l'utilisation de mots de passe différents pour différents comptes ou sites Web. Depuis que la question a été posée pour la première fois en 2016, de plus en plus de gens affirment éviter de faire du magasinage en ligne ou de réaliser des transactions bancaires sur un réseau sans fil public.

Graphique 17 : Connaissance de mesures de précaution

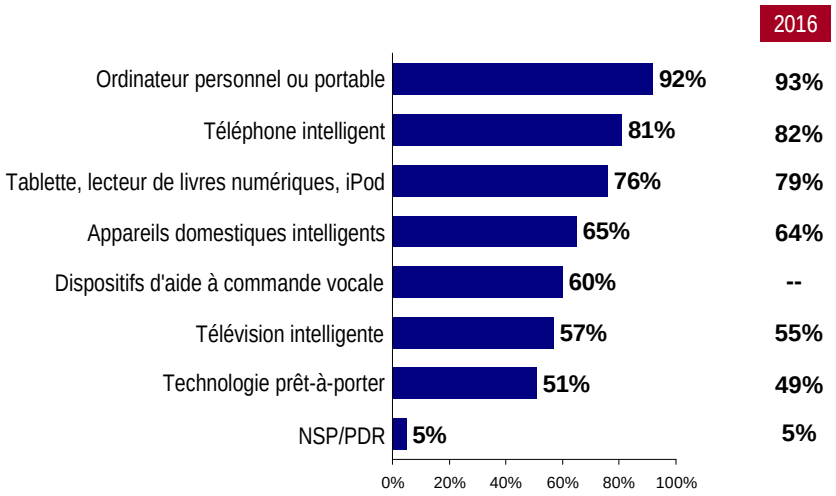
« Voici une liste de mesures visant à réduire le risque de faire l'objet d'une menace en ligne. Certains sont au courant de ces mesures, tandis que d'autres ne le sont pas. Lesquelles des suivantes connaissiez-vous déjà? »

- Les Canadiens de moins de 25 ans sont systématiquement moins enclins à déclarer qu'ils connaissent bien ces mesures de précaution.
- La connaissance de ces mesures de précaution augmente immanquablement avec le revenu et le niveau de scolarité.

Les Canadiens savent que la plupart des appareils sont susceptibles d'être touchés. Neuf répondants sur dix (92 p. cent) sont d'avis que les ordinateurs personnels et les portables sont susceptibles de faire l'objet d'une menace en ligne. Dans une proportion d'environ huit sur dix, les répondants estiment que les téléphones intelligents (81 p. cent) ainsi que les tablettes ou les lecteurs de livres numériques (76 p. cent) sont susceptibles de faire l'objet d'une menace en ligne. Les deux tiers (65 p. cent) croient que leurs appareils domestiques intelligents peuvent également être touchés, alors que quelque six personnes sur dix ont l'impression que les dispositifs à commande vocale (60 p. cent) et les télévisions intelligentes (57 p. cent) peuvent être ciblés. La moitié (51 p. cent) est au courant de la menace potentielle que présentent les dispositifs portables. Ces résultats sont en harmonie avec ceux de 2016.

Graphique 18 : Appareils potentiellement en danger

« Quels appareils parmi les suivants peuvent faire l'objet d'une menace en ligne? »



Les Associés de recherche EKOS

n=2072

Sondage de SP sur la cybersécurité, 2018

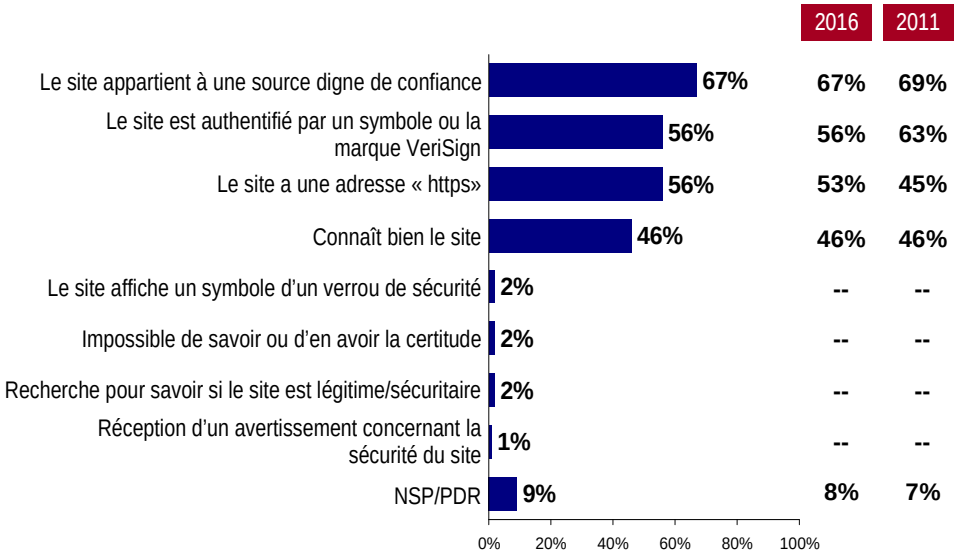
- Les Canadiens âgés de 25 à 54 ans, de même que ceux dont le revenu et le niveau de scolarité sont plus élevés, sont plus susceptibles de savoir que la plupart des appareils peuvent faire l'objet d'une menace en ligne.
- Dans l'ensemble des régions, les Canadiens perçoivent dans des proportions semblables les menaces dont peuvent faire l'objet les ordinateurs, tablettes et téléphones intelligents. Toutefois, les résidents du Québec sont moins enclins à considérer comme risqués les appareils domestiques intelligents, les appareils à commande vocale, les télévisions intelligentes et les dispositifs portables.

4.3 CERNER LES SITES WEB SÛRS

Au nombre des Canadiens qui affirment faire des opérations bancaires en ligne, les deux tiers (67 p. cent) disent savoir qu'un site Web est sécurisé lorsqu'il appartient à une source digne de confiance (comme un fournisseur de services connu, un fournisseur de logiciel, un site Web du gouvernement, etc.). Plus de la moitié d'entre eux déterminent si un site Web est sécurisé au moyen du symbole ou de la marque VeriSign (56 p. cent; 58 p. cent en comptant les gens qui font sans aide allusion au symbole d'un cadenas[3]) ou grâce à l'adresse https (56 p. cent). Un peu moins de la moitié des répondants (46 p. cent) estiment qu'un site Web est sécurisé s'ils le connaissent bien. Ces résultats sont en harmonie avec ceux de 2016.

Graphique 19 : Cerner les sites Web sûrs

« Comment peut-on savoir si un site Web est sécurisé? »



Les Associés de recherche EKOS

n=1880 (Fait des transactions bancaires en ligne)

Sondage de SP sur la cybersécurité, 2018

[3] Le symbole du cadenas qu'ont décrit quelques personnes ne faisait pas partie de la liste initiale des catégories de réponse à laquelle les répondants avaient accès, mais était codifié pour les réponses ouvertes à la suite de la collecte des sondages.

- Les Canadiens plus jeunes (moins de 35 ans) sont plus enclins à estimer qu'un site Web est sécurisé s'il appartient à une source digne de confiance. Par rapport aux autres groupes d'âge, les personnes ayant de 25 à 44 ans sont plus enclines à estimer qu'un site assorti d'une adresse https ou d'un symbole ou de la marque VeriSign est un site sécurisé.
- À l'échelle régionale, les résidents du Québec ont moins tendance à considérer qu'un site qu'ils connaissent personnellement ou qu'un site assorti d'un symbole ou de la marque VeriSign est un site sécurisé.
- Les gens qui ont fait des études universitaires sont plus susceptibles de mentionner un site assorti d'une adresse https ou d'un symbole ou de la marque VeriSign.

5. ATTITUDES

La présente section brosse un tableau des attitudes des Canadiens qui sont en ligne en ce qui concerne les risques en ligne et la nécessité de s'en protéger. Ces résultats prolongent en quelque sorte ceux de la section 3. Ils démontrent que la plupart des Canadiens sont très conscients de la menace et croient fermement que les gens doivent prendre des mesures pour assurer leur sécurité en ligne, bien qu'il y ait certains écarts particuliers en ce qui a trait au niveau de connaissance.

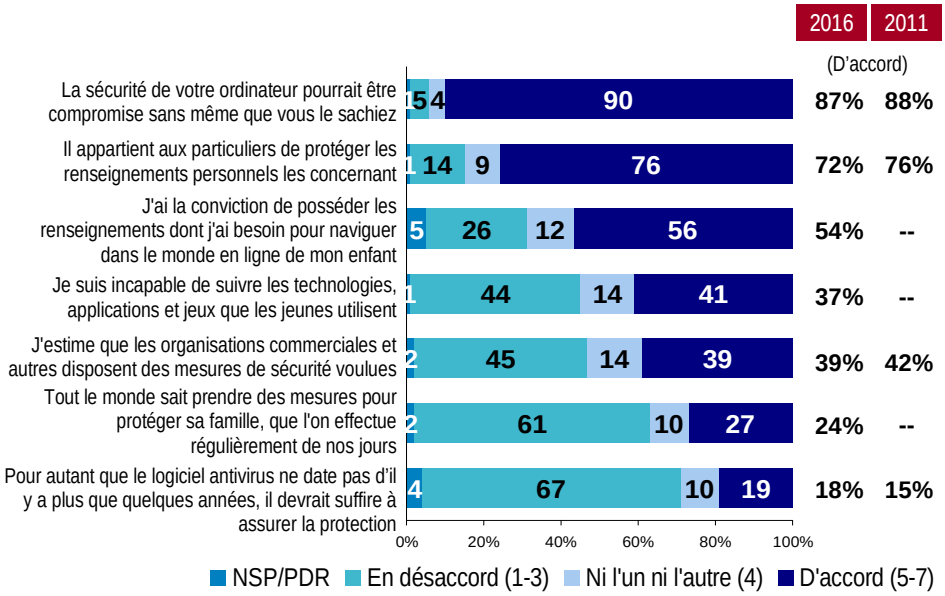
5.1 ATTITUDES AU SUJET DES MENACES EN LIGNE

À l'instar des résultats de 2016, neuf Canadiens sur dix (90 p. cent) savent qu'un ordinateur peut être affecté sans que le propriétaire le sache. Ils ont tendance à croire qu'il est de la responsabilité des gens de protéger leurs renseignements personnels, trois personnes sur quatre (76 p. cent) étant d'accord avec cet énoncé (une légère hausse en comparaison avec les 72 p. cent de 2016, mais en harmonie avec les résultats de 2011).

Les Canadiens affichent un peu moins de confiance en ce qui concerne leur capacité à se protéger contre la plupart des menaces en ligne. Un peu plus de la moitié des parents (56 p. cent) sont d'accord pour dire qu'ils ont les renseignements dont ils ont besoin pour naviguer dans le monde virtuel de leur enfant. Quatre parents sur dix ont l'impression de ne pas être en mesure de suivre l'évolution des technologies que les jeunes utilisent (41 p. cent, une légère hausse par rapport aux 37 p. cent de 2016). Quatre Canadiens sur dix conviennent que les entreprises ont recours à des mesures de sécurité adéquates pour protéger leurs renseignements personnels (39 p. cent). Les Canadiens sont toujours pessimistes en ce qui a trait à leur capacité à se protéger en ligne, alors que seuls 27 pour cent sont d'accord pour dire que tout le monde connaît les mesures à prendre pour se protéger. Soixante-et-un pour cent sont en désaccord avec cet énoncé. Dans une proportion de près d'un sur cinq (19 p. cent), les Canadiens adhèrent à tort à l'énoncé indiquant que tant qu'un logiciel antivirus qui est installé sur leur ordinateur n'a pas plus que quelques années, il devrait protéger leur ordinateur.

Graphique 20 : Attitudes au sujet des menaces en ligne

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



Les Associés de recherche EKOS

Sondage de SP sur la cybersécurité, 2018

- Les jeunes Canadiens (moins de 25 ans) sont moins enclins à convenir que la sécurité de leur ordinateur peut être compromise sans qu'ils le sachent. Ils ont également plus tendance à être d'accord pour dire que tout le monde connaît les mesures à prendre pour se protéger contre les menaces en ligne.
- Les Canadiens qui ont fait des études universitaires sont plus susceptibles d'être en désaccord avec l'énoncé voulant qu'il soit de la responsabilité des gens de protéger leurs renseignements personnels.
- Les plus jeunes Canadiens, tout comme ceux qui ont un plus faible revenu ou qui vivent au Québec, ont plus tendance à croire que les entreprises prennent des mesures de sécurité adéquates pour protéger leurs renseignements personnels.
- Les jeunes parents sont plus susceptibles de ne pas être d'accord pour dire qu'ils sont incapables de suivre l'évolution des technologies que les jeunes utilisent.
- Les jeunes Canadiens sont près de deux fois plus susceptibles de convenir que pour autant que leur logiciel antivirus est à jour, ils sont protégés. Les hommes ont plus tendance que les femmes à être en désaccord.

6. MESURES DE PRÉCAUTION

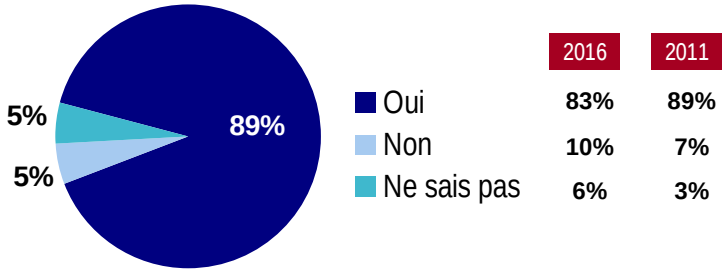
La présente section traite des comportements qu'adoptent concrètement les Canadiens pour se protéger contre les risques en ligne. Les résultats du sondage contribuent à éclairer nos connaissances au sujet des groupes de la population qui prennent des mesures de protection et de ceux qui ne le font pas.

6.1 FRÉQUENCE DÉCLARÉE DES MESURES DE PRÉCAUTION

Neuf Canadiens sur dix (89 p. cent) affirment prendre des mesures de précaution pour protéger leur ordinateur et autres appareils qu'ils utilisent pour accéder à Internet, une baisse de six points par rapport à 2016. Cinq pour cent des répondants indiquent ne pas prendre de mesures de précaution pour protéger leurs appareils et cinq pour cent sont incertains.

Graphique 21 : Fréquence déclarée des mesures de précaution

« Certains prennent des précautions pour protéger leur ordinateur et les autres appareils qu'ils utilisent pour accéder à internet, alors que d'autres n'en prennent pas. Prenez-vous des précautions pour protéger vos appareils? »



	2016	2011
Oui	83%	89%
Non	10%	7%
Ne sais pas	6%	3%

Les Associés de recherche EKOS

n=2014

Sondage de SP sur la cybersécurité, 2018

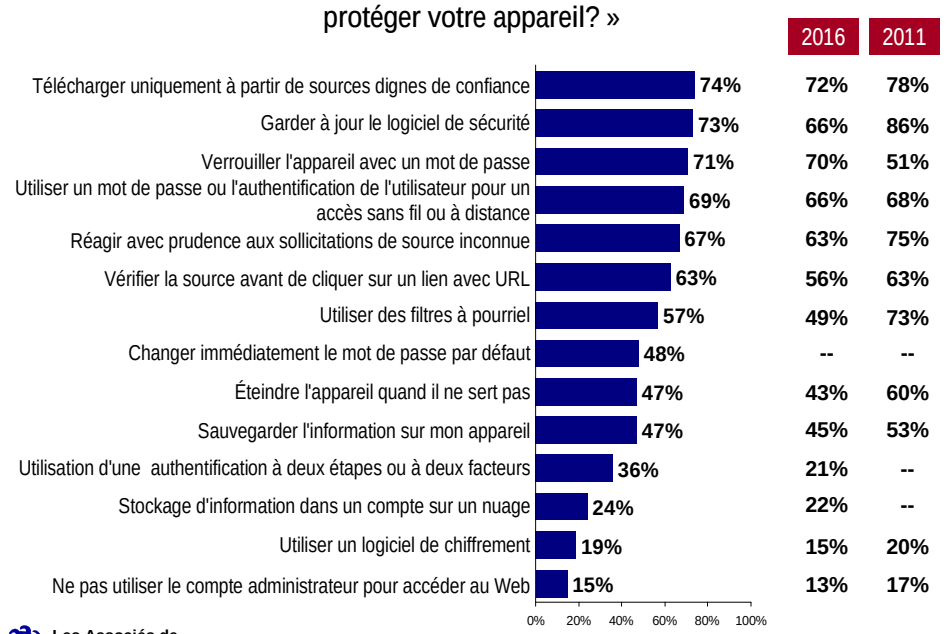
- Les répondants de moins de 35 ans sont plus enclins à dire qu'ils ne prennent pas de mesures de précaution.

6.2 TYPES DE MESURES DE PRÉCAUTION ADOPTÉES (PROTECTION DES APPAREILS)

Les Canadiens signalent aussi un large éventail de mesures de précaution pour protéger leurs appareils. Les trois quarts disent effectuer des téléchargements seulement à partir de sources de confiance (74 p. cent) et garder leur logiciel de sécurité à jour (73 p. cent, une hausse par rapport aux 66 p. cent de 2016). Environ sept répondants sur dix assurent protéger leurs appareils avec un mot de passe (71 p. cent), protéger leur réseau sans fil à l'aide d'un mot de passe (69 p. cent) et faire preuve de prudence lorsqu'ils répondent à des sollicitations d'étrangers (67 p. cent, une hausse par rapport aux 63 p. cent de 2016). Quelque six personnes sur dix vérifient la source d'un lien URL avant de cliquer dessus (63 p. cent, une hausse par rapport à 56 p. cent) et utilisent des filtres antipourriel (57 p. cent, une hausse par rapport à 49 p. cent). Environ la moitié dit modifier immédiatement les mots de passe par défaut (48 p. cent), éteindre les appareils quand ils ne les utilisent pas (47 p. cent, une hausse par rapport à 43 p. cent) et faire des copies de sécurité de leurs appareils (47 p. cent). Le tiers a recours à un processus d'authentification à deux étapes (36 p. cent, une hausse de 15 points par rapport à 2016), tandis que le quart (24 p. cent) stocke de l'information dans un service infonuagique. Une personne sur cinq indique utiliser un logiciel de chiffrement (19 p. cent, une hausse par rapport à 15 p. cent) et 15 pour cent n'utilisent pas un compte d'administrateur pour accéder au Web.

Graphique 22 : Types de mesures de précaution adoptées (protection des appareils)

« Quelles mesures de précaution parmi les suivantes prenez-vous pour protéger votre appareil? »



Les Associés de recherche EKOS

n=2014

Sondage de SP sur la cybersécurité, 2018

- Les Canadiens âgés de 55 ans et plus sont plus susceptibles de garder leur logiciel de sécurité à jour et d'éteindre leurs appareils lorsqu'ils ne les utilisent pas. Ceux âgés de 25 à 44 ans ont plus tendance à recourir à la plupart des autres tactiques testées.
- Les résidents de la Colombie-Britannique sont plus susceptibles de modifier immédiatement leurs mots de passe par défaut et d'utiliser un processus d'authentification à deux étapes. Les résidents du Québec sont moins enclins à télécharger des fichiers exclusivement d'une source sûre, à utiliser des filtres antipourriel, à faire de copies de sécurité de leurs appareils, à utiliser un processus d'authentification à deux étapes ou à modifier immédiatement leurs mots de passe par défaut.
- Les hommes ont plus tendance que les femmes à garder leur logiciel de sécurité à jour, à faire des copies de sécurité de leurs appareils, à utiliser un processus d'authentification à deux étapes et à utiliser un logiciel de chiffrement.
- Dans l'ensemble, les répondants dont les niveaux de revenu et de scolarité sont supérieurs sont plus susceptibles de prendre des mesures de précaution pour protéger leur ordinateur et leurs autres appareils.

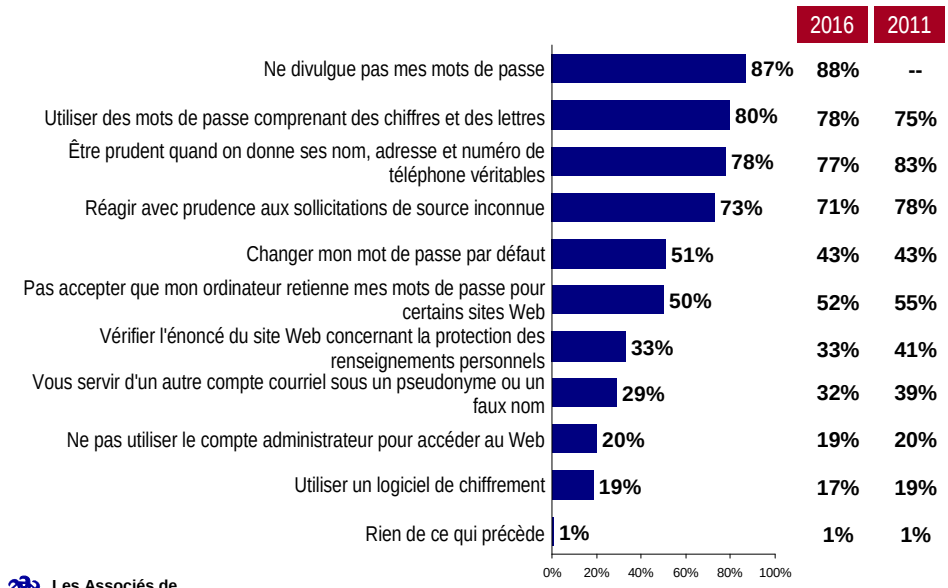
6.3 TYPES DE MESURES DE PRÉCAUTION PRISES (MENACES EN LIGNE)

La plupart des Canadiens prennent des mesures de précaution pour protéger leurs renseignements personnels contre les menaces en ligne. Ces résultats sont en grande partie en harmonie avec ceux de 2016. Environ neuf personnes sur dix (87 p. cent) affirment ne pas partager leurs mots de passe. D'autre part, environ huit Canadiens sur dix recourent à des mots de passe contenant un mélange aléatoire de chiffres et de lettres (80 p. cent) ou font preuve de prudence lorsqu'ils communiquent de l'information comme leur vrai nom, leur adresse ou leur numéro de téléphone (78 p. cent). Quelque sept répondants sur dix (73 p. cent) font preuve de prudence lorsqu'ils répondent à des sollicitations d'étrangers. La moitié modifie ses mots de passe (51 p. cent, une hausse par rapport aux 43 p. cent de 2016) ou ne permet pas à son ordinateur de se rappeler les mots de passe des sites Web (50 p. cent).

Environ trois répondants sur dix vérifient les politiques des sites en matière de protection de la vie privée (33 p. cent) ou utilisent des comptes de courriels supplémentaires en ayant recours à un pseudonyme (29 p. cent). Au nombre des mesures adoptées moins souvent figurent la non-utilisation d'un compte administrateur pour accéder au Web (20 p. cent), de même que l'utilisation d'un logiciel de chiffrement (19 p. cent).

Graphique 23 : Types de mesures adoptées (menaces en ligne)

« Lesquelles des précautions suivantes prenez-vous pour vous protéger contre les menaces en ligne et protéger vos renseignements personnels? »



Les Associés de recherche EKOS

n=2072

Sondage de SP sur la cybersécurité, 2018

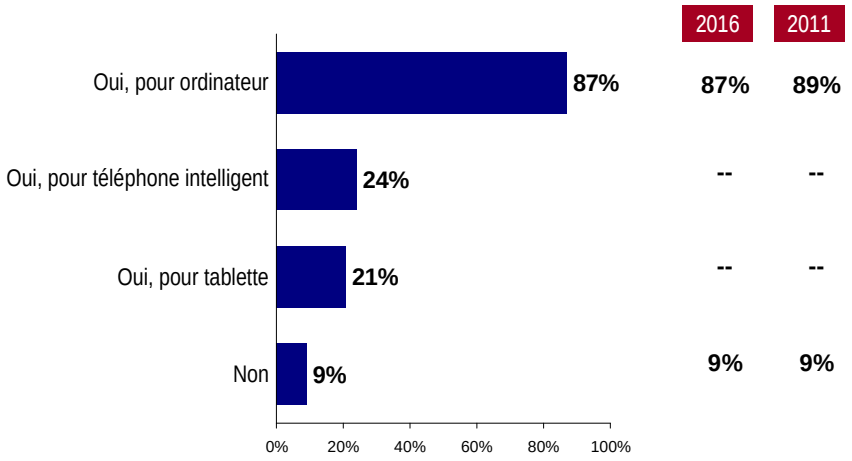
- Les Canadiens âgés de 25 à 44 ans sont plus enclins à modifier leurs mots de passe, à utiliser des comptes de courriels supplémentaires en ayant recours à un pseudonyme et à utiliser un logiciel de chiffrement. Ceux âgés de 55 à 64 ans ont plus tendance à s'abstenir d'utiliser des comptes d'administrateur lorsqu'ils accèdent au Web. Les moins de 25 ans sont systématiquement moins enclins à prendre la plupart des mesures de précaution examinées. Comparativement, ceux âgés de 55 ans et plus sont moins susceptibles de modifier leurs mots de passe ou d'utiliser des comptes de courriels supplémentaires en ayant recours à un pseudonyme.
- À l'échelle régionale, les résidents du Québec sont plus susceptibles de déclarer qu'ils ne permettent pas à leur navigateur de se rappeler leurs mots de passe.
- En comparaison avec les femmes, les hommes sont plus enclins à modifier leurs mots de passe, à utiliser des comptes de courriels supplémentaires en ayant recours à un pseudonyme et à utiliser un logiciel de chiffrement. En revanche, les femmes ont plus tendance à s'abstenir de conserver leurs mots de passe dans leur navigateur.
- Les gens qui ont fait des études universitaires et ceux qui ont des revenus plus élevés sont plus enclins à affirmer avoir recours à toutes ces mesures de précaution.

6.4 Recours à un logiciel antivirus

À l'instar des résultats obtenus dans les versions antérieures du sondage, la vaste majorité des répondants (87 p. cent) ont un logiciel antivirus sur leur ordinateur. Les répondants semblent toutefois faire preuve de moins de prudence avec leurs appareils mobiles. Seul le quart (24 p. cent) a un logiciel antivirus sur son téléphone intelligent et un cinquième (21 p. cent) en a un sur sa tablette.

Graphique 24 : Recours à un logiciel antivirus

« Avez-vous un logiciel antivirus sur votre ordinateur, téléphone intelligent ou tablette? »



Les Associés de recherche EKOS

n=1907

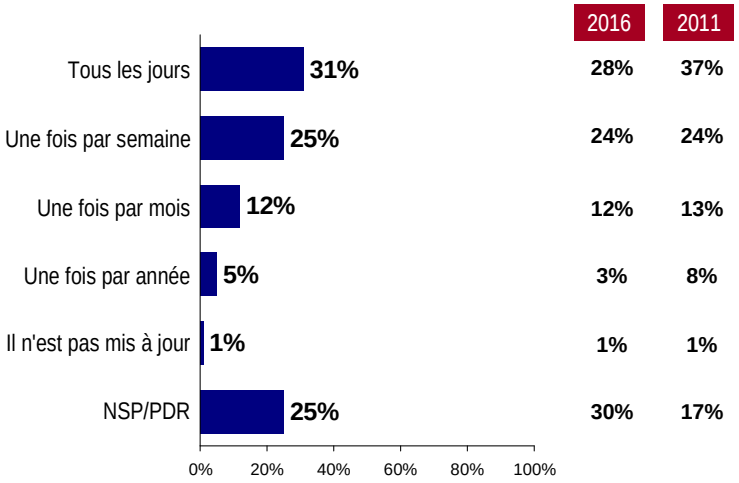
Sondage de SP sur la cybersécurité, 2018

- Les Canadiens de moins de 45 ans sont moins enclins à avoir un logiciel antivirus sur leur ordinateur, tandis que les Canadiens plus âgés ont beaucoup plus tendance à en avoir un.

Les résultats donnent à penser que trois Canadiens sur dix (31 p. cent) actualisent leur logiciel antivirus au quotidien (manuellement ou automatiquement), tandis que le quart (25 p. cent) le fait toutes les semaines. Une personne sur huit (12 p. cent) actualise son logiciel sur une base mensuelle, alors qu'une personne sur vingt (5 p. cent) le fait sur une base annuelle. Le quart des répondants (25 p. cent) ne savent pas à quelle fréquence le logiciel antivirus de leur ordinateur est mis à jour. Ces résultats sont en harmonie avec ceux de 2016.

Graphique 25 : Choix du moment des mises à jour

[SI OUI] « À quelle fréquence le logiciel antivirus de votre ordinateur, téléphone intelligent ou tablette est-il actualisé (par vous ou automatiquement) pour obtenir la protection la plus récente? »



(A un logiciel antivirus dans son ordinateur)

Les Associés de recherche EKOS

n=1653

Sondage de SP sur la cybersécurité, 2018

- Les gens âgés de moins de 25 ans ont tendance à attendre plus longtemps avant d'actualiser leur logiciel antivirus, alors que les 45 à 64 ans sont plus susceptibles de le faire tous les jours.
- Les hommes sont beaucoup plus enclins à affirmer mettre à jour leur logiciel antivirus tous les jours, alors que les femmes sont plus susceptibles de déclarer ne pas savoir à quelle fréquence leur logiciel est mis à jour.

6.5 RAISONS DE NE PAS AVOIR DE LOGICIEL ANTIVIRUS

Les Canadiens dont l'ordinateur n'est pas doté d'un logiciel antivirus devaient indiquer les raisons pour lesquelles ils n'en ont pas en s'appuyant sur une liste. Ces résultats sont en grande partie en harmonie avec ceux de 2016. Quatre répondants sur dix (40 p. cent) disent ne pas croire qu'il est nécessaire d'avoir un logiciel antivirus pour leur téléphone intelligent ou leur tablette, alors qu'une personne sur trois (34 p. cent) a l'impression de ne pas en avoir besoin en général. Le quart d'entre eux (25 p. cent) affirme que son système d'exploitation n'est pas sensible aux virus, une diminution de onze points de pourcentage par rapport à 2016. Le cinquième des répondants estime que cela coûterait trop cher (21 p. cent), qu'il ne fait que des activités sécuritaires quand il est en ligne (20 p. cent) ou encore, qu'il ne consulte que des sites Web sécuritaires (16 p. cent). Une personne sur sept croit que son ordinateur vérifie automatiquement la présence de virus (14 p. cent). Des répondants indiquent également ne pas savoir quoi acheter et installer (7 p. cent), se disent préoccupés par la possibilité qu'un logiciel antivirus réduise le rendement de leur appareil (7 p. cent) ou croient que les logiciels antivirus sont inefficaces (5 p. cent).

Graphique 26a : Raisons de ne pas avoir de logiciel antivirus

[SI NON] « Il y a diverses raisons pour lesquelles les gens n'ont pas de logiciel antivirus. Pourquoi n'avez-vous pas de logiciel antivirus? »

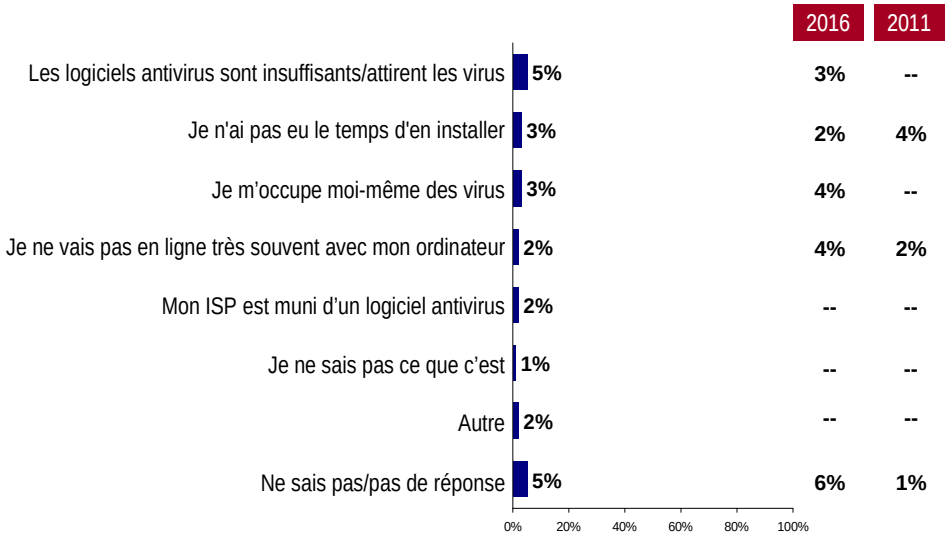
Les Associés de recherche EKOS

n=176; pas de logiciel antivirus

Sondage de SP sur la cybersécurité, 2018

Graphique 26b : Raisons de ne pas avoir de logiciel antivirus

[SI NON] « Il y a diverses raisons pour lesquelles les gens n'ont pas de logiciel antivirus. Pourquoi n'avez-vous pas de logiciel antivirus? »



Les Associés de recherche EKOS

n=176; pas de logiciel antivirus

Sondage de SP sur la cybersécurité, 2018

6.6 Fréquence du changement des mots de passe en ligne

Lorsqu'interrogés sur la fréquence à laquelle ils modifient leurs mots de passe, les répondants affirment dans une proportion d'un sur cinq environ (15 à 18 p. cent) qu'ils ne mettent jamais leurs comptes à jour, alors qu'environ la même proportion (14 à 23 p. cent) affirme mettre ses comptes à jour quelques fois par année. Environ une personne sur dix actualise les mots de passe de ses comptes en ligne une fois par année (11 à 12 p. cent) ou quelques fois par année (10 à 12 p. cent). Seuls six à sept pour cent actualisent leurs mots de passe plus que quelques fois par année. Environ le dixième des répondants dit mettre à jour ses mots de passe lorsqu'on l'invite à le faire (8 à 10 p. cent) ou lorsqu'il y pense (8 à 9 p. cent). De six à sept pour cent mettent à jour leurs mots de passe seulement lorsqu'ils apprennent l'existence d'une brèche de sécurité.

Il est plus courant que les Canadiens affirment que cela ne s'applique pas aux comptes des médias sociaux (13 p. cent) ou aux comptes de magasinage en ligne (15 p. cent) que ce ne l'est au sujet des comptes courriel (1 p. cent).

Tableau 2: Fréquence du changement des mots de passe

Bien des gens utilisent les mêmes mots de passe pour différents comptes et appareils, et conservent les mêmes mots de passe au fil du temps. À quelle fréquence diriez-vous que vous modifiez un mot de passe dans chacune des situations suivantes? (n=1050)

	Comptes de médias sociaux	Comptes de magasinage en ligne	Comptes de courriel
Jamais	18 %	15 %	18 %
Après quelques années	17 %	14 %	23 %
Une fois par année	11 %	12 %	11 %
Quelques fois par année	10 %	10 %	12 %
Plus souvent que quelques fois par année	6 %	7 %	7 %
Quand on m'invite à le faire	8 %	10 %	10 %
Quand j'y pense/Pas à intervalle fixe	8 %	9 %	9 %
Lorsque j'apprends l'existence d'une brèche de sécurité	6 %	6 %	7 %
Sans objet (n'en a pas)	13 %	15 %	1 %
Pas de réponse	3 %	3 %	2 %

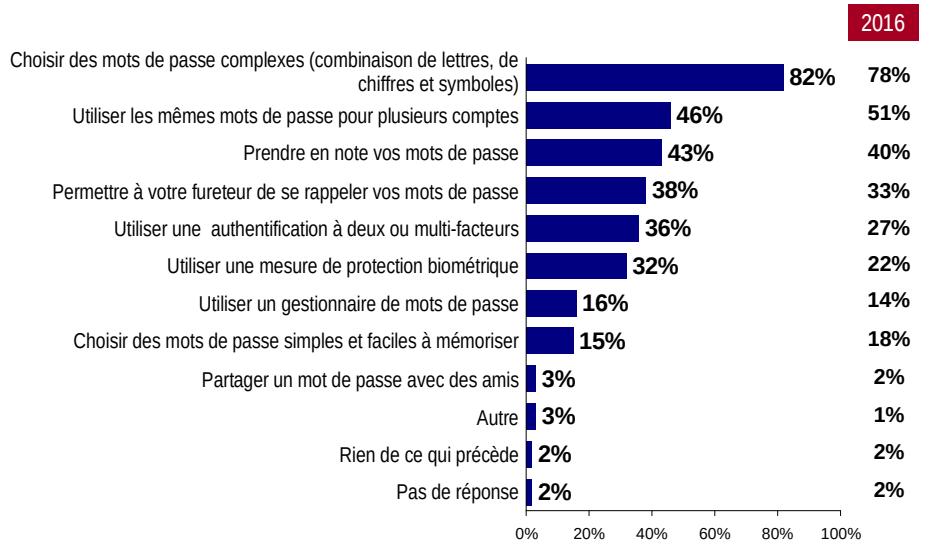
- Les plus jeunes Canadiens (moins de 25 ans) sont plus enclins à actualiser leurs mots de passe seulement lorsqu'ils entendent parler d'une brèche de sécurité.

Les Canadiens adoptent divers comportements pour protéger leurs mots de passe. Dans une proportion de huit sur dix (82 p. cent, une légère augmentation en comparaison avec les 78 p. cent de 2016), les répondants tentent de faire en sorte que leurs mots de passe soient complexes, et environ un Canadien sur trois dit recourir à des pratiques de sécurité comme l'authentification à deux étapes (36 p. cent, une hausse par rapport à 27 p. cent) ou la protection biométrique (32 p. cent, une hausse par rapport à 22 p. cent).

Pour se rappeler leurs mots de passe, les Canadiens utilisent le même mot de passe pour plusieurs comptes (46 p. cent, en légère baisse par rapport à 51 p. cent), prennent en note leurs mots de passe (43 p. cent) ou permettent à un navigateur de se rappeler leurs mots de passe (38 p. cent, une hausse par rapport à 33 p. cent). Seule une personne sur six dit utiliser un gestionnaire de mots de passe (16 p. cent) ou utiliser des mots de passe simples (15 p. cent). Peu de membres de la population disent partager leur mot de passe avec leurs amis (3 p. cent).

Graphique 27 : Pratiques sécuritaires

« Quels gestes parmi les suivants posez-vous, s'il y a lieu? »



Les Associés de recherche EKOS

n=2072

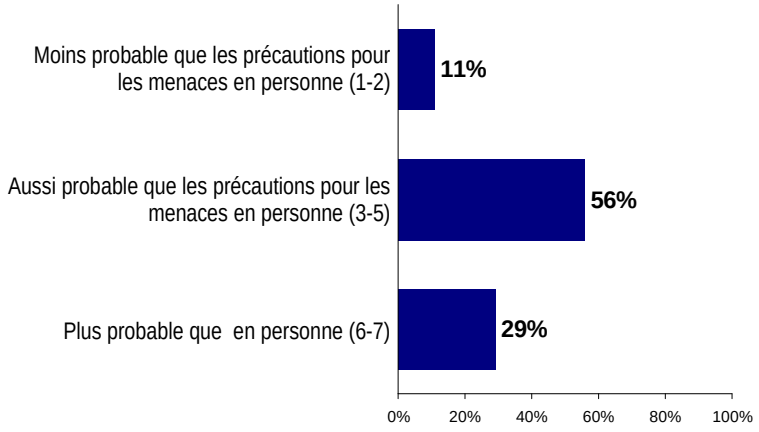
Sondage de SP sur la cybersécurité, 2018

- Les Canadiens plus âgés (plus de 55 ans) sont plus susceptibles d'écrire leurs mots de passe pour s'en souvenir, tandis que les Canadiens de 25 à 44 ans sont plus susceptibles d'adopter chacun des comportements testés.
- Les résidents du Québec sont plus susceptibles d'écrire leurs mots de passe et moins enclins à utiliser le même mot de passe pour plusieurs comptes ou à permettre à un navigateur de retenir leurs mots de passe.
- Les gens qui ont fait des études universitaires ont plus tendance à mettre en pratique chacune des procédures testées (c.-à-d. mots de passe complexes, authentification à deux étapes et renseignements biométriques). Ils sont aussi plus enclins à utiliser le même mot de passe pour plusieurs comptes et à permettre à un navigateur de retenir leurs mots de passe.
- Les personnes dont le revenu du ménage est plus bas sont plus susceptibles d'écrire leurs mots de passe. Les répondants dont les niveaux de revenu sont plus élevés sont plus susceptibles de faire état de la plupart des comportements, aussi bien les plus bénéfiques que les plus nuisibles.

Les répondants ont été invités à indiquer s'ils faisaient preuve d'autant de prudence face aux menaces en ligne que face à celles en personne. Une personne sur dix (11 p. cent) affirme être moins susceptible de prendre des mesures de précaution contre les menaces en ligne que contre les menaces en personne, alors que trois sur dix (29 p. cent) ont plus tendance à faire preuve de prudence dans le monde numérique que dans le monde réel. Un peu plus de la moitié des répondants (56 p. cent) sont aussi prudents dans l'une ou l'autre de ces deux situations.

Graphique 28 : Probabilité de prendre des mesures de précaution contre les menaces en ligne par rapport aux menaces en personne

« Dans quelle mesure seriez-vous susceptible de prendre des précautions contre les menaces en ligne à la façon dont vous le faites pour les menaces en personne? »



Les Associés de recherche EKOS

n=1036 (demi échantillon)

Sondage de SP sur la cybersécurité, 2018

- Les gens âgés de 55 ans et plus sont plus enclins à déclarer prendre plus de mesures de précaution dans le monde virtuel que dans le monde réel.

7. FRÉQUENCE À LAQUELLE LES GENS SONT DES VICTIMES

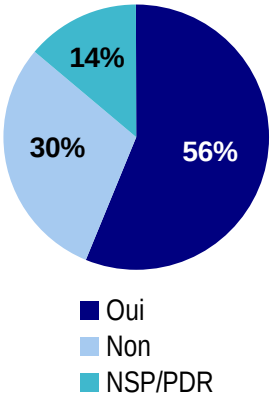
La présente section expose certaines données au sujet de la fréquence à laquelle les menaces en ligne se concrétisent. Peut-être plus important encore, cette section donne une idée de la mesure dans laquelle une expérience antérieure influe (ou pas) sur des changements d'opinion au sujet de la probabilité d'être touché ou sur des changements sur le plan des comportements de protection.

7.1 FRÉQUENCE ET EFFETS DES ATTAQUES INFORMATIQUES

Plus de la moitié des Canadiens (56 p. cent) dit avoir vécu un incident où un virus, un logiciel espion ou un logiciel malveillant se trouvait sur leur ordinateur. Près d'une personne sur trois (30 p. cent) n'a pas subi d'attaque informatique et 14 pour cent s'en disent incertains.

Graphique 29 : Fréquence des attaques informatiques

« Vos appareils ont-t-ils déjà été infecté par un virus, un logiciel espion ou un logiciel malveillant? »



Les Associés de recherche EKOS

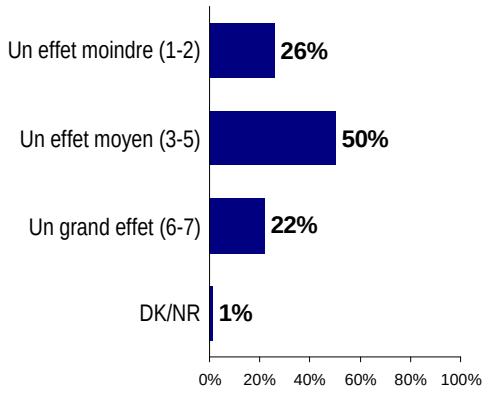
n=1672

Sondage de SP sur la cybersécurité, 2018

Parmi les 56 pour cent qui disent avoir été la victime d'un virus, d'un logiciel espion ou d'un logiciel malveillant, une personne sur cinq (22 p. cent) indique que l'attaque a eu une grande incidence. La moitié (50 p. cent, comparativement à 57 p. cent en 2016) estime que l'incidence était moyenne et le quart (26 p. cent, comparativement à 20 p. cent en 2016) indique que les conséquences ont été mineures.

Graphique 30 : Incidence des attaques informatiques

[SI OUI] « Quelle sorte d'effet ce virus, logiciel espion ou logiciel malveillant a-t-il eu sur vous ou votre famille? »



Les Associés de recherche EKOS

n=944

Sondage de SP sur la cybersécurité, 2018

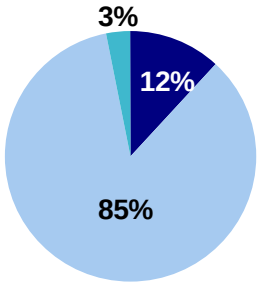
- Les hommes ont plus tendance que les femmes à affirmer avoir été victimes d'un virus, d'un logiciel espion ou d'un logiciel malveillant sur leurs appareils.
- Les Canadiens des Prairies sont plus susceptibles que ceux des autres régions à dire avoir été victimes d'une attaque, mais également plus enclins à considérer comme faibles les conséquences de l'incident. À l'inverse, les résidents du Québec sont moins susceptibles de signaler un incident, mais plus enclins à considérer les conséquences comme graves.
- Ceux dont le revenu est plus faible (40 000 dollars ou moins) ont plus tendance à dire que l'attaque a eu de graves conséquences.

7.2 FRÉQUENCE ET CONSÉQUENCES DES PERTES FINANCIÈRES

La proportion de Canadiens ayant subi des pertes financières à cause d'une activité en ligne s'est accrue, passant de six pour cent en 2011 à 12 p. cent en 2016 et en 2018. Quand même, la majorité, soit 85 pour cent, déclare ne pas avoir été victime d'un incident de fraude ou d'une attaque entraînant une perte financière.

Graphique 31 : Fréquence des pertes financières

« Avez-vous déjà subi des pertes financières ou été victime d'une fraude financière par suite d'une activité en ligne? »



	2016	2011
Oui	12%	6%
Non	84%	91%
NSP/PDR	4%	3%

Les Associés de recherche EKOS

n=2072

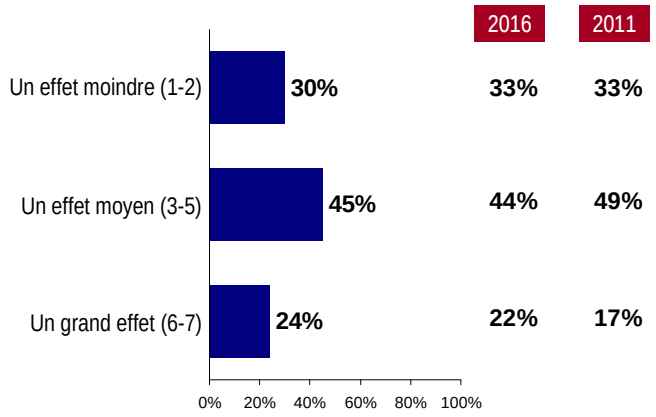
Sondage de SP sur la cybersécurité, 2018

- Les plus jeunes Canadiens (18 à 25 ans) et ceux à plus faible revenu font plus souvent état d'une perte financière que les autres Canadiens.

Le quart des répondants (24 p. cent, une augmentation par rapport aux 22 p. cent de 2016 et aux 17 p. cent de 2011) qui ont dû composer avec une perte financière affirme que la fraude a eu de graves conséquences. Moins de la moitié d'entre eux (45 p. cent) indique que l'impact a été modéré, et trois personnes sur dix (30 p. cent) disent que les conséquences ont été mineures.

Graphique 32 : Conséquences des pertes financières

[SI OUI] « Quelle sorte d'effet cette fraude financière par suite d'une activité en ligne a-t-elle eu sur vous ou votre famille? »



Les Associés de recherche EKOS

n=274

Sondage de SP sur la cybersécurité, 2018

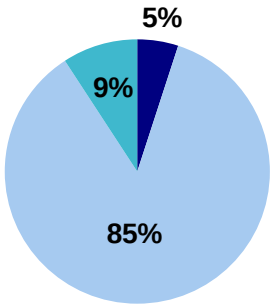
- Les Canadiens dont le revenu est plus faible (40 000 dollars ou moins) ont plus tendance à dire que la fraude financière a eu de graves conséquences.

7.3 FRÉQUENCE ET CONSÉQUENCES DES VOLS D'IDENTITÉ

Une faible minorité des Canadiens (5 p. cent) dit avoir été victimes d'un vol d'identité à la suite d'activités menées en ligne. La plupart des répondants (85 p. cent) n'ont jamais vécu un vol d'identité, bien que neuf pour cent affirment ne pas en être convaincus.

Graphique 33 : Fréquence des vols d'identité

« Avez-vous déjà été victime d'un vol d'identité par suite d'une activité en ligne? »



	2016	2011
Oui	5%	2%
Non	86%	88%
NSP/PDR	9%	9%

Les Associés de recherche EKOS

n=2072

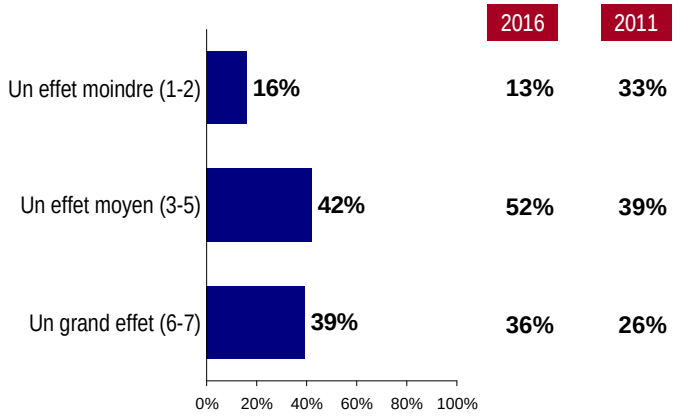
Sondage de SP sur la cybersécurité, 2018

- Les plus jeunes Canadiens (18 à 25 ans) sont plus enclins à affirmer avoir été victimes d'un vol d'identité.

Parmi la faible proportion de Canadiens qui signalent un vol d'identité, près de quatre personnes sur dix (39 p. cent) déclarent que cela a de graves conséquences. Une proportion semblable considère les conséquences comme modérées (42 p. cent) et 16 pour cent croient que les conséquences sont mineures. Il faut faire preuve de prudence au moment de comparer les résultats avec des périodes antérieures compte tenu de la taille relativement petite de l'échantillon.

Graphique 34 : Conséquences des vols d'identité

[SI OUI] « Quelle sorte d'effet le vol de votre identité a-t-il eu sur vous ou votre famille? »



Les Associés de recherche EKOS

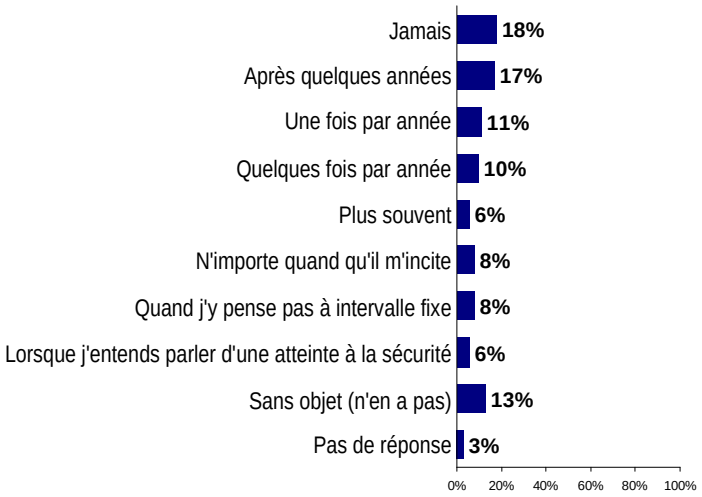
n=118

Sondage de SP sur la cybersécurité, 2018

Les répondants ont été informés du fait que bien des gens utilisent les mêmes mots de passe pour différents comptes et appareils, et que plusieurs d'entre eux conservent les mêmes mots de passe au fil du temps. En ce qui concerne leurs propres comptes de médias sociaux, un peu moins d'un répondant sur cinq déclare ne jamais modifier son mot de passe (18 p. cent) ou le faire une fois toutes les quelques années (17 p. cent). Une personne sur dix modifie plus assidûment ses mots de passe une fois par année (11 p. cent) ou quelques fois par année (10 p. cent). Moins d'un répondant sur dix modifie ses mots de passe plus de quelques fois par année (6 p. cent), lorsqu'on l'invite à le faire (8 p. cent), lorsqu'il y pense (8 p. cent) ou lorsqu'il a vent d'une brèche de sécurité (6 p. cent).

Graphique 35 : Modifications de mots de passe – Médias sociaux

« Bien des gens utilisent les mêmes mots de passe pour différents comptes et appareils, et conservent les mêmes mots de passe au fil du temps. À quelle fréquence diriez-vous que vous modifiez un mot de passe dans vos comptes de médias sociaux? »



Les Associés de recherche EKOS

n=1050 (demi échantillon)

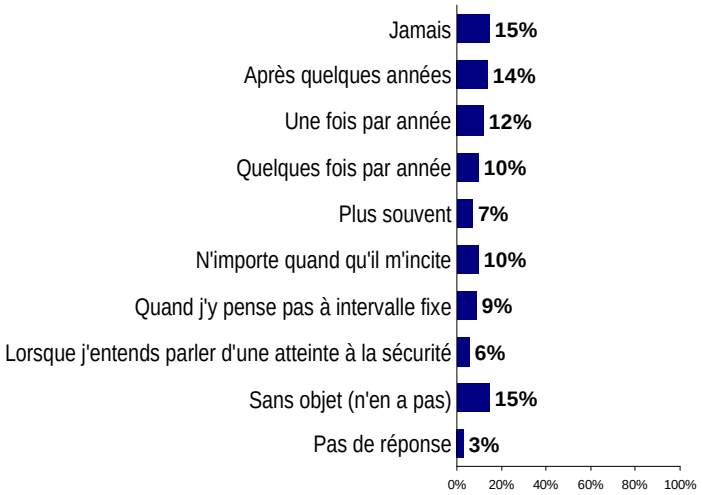
Sondage de SP sur la cybersécurité, 2018

- Les jeunes Canadiens sont plus susceptibles que ceux âgés de 25 ans et plus à déclarer modifier les mots de passe de leurs comptes de médias sociaux lorsqu'ils entendent parler d'une brèche de sécurité.
- Les gens qui ont fait des études secondaires ou moins ont tendance à affirmer qu'ils modifient les mots de passe de leurs comptes de médias sociaux quelques fois par année ou plus souvent que quelques fois par année.

Lorsqu'ils prennent en compte leurs comptes de magasinage en ligne, un peu moins d'un répondant sur cinq déclare ne jamais modifier son mot de passe (15 p. cent) ou le faire une fois toutes les quelques années (14 p. cent). Une personne sur dix modifie ses mots de passe une fois par année (12 p. cent) ou quelques fois par année (10 p. cent). Une faible proportion modifie ses mots de passe plus que quelques fois par années (7 p. cent). Un répondant sur dix ou moins ne respecte pas un calendrier pour modifier les mots de passe de ses comptes de magasinage en ligne et le fait lorsqu'on l'invite à le faire (10 p. cent), lorsqu'il y pense (9 p. cent) ou lorsqu'il apprend l'existence d'une brèche de sécurité (6 p. cent).

Graphique 36 : Modifications de mots de passe – Magasinage en ligne

« Bien des gens utilisent les mêmes mots de passe pour différents comptes et appareils, et conservent les mêmes mots de passe au fil du temps. À quelle fréquence diriez-vous que vous modifiez un mot de passe dans vos comptes de magasinage en ligne? »



Les Associés de recherche EKOS

n=1050 (demi échantillon)

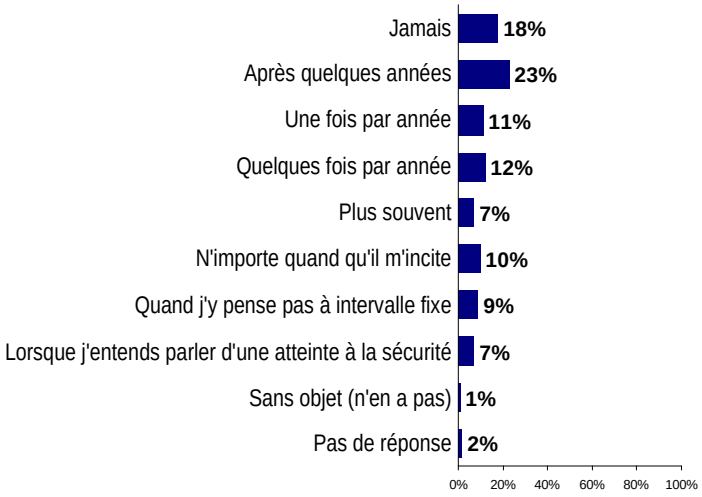
Sondage de SP sur la cybersécurité, 2018

- Comme dans le cas des médias sociaux, les jeunes Canadiens sont plus enclins à modifier les mots de passe de leurs comptes de magasinage en ligne lorsqu'ils entendent parler d'une brèche de sécurité.
- Les gens qui ont fait des études secondaires ou moins ont tendance à affirmer qu'ils modifient les mots de passe de leurs comptes de magasinage en ligne quelques fois par année ou plus souvent que quelques fois par année.

Un Canadien sur cinq (18 p. cent) affirme ne jamais modifier les mots de passe de ses comptes de courriels. Le quart des répondants (23 p. cent) modifie ses mots de passe une fois toutes les quelques années alors qu'une personne sur dix le fait une fois par année (11 p. cent) ou quelques fois par année (12 p. cent). Sept pour cent changent les mots de passe de leurs comptes de courriels plus souvent que quelques fois par année. À l'instar des tendances de modification des autres mots de passe, un répondant sur dix ou moins ne respecte pas un calendrier pour modifier ses mots de passe de comptes de courriels et le fait lorsqu'on l'invite à le faire (10 p. cent), lorsqu'il y pense (9 p. cent) ou lorsqu'il apprend l'existence d'une brèche de sécurité (7 p. cent).

Graphique 37 : Modifications de mots de passe – Courriels

« Bien des gens utilisent les mêmes mots de passe pour différents comptes et appareils, et conservent les mêmes mots de passe au fil du temps. À quelle fréquence diriez-vous que vous modifiez un mot de passe dans vos comptes de courriel? »



Les Associés de recherche EKOS

n=1050 (demi échantillon)

Sondage de SP sur la cybersécurité, 2018

- Comme dans le cas des modifications des mots de passe des comptes de magasinage en ligne, les jeunes Canadiens sont plus enclins à modifier leurs mots de passe lorsqu'ils entendent parler d'une brèche de sécurité. Les 55 ans et plus sont plus susceptibles de ne jamais modifier les mots de passe de leurs comptes de courriels.
- Les gens qui ont fait des études secondaires ou moins ont plus tendance à modifier les mots de passe de leurs comptes de courriels quelques fois par année ou plus souvent que quelques fois par année.

8. INFORMATION ET RESPONSABILITÉS

La présente section porte sur les besoins d'information et renferme des renseignements sur les sources auxquelles se fient les Canadiens pour obtenir de l'information impartiale, fiable et à jour. Les Canadiens continuent de chercher à obtenir de l'information sur les menaces en ligne. La majorité des Canadiens est toujours d'accord pour dire que l'information peut les aider à se protéger en ligne et estime que la sécurité des appareils personnels en ligne est une responsabilité qui revient aux propriétaires des appareils. Par ailleurs, ils continuent de consulter des organismes d'application de la loi et le gouvernement pour obtenir l'information dont ils ont besoin pour s'acquitter de ces responsabilités.

8.1 INFORMATION RECHERCHÉE

La plupart des Canadiens recherchent de l'information sur les types de menaces qui existent en ligne. Seuls trois répondants sur dix (26 p. cent, une légère baisse par rapport aux 30 p. cent de 2016) disent ne pas rechercher d'information. Près de la moitié d'entre eux (48 p. cent) recherche de l'information sur la protection des appareils avec un logiciel antivirus. Quatre personnes sur dix en recherchent sur les façons de sécuriser les réseaux domestiques et les réseaux sans fil (38 p. cent) ou sur les façons de savoir si un courriel est frauduleux (38 p. cent). Trois sur dix (30 p. cent) recherchent des mesures à prendre pour protéger les fichiers de leur ordinateur. Le quart recherche de l'information sur les façons de protéger leurs appareils mobiles (26 p. cent) ou les mesures à prendre pour utiliser en toute sécurité des sites de réseautage social (24 p. cent). Une personne sur cinq ou moins recherche de l'information sur l'utilisation sécuritaire de réseaux sans fil publics (20 p. cent), sur les mesures à prendre pour protéger d'autres appareils connectés (17 p. cent) ou sur la cyberintimidation et le harcèlement en ligne (15 p. cent). Un répondant sur dix s'informe sur la sécurité des enfants (11 p. cent) ou des aînés (10 p. cent) sur Internet. Plus de Canadiens recherchent de l'information sur chaque type de menace en ligne qu'en 2016.

Graphique 38 : Information recherchée

« Sur quels types de menaces en ligne parmi les suivantes avez-vous recherché des renseignements, s'il y a lieu? »

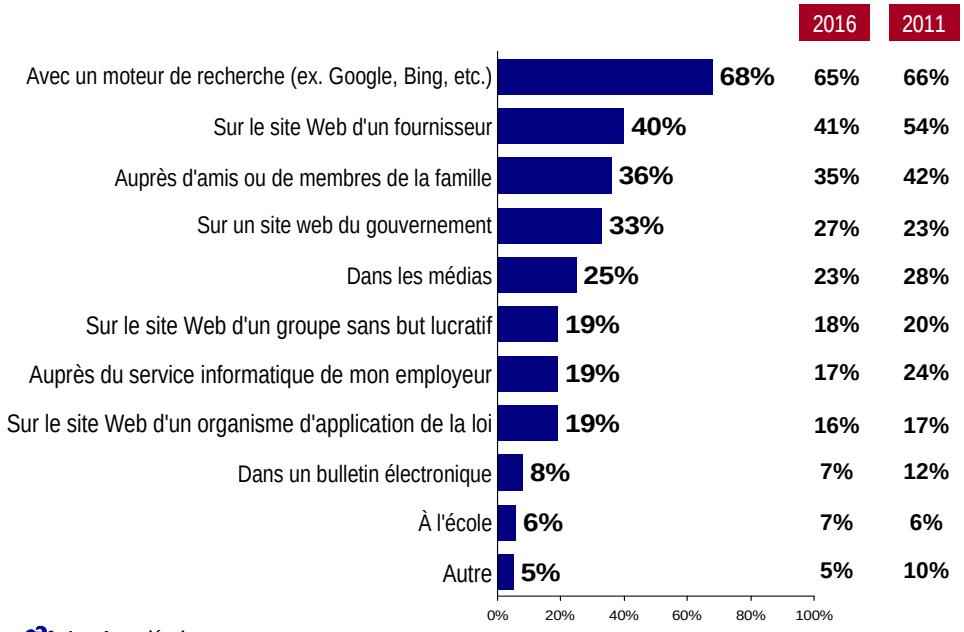
- Les jeunes Canadiens sont plus enclins que ceux âgés à rechercher de l'information sur la cyberintimidation ainsi que sur les mesures à prendre pour utiliser des réseaux sans fil publics et des sites de médias sociaux en toute sécurité, et pour protéger des appareils mobiles. Les Canadiens plus âgés (65 ans et plus) ont plus tendance à rechercher des renseignements sur la sécurité des aînés sur Internet.
- Les hommes sont plus susceptibles que les femmes de rechercher de l'information sur la plupart des domaines mentionnés.
- Les résidents du Québec sont moins enclins que les autres Canadiens à rechercher de l'information sur la plupart des domaines évoqués.
- La propension à chercher à obtenir de l'information augmente avec le niveau de scolarité.

En harmonie avec les résultats des autres sondages menés antérieurement, les Canadiens sont plus susceptibles de recourir à des moteurs de recherche pour rechercher de l'information au sujet des menaces en ligne (68 p. cent). Quatre répondants sur dix consultent le site Web d'un vendeur (40 p. cent, semblable aux 41 p. cent de 2016, mais en baisse par rapport aux 54 p. cent de 2011). Les amis et la famille sont cités comme une source d'information par

36 pour cent des répondants. L'utilisation de sites Web du gouvernement semble être une source d'information de plus en plus prisée, le tiers des répondants (33 p. cent) affirmant qu'il en visiterait un, une proportion plus élevée qu'en 2016 (27 p. cent) et 2011 (23 p. cent). Le quart (25 p. cent) dit utiliser les médias traditionnels comme source d'information. Une personne sur cinq déclare utiliser le site Web d'un organisme sans but lucratif (19 p. cent), le service des TI d'un employeur (19 p. cent) ou le site Web d'un organisme d'application de la loi (19 p. cent).

Graphique 39 : Sources d'information

« Où êtes-vous allé chercher cette information? »



Les Associés de recherche EKOS

n=1038 (a cherché l'information)

Sondage de SP sur la cybersécurité, 2018

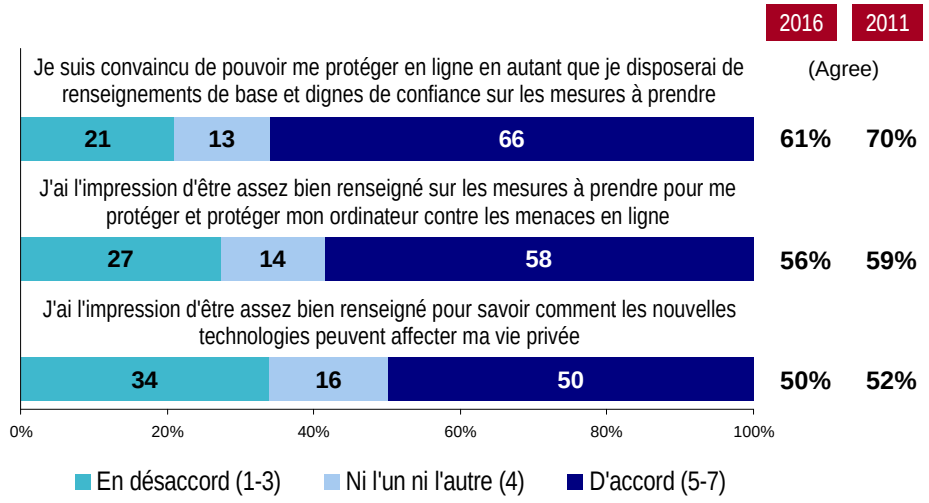
- Les moins de 25 ans sont beaucoup plus enclins à affirmer avoir obtenu de l'information à l'école (24 p. cent par rapport à 6 p. cent pour l'ensemble des répondants).
- Les hommes ont plus tendance que les femmes à trouver de l'information par le biais d'un moteur de recherche, du site Web d'un vendeur, des médias, du site Web d'un organisme sans but lucratif ou d'un bulletin. Les femmes ont plus tendance que les hommes à affirmer obtenir de l'information auprès d'amis et de membres de leur famille.
- Les gens dont le niveau de scolarité et le revenu sont plus élevés sont plus susceptibles d'avoir recours au service des TI d'un employeur pour obtenir des renseignements. Ceux qui ont fait des études universitaires sont également plus enclins à utiliser un moteur de recherche ou le site Web d'un organisme sans but lucratif.

8.2 ATTITUDES – PROTECTION CONTRE LES RISQUES EN LIGNE

Deux Canadiens sur trois (66 p. cent) se disent convaincus de pouvoir se protéger en ligne tant qu'ils disposeront des renseignements de base dignes de confiance au sujet des mesures à prendre. Cette proportion est plus élevée que les 61 pour cent de 2016 et demeure sous le taux de confiance de 70 pour cent obtenu en 2011. Plus de la moitié des Canadiens (58 p. cent, semblable aux 56 p. cent de 2016 et aux 59 p. cent de 2011) sont d'accord pour dire qu'ils sont assez bien renseignés pour savoir quelles mesures prendre pour se protéger, bien que le quart (27 p. cent) ne soit pas d'accord avec cet énoncé. Dans un même ordre d'idées, la proportion de Canadiens qui croient posséder assez d'information sur la façon dont les nouvelles technologies peuvent exercer une incidence sur la protection de leur vie privée demeure à peu de choses près la même qu'en 2016, 50 pour cent étant d'accord contre une proportion notable de 34 pour cent qui se dit en désaccord.

Graphique 40 : Attitudes – Protection contre les menaces en ligne

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



Les Associés de recherche EKOS

n=2072

Sondage de SP sur la cybersécurité, 2018

- Les Canadiens âgés de 44 ans ou moins et les hommes ont généralement plus tendance à être d'accord avec les trois énoncés.
- Les gens dont le revenu est plus élevé sont plus susceptibles de croire qu'ils possèdent suffisamment d'information sur la façon dont les nouvelles technologies peuvent exercer une incidence sur la protection de leur vie privée et sur les façons de se protéger contre les menaces en ligne.

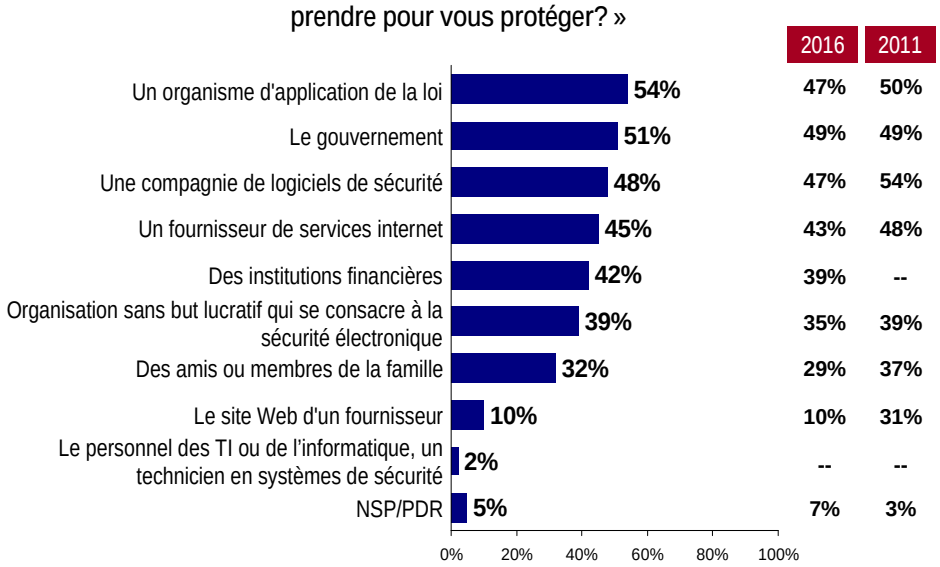
8.3 ORGANISATIONS DIGNES DE CONFIANCE POUR L'OBTENTION D'INFORMATION

Un peu plus de la moitié des Canadiens dit se fier aux organismes d'application de la loi (54 p. cent, une augmentation par rapport aux 47 p. cent de 2016) ou au gouvernement (51 p. cent) pour obtenir l'information la plus fiable techniquement et la plus à jour sur les menaces en ligne et sur les mesures à prendre pour se protéger. Moins de la moitié se fie aux entreprises de logiciel de sécurité (48 p. cent), aux fournisseurs de services Internet (45 p. cent) ou aux institutions financières (42 p. cent). Quatre personnes sur dix (39 p. cent) se fient aux organismes sans but lucratif œuvrant dans le domaine de la sécurité électronique. Le tiers des répondants (32 p. cent) se fie aux amis et à la famille, alors que cette proportion passe à dix pour cent dans le cas du site Web de vendeurs. Deux pour cent se fient aux techniciens en TI ou en sécurité informatique (cette réponse ne faisait pas partie des versions antérieures).

C'est la première fois que les organismes d'application de la loi atteignent la tête du classement, alors que les entreprises de logiciel de sécurité sont passées de la première place en 2011 au troisième échelon en 2018.

Graphique 41 : Organisations dignes de confiance pour l'obtention d'information

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



Les Associés de recherche EKOS

n=2072

Sondage de SP sur la cybersécurité, 2018

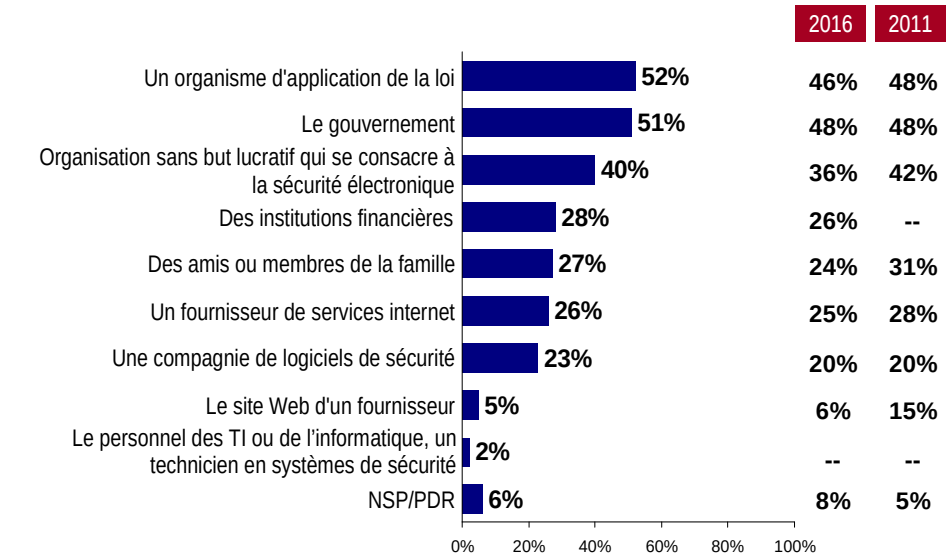
- L'âge est un facteur lorsqu'il est question du niveau de confiance que suscitent diverses sources. Les Canadiens âgés (65 ans ou plus) sont plus susceptibles d'estimer que leurs amis et leurs proches, leur fournisseur de services Internet et les institutions financières sont dignes de confiance pour obtenir de l'information. Les gens âgés de 25 à 54 ans sont plus susceptibles à se fier à des organismes sans but lucratif que les autres groupes d'âge. Les jeunes Canadiens (moins de 24 ans) sont plus enclins à se fier au site Web d'un vendeur, comme une boutique en ligne.
- Les hommes ont plus tendance que les femmes à se fier à une entreprise de logiciel de sécurité, à un organisme sans but lucratif ou au site Web d'un vendeur. Les femmes sont plus enclines à se fier aux organismes d'application de la loi, au gouvernement ainsi qu'à des amis et à des membres de leur famille.
- Les gens dont le niveau de scolarité et le revenu sont plus élevés sont plus susceptibles de se fier aux organismes sans but lucratif.

8.4 ORGANISATIONS IMPARTIALES POUR L'OBTENTION DE L'INFORMATION

Les services publics figurent toujours en tête de liste des organisations auxquelles se fient le plus les répondants pour obtenir des renseignements impartiaux sur les menaces en ligne et sur les mesures à prendre pour assurer leur protection personnelle. Environ la moitié des répondants se fie aux organismes d'application de la loi (52 p. cent, une hausse par rapport aux 56 p. cent de 2016) ou au gouvernement (51 p. cent) pour obtenir des renseignements impartiaux. Les organismes sans but lucratif ont la confiance de quatre répondants sur dix (40 p. cent, une légère hausse par rapport aux 36 p. cent de 2016). Environ le quart dit se fier aux institutions financières (28 p. cent), aux amis et à la famille (27 p. cent), aux fournisseurs de services Internet (26 p. cent) ou aux entreprises de logiciel de sécurité (32 p. cent).

Graphique 42 : Organisations impartiales pour l'obtention de l'information

« À qui vous fieriez-vous pour recevoir les renseignements les plus impartiaux sur les menaces en ligne et les mesures que vous pouvez prendre pour vous protéger? »



Les Associés de recherche EKOS

n=2072

Sondage de SP sur la cybersécurité, 2018

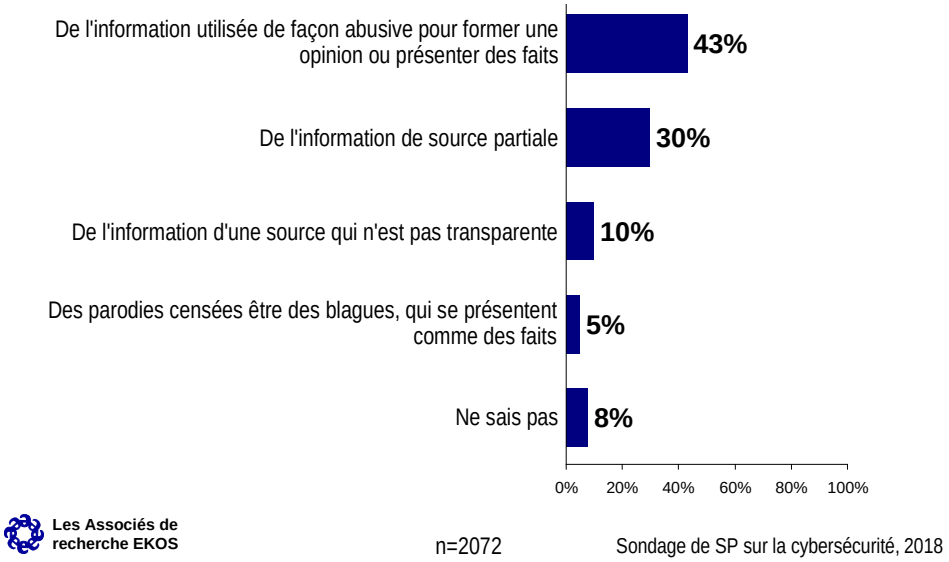
- Comme dans le cas des sources considérées comme dignes de confiance, l'âge est un facteur lorsqu'il est question de sources impartiales. Les Canadiens âgés (65 ans ou plus) sont plus susceptibles d'estimer que leurs amis et leurs proches, leur fournisseur de services Internet, les institutions financières et les entreprises de logiciel de sécurité sont des sources impartiales. Les gens âgés de 25 à 54 ans sont plus susceptibles que les autres groupes d'âge de croire que les organismes sans but lucratif sont impartiaux. Les jeunes Canadiens (moins de 25 ans) sont plus enclins à nommer le site Web de vendeurs comme une source impartiale.
- Les hommes ont plus tendance que les femmes à se fier à une institution financière, à un fournisseur de services Internet, à une entreprise de logiciel de sécurité ou à un organisme sans but lucratif. Les femmes sont plus enclines à se fier aux organismes d'application de la loi ainsi qu'à des amis et à des membres de leur famille.
- Les gens dont le niveau de scolarité et le revenu sont plus élevés sont plus susceptibles de se fier aux gouvernements et aux organismes sans but lucratif. Les diplômés universitaires sont également plus enclins à se fier à des organismes d'application de la loi.

8.5 Comprendre les « Fausses nouvelles »

Lorsqu'il est question de « fausses nouvelles » en lien avec les renseignements dont les gens ont besoin pour assurer leur protection, environ quatre Canadiens sur dix (43 p. cent) sont d'avis que cela fait allusion à de l'information qui est faussement utilisée pour façonner des opinions ou des faits. Trois répondants sur dix (30 p. cent) croient que les « fausses nouvelles » sont des renseignements qui proviennent d'une source partiale, alors qu'une personne sur dix (10 p. cent) affirme qu'il s'agit d'information provenant d'une source qui n'est pas transparente. Peu de gens (5 p. cent) déclarent qu'ils considèrent les « fausses nouvelles » comme des parodies qui sont à la base des blagues, mais qui sont présentées comme des faits. Huit pour cent sont incertains.

Graphique 43 : Fausses nouvelles

« Quand quelqu'un parle de « fausses nouvelles » dans le contexte de l'information dont les gens ou les clients ont besoin pour se protéger, à votre avis, est-ce que ces fausses nouvelles désignent habituellement…? »

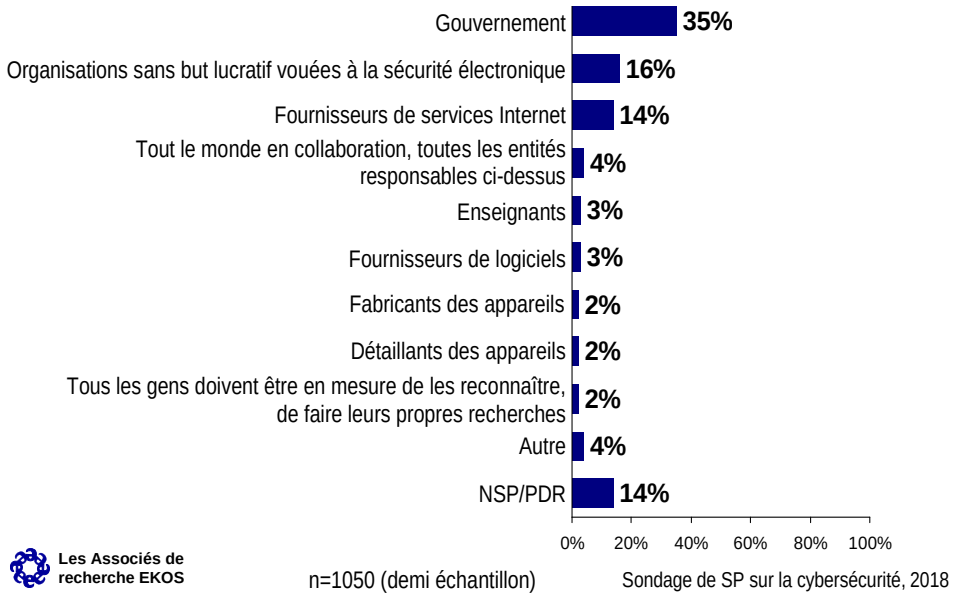


- Les jeunes Canadiens (moins de 24 ans) et les résidents du Québec sont plus enclins à déclarer que les « fausses nouvelles » sont de l'information provenant d'une source qui n'est pas transparente ou qu'il s'agit d'une parodie.

Le tiers des répondants (35 p. cent) croit que le gouvernement devrait avoir un rôle à jouer pour aider les Canadiens à reconnaître ce que sont les « fausses nouvelles » lorsqu'elles traitent d'informations sur des menaces en ligne et sur la protection du consommateur. Plus d'une personne sur dix affirme que les organismes sans but lucratif qui se consacrent à la sécurité électronique (16 p. cent) ou les fournisseurs de services Internet (14 p. cent) ont un rôle à jouer. Un éventail d'autres sources sont mentionnées, y compris le travail commun de tout le monde (4 p. cent), les enseignants (3 p. cent), les fournisseurs de logiciels (3 p. cent), les fabricants d'appareils (2 p. cent), les détaillants d'appareils (2 p. cent), ou le fait que les gens devraient pouvoir discerner et mener leurs propres recherches (2 p. cent). Quatorze pour cent des répondants ne savent pas qui devrait jouer un rôle.

Graphique 44 : Sources aidant à reconnaître une fausse nouvelle

« Qui devrait jouer un rôle pour aider les Canadiens à reconnaître ce qui constitue des « fausses nouvelles » pour ce qui concerne l'information au sujet des menaces en ligne et la protection des clients? »



- Les Canadiens âgés (55 ans et plus) sont plus enclins à affirmer que les fournisseurs de services Internet devraient avoir un rôle à jouer. Les jeunes Canadiens ont plus tendance à nommer le gouvernement.
- Les résidents du Québec sont plus susceptibles que ceux des autres régions à croire que le gouvernement a un rôle à jouer.

8.6 RESPONSABILITÉ EN CE QUI CONCERNE LA SÉCURITÉ DES APPAREILS

La plupart des Canadiens (67 p. cent) sont d'avis que la responsabilité en ce qui concerne la sécurité des appareils dotés d'une connexion à Internet revient aux particuliers à qui appartiennent ces appareils, une légère baisse par rapport à 2011 (70 p. cent), mais une proportion semblable à celle de 2016 (66 p. cent). D'autres sources font l'objet d'une mention un peu plus souvent que dans les sondages antérieurs, y compris les fournisseurs de services Internet (30 p. cent), les fabricants d'appareils (33 p. cent), les fournisseurs de logiciels (31 p. cent) et le gouvernement (31 p. cent). Seize pour cent croient que les détaillants d'appareils ont une responsabilité en ce qui a trait à la sécurité des appareils. Une personne sur dix déclare que le secteur privé (10 p. cent) ou les organismes sans but lucratif qui œuvrent dans le domaine de la sécurité électronique (10 p. cent) doivent être tenus responsables.

Graphique 45 : Responsabilité en ce qui concerne la sécurité des appareils

« D'après vous, qui a principalement la responsabilité de voir à ce que les appareils personnels dont se servent les Canadiens pour accéder à internet sont sûrs et sécuritaires? »

Les Associés de recherche EKOS

n=2072

Sondage de SP sur la cybersécurité, 2018

- Tout comme en 2016, les résidents du Québec sont moins susceptibles que les autres Canadiens d'affirmer que les propriétaires des appareils sont responsables de veiller à la sécurité de leurs appareils. Toutefois, ils sont beaucoup plus susceptibles d'affirmer que les autres intervenants (exception faite du secteur privé), et en particulier le gouvernement, ont la principale responsabilité à cet égard.
- La perception voulant que les fournisseurs de services Internet soient principalement responsables de veiller à la sécurité des appareils est toujours beaucoup plus répandue chez les Canadiens plus âgés (55 ans ou plus).
- Fait intéressant, les répondants qui avaient entre 25 et 34 en 2011 sont plus susceptibles d'affirmer que les particuliers sont responsables de la sécurité de leurs appareils. En 2016 et en 2018, les Canadiens de 35 à 44 ans sont beaucoup plus enclins à être d'accord avec ce point de vue que les répondants de 25 à 34 ans et que les répondants de moins de 25 ans. Cela pourra révéler un changement générationnel, étant donné que les membres du groupe des 25 à 34 ans en 2011 ont désormais 35 à 44 ans. Les membres du groupe le plus jeune (les 18 à 24 ans) sont les moins susceptibles de croire que les propriétaires d'appareils devraient être les principaux responsables.
- Comme ce fut le cas dans les éditions antérieures, les répondants faisant état des revenus les plus élevés sont beaucoup plus susceptibles que les autres répondants d'estimer que les particuliers sont les principaux responsables de la sécurité de leurs appareils.

9. PRÉOCCUPATIONS DES PARENTS

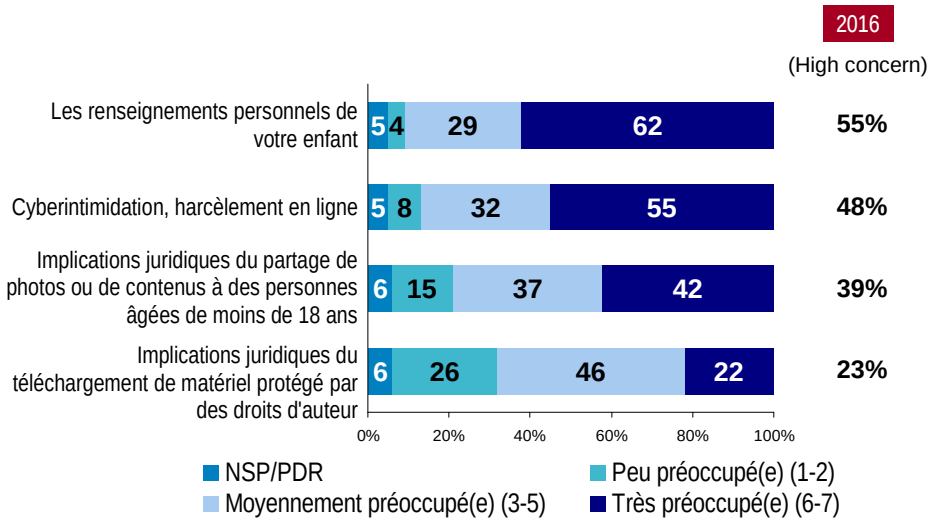
La présente section met en évidence des préoccupations précises que partagent les parents canadiens en ce qui a trait aux activités en ligne de leurs enfants. Les résultats révèlent que les parents se préoccupent davantage de la protection des renseignements personnels de leurs enfants et du bien-être de leurs enfants en général que des implications juridiques associées à ces activités. Dans le cas des parents qui ne sont pas préoccupés, nous observons une scission entre ceux qui prennent des mesures pour se renseigner et renseigner leurs enfants dans ce domaine et ceux qui sont convaincus que leurs enfants feront leurs propres démarches de surveillance pour éviter des menaces précises en ligne.

9.1 PRÉOCCUPATIONS CHEZ LES PARENTS

Six parents sur dix (62 p. cent) sont préoccupés par la protection de la vie privée de leurs enfants lorsqu'ils sont en ligne. Un peu plus de la moitié se dit préoccupée par la cyberintimidation et le harcèlement en ligne (55 p. cent). Environ quatre personnes sur dix ont également des préoccupations par rapport aux conséquences liées au partage de photos de personnes âgées de moins de 18 ans (42 p. cent), bien qu'elles soient beaucoup moins nombreuses à se soucier des conséquences juridiques du téléchargement par des enfants de matériel protégé par le droit d'auteur (22 p. cent).

Graphique 46 : Préoccupations chez les parents

« En tant que parent, à quel point êtes-vous préoccupé(e) par chacune des choses suivantes? »



Les Associés de recherche EKOS

n=600 (parents)

Sondage de SP sur la cybersécurité, 2018

- Les parents qui ont un diplôme universitaire se préoccupent généralement davantage que les autres parents des conséquences juridiques liées au partage de photos.
- Il y a des tendances régionales en ce qui concerne la façon dont les parents perçoivent les menaces en ligne, les parents vivant en Colombie-Britannique étant plus susceptibles de se préoccuper de la cyberintimidation et du harcèlement en ligne.
- Bien qu'il y ait des différences au niveau des genres, la cyberintimidation et la protection de la vie privée de leurs enfants préoccupent un peu plus les femmes que les hommes.

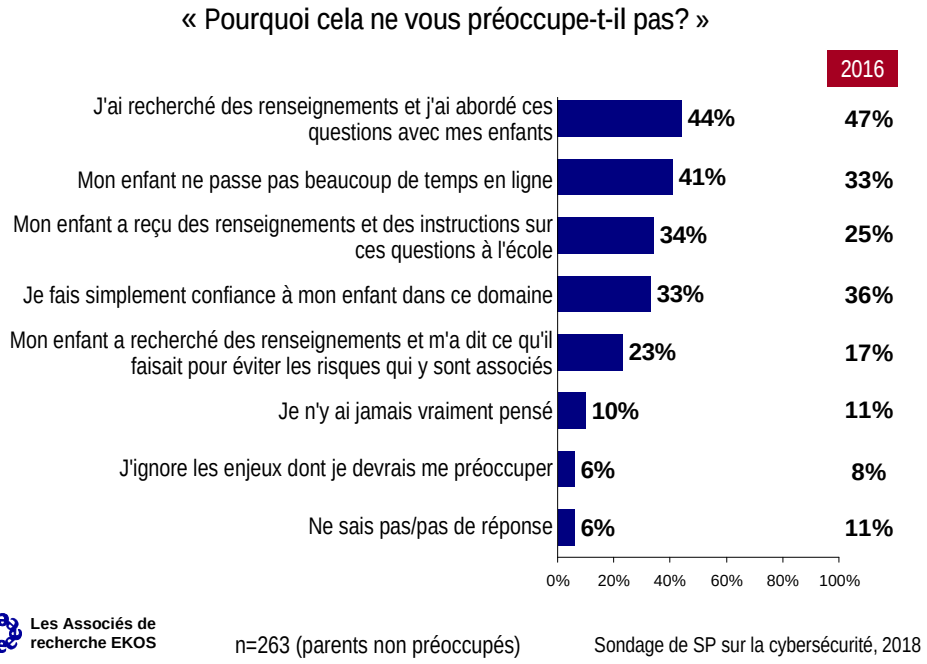
9.2 Raisons de ne pas être préoccupés

Chez les parents qui ne se préoccupent pas de l'exposition de leurs enfants à des menaces en ligne précises, la moitié environ (44 p. cent) explique que cela est lié au fait qu'ils ont cherché à obtenir de l'information sur le sujet et qu'ils ont discuté avec leurs enfants de certains enjeux. D'autres parents affirment que leurs enfants ont reçu les instructions et les renseignements sur ces enjeux (34 p. cent) ou ont confiance dans la capacité de leurs enfants à savoir quoi faire (33 p. cent). Un troisième segment répond que leur enfant n'est pas trop souvent en ligne (41 p. cent). Cette option est citée le plus souvent par les parents d'enfants de moins de 10 ans.

En grande majorité, ces parents cherchent à trouver de l'information eux-mêmes afin de pouvoir la communiquer à leurs enfants. Ils affirment que les écoles se chargent de renseigner les enfants à ce sujet ou ils sont convaincus que leurs enfants se sont renseignés eux-mêmes.

En comparaison avec 2016, il y a une augmentation notable dans la proportion de parents qui indiquent que leur enfant a reçu des informations et des instructions à l'école (25 p. cent à 34 p. cent).

Graphique 47 : Raisons de ne pas être préoccupés



- L'âge des enfants a un effet appréciable sur les raisons pour lesquelles les parents choisissent de ne pas se préoccuper de ces questions. Au moins la moitié des parents dont les enfants ont moins de six ans (75 p. cent) ou entre six et dix ans (58 p. cent) affirment ne pas se préoccuper de ces questions, car leurs enfants ne passent pas beaucoup de temps en ligne. Ce résultat chute considérablement chez les parents dont les enfants sont âgés de 11 à 15 ans (19 p. cent) ou de 16 ans ou plus (12 p. cent). Les parents d'enfants âgés de onze ans et plus sont plus enclins à avoir recherché des informations afin d'éduquer leurs enfants, à avoir confiance dans la capacité de leur enfant à savoir quoi faire ou à croire que leur enfant a cherché des renseignements ou en a reçu à l'école.

- Les parents qui ont fait des études universitaires sont plus susceptibles d'affirmer avoir recherché des renseignements pour éduquer leurs enfants.
- Les parents québécois ont plus tendance que ceux des autres régions du pays à déclarer ne pas avoir pensé à ces enjeux ou à ne pas en avoir conscience.

10. Expériences d'entreprises

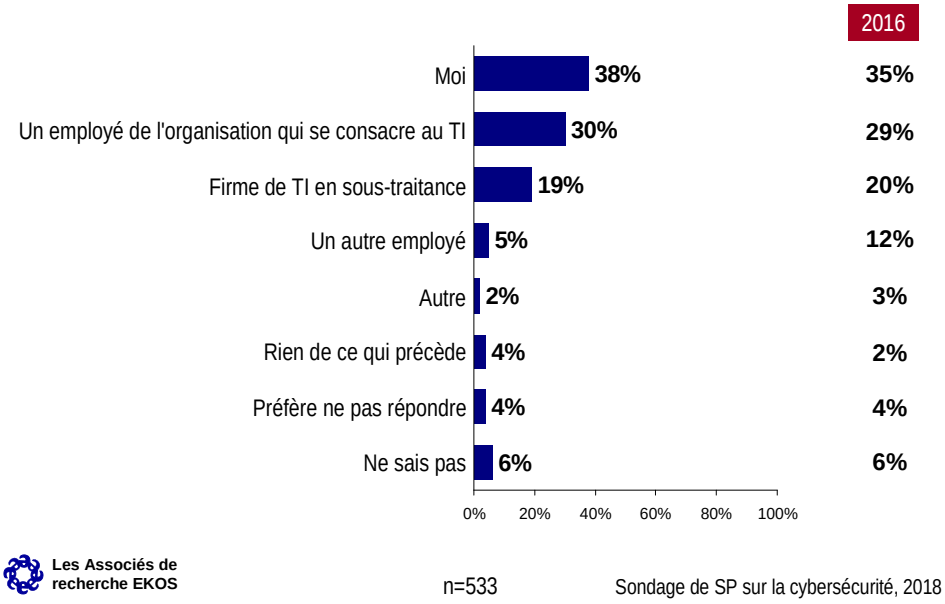
La présente section, qui traite exclusivement de propriétaires ou de dirigeants d'entreprise, aborde les préoccupations et perceptions de ce segment de la population à l'égard des menaces en ligne. Les résultats indiquent qu'en proportion considérable, les préoccupations des entreprises entretiennent un lien avec d'éventuelles interruptions de travail et avec des pertes financières attribuables aux menaces en ligne. Même si la majorité de ces entreprises prennent des mesures de précaution pour se protéger contre les menaces en ligne, un fort pourcentage de répondants estiment qu'il serait utile que les organisations soient éclairées au sujet des types particuliers de menaces et qu'elles reçoivent des directives sur la façon d'y faire face.

10.1 Responsabilités du service des TI

Fait dont il ne faut pas se surprendre, la taille de l'entreprise détermine en quelque sorte la personne qui est responsable des TI au sein des organisations. Un peu comme c'était le cas en 2016, les répondants de 38 pour cent des entreprises constituant l'échantillon affirment être la personne responsable des TI, ce qui témoigne de la forte concentration de petites entreprises dans l'échantillon. Dans les faits, pour 67 pour cent des entreprises comptant entre un et dix employés, le répondant était aussi la personne responsable des TI. En revanche, de 69 à 73 pour cent des sociétés ayant plus de 50 employés comptaient au sein de leur personnel une personne affectée particulièrement aux TI. Dans 19 pour cent des cas, les répondants indiquent que les TI sont confiées à une entreprise tierce.

Graphique 48 : Répondants du sondage

« Qui est responsable des TI de votre société? »



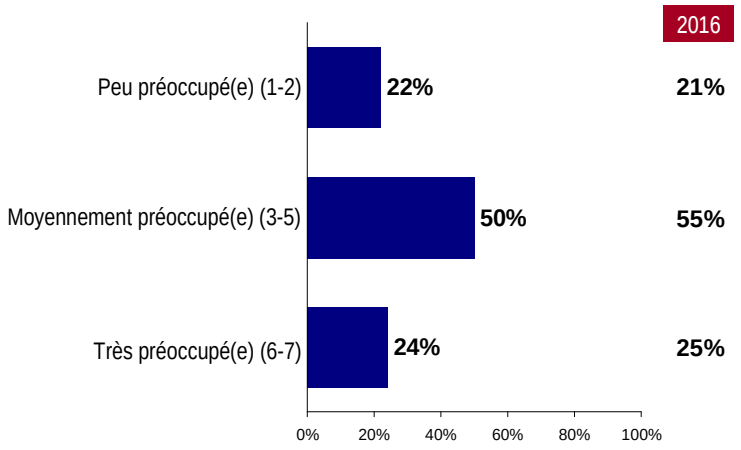
10.2 PRÉOCCUPATION PAR RAPPORT AUX INTERRUPTIONS

Alors que la moitié des représentants d'entreprise affirment être moyennement préoccupés (50 p. cent), entre le quart et le cinquième des répondants se disent peu préoccupés ou très préoccupés, ce qui était également le cas en 2016. Les organisations comptant de 11 à 20 employés sont les plus préoccupées dans ce domaine, 37 p. cent des répondants affirmant se préoccuper des possibilités d'interruptions du travail ou de pertes consécutives en raison d'une menace en ligne (c.-à-d. 6 ou 7 sur une échelle de 7).

Dans les organisations dont les représentants sont peu préoccupés, un peu moins de la moitié des répondants estiment que le risque d'un incident en ligne est très faible (43 p. cent), tendance qui semble à la hausse par rapport à 2016, alors que cette proportion était de 33 pour cent. Trois personnes sur dix ont également confiance dans leurs recherches et dans leur préparation à de tels événements (30 p. cent). Il n'y a pas de différences perceptibles entre les entreprises de diverses tailles en ce qui a trait à la nature de la préoccupation, ce qui est dû en partie à la petite taille de l'échantillon.

Graphique 49 : Niveau de préoccupation dans les entreprises

« En ce qui concerne les diverses préoccupations liées à l'exploitation quotidienne de votre organisation, à quel point êtes-vous préoccupé(e) par les interruptions de travail ou les pertes financières relatives aux menaces en ligne? »



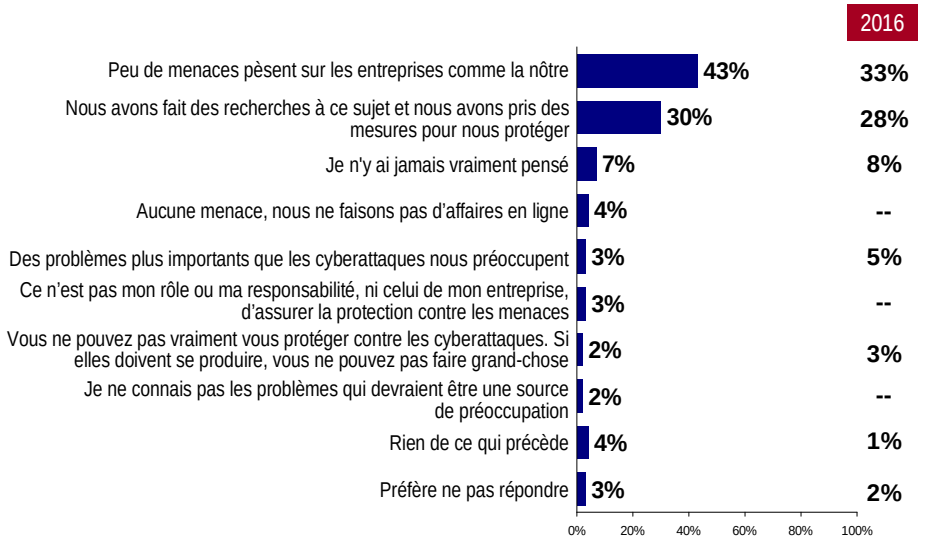
Les Associés de recherche EKOS

n=533

Sondage de SP sur la cybersécurité, 2018

Graphique 50 : Raison de l'absence de préoccupation

« Pourquoi est-ce le cas? »



Les Associés de recherche EKOS

n=195 (entreprises non préoccupées)

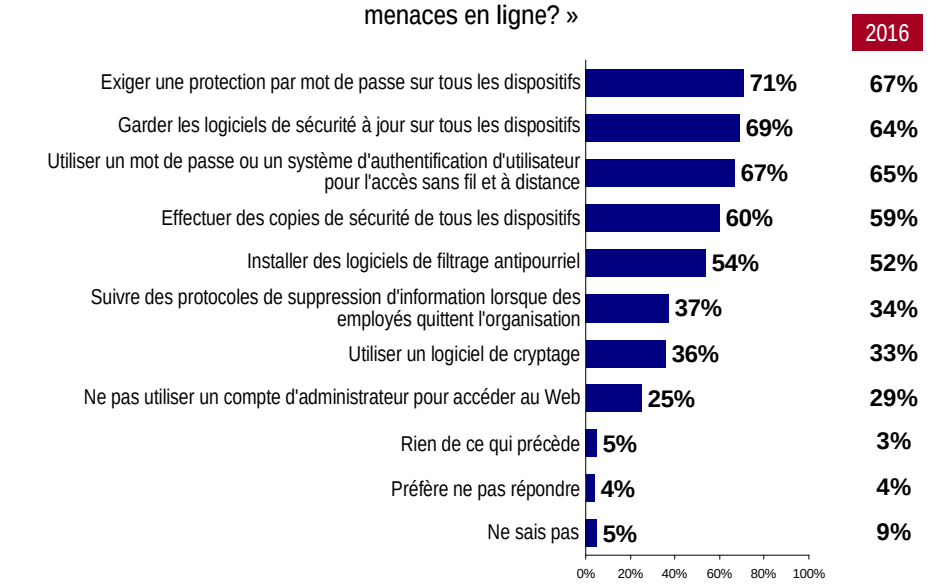
Sondage de SP sur la cybersécurité, 2018

10.3 MESURES DE PROTECTION CONTRE LES MENACES EN LIGNE

La plupart des entreprises canadiennes prennent des mesures de base pour se protéger contre les menaces en ligne. Environ sept entreprises sur dix exigent l'utilisation d'un mot de passe sur tous les appareils (71 p. cent), actualisent leur logiciel de sécurité (69 p. cent, une augmentation par rapport aux 64 p. cent de 2016) ou ont recours à une authentification par mot de passe pour l'accès à distance (67 p. cent). Comme en 2016, plus de la moitié des répondants effectuent des copies de sécurité (60 p. cent) ou installent des filtres antipourriel (54 p. cent). Les entreprises sont moins nombreuses à prendre des mesures plus exigeantes. Un peu plus du tiers d'entre elles suivent les protocoles de retrait d'information lorsque des employés quittent l'organisation (37 p. cent) ou utilisent un logiciel de chiffrement (36 p. cent). Le quart (25 p. cent) évite d'utiliser des comptes d'administrateur pour accéder au Web. Seuls cinq pour cent des répondants affirment explicitement ne prendre aucune des mesures de précaution abordées.

Graphique 51 : Mesures prises par des entreprises

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



Les Associés de recherche EKOS

n=533

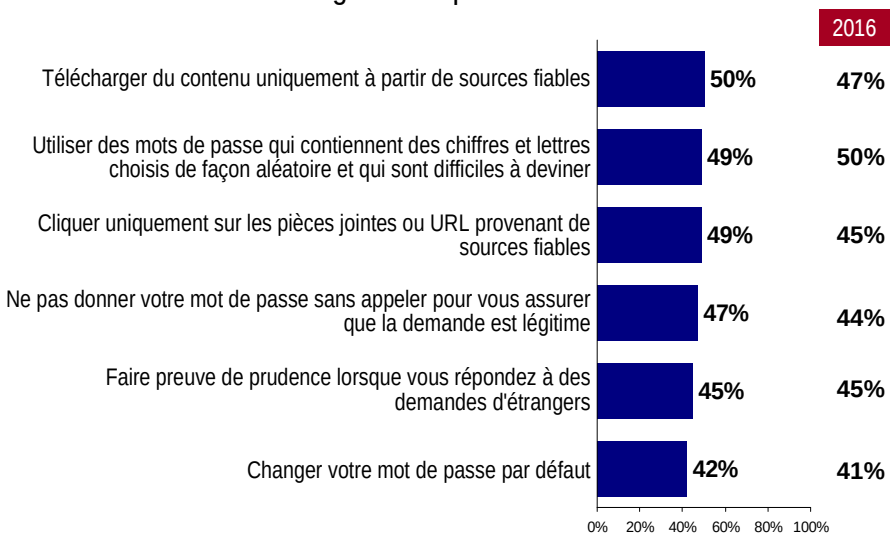
Sondage de SP sur la cybersécurité, 2018

- Les organisations qui ont des ressources internes dédiées aux TI, ainsi que celles qui confient à des tiers ces tâches, sont plus susceptibles de prendre toutes les mesures examinées.

Environ la moitié des entreprises demandent aussi à leurs employés de ne télécharger du contenu qu'à partir de sources dignes de confiance (50 p. cent), d'utiliser des mots de passe qui contiennent un mélange aléatoire de chiffres et de lettres (49 p. cent), de ne cliquer que sur les pièces jointes provenant de sources sures (49 p. cent), de faire preuve de prudence lorsqu'ils répondent à des étrangers (47 p. cent) ou de ne pas partager de mots de passe sans effectuer une vérification (47 p. cent). Quatre entreprises sur dix (42 p. cent) mettent l'accent sur la modification des mots de passe par défaut alors que le tiers (32 p. cent) ne permet pas aux navigateurs de retenir les mots de passe. Environ une entreprise sur quatre indique à ses employés d'utiliser un logiciel de chiffrement (27 p. cent), de consulter les politiques des sites Web en matière de protection de la vie privée (23 p. cent) ou de lire les conditions d'utilisation (22 p. cent). Une entreprise sur dix (11 p. cent) ne fournit pas à ses employés l'une ou l'autre de ces instructions et une sur cinq (22 p. cent) n'a pas fourni de réponse à cette question. Ces résultats sont en grande partie en harmonie avec ceux de 2016.

Graphique 52a : Instructions de sécurité précises à l'intention des employés

« Quelles instructions parmi les suivantes fournissez-vous aux employés pour protéger l'organisation contre les menaces en ligne et pour protéger vos renseignements personnels? »



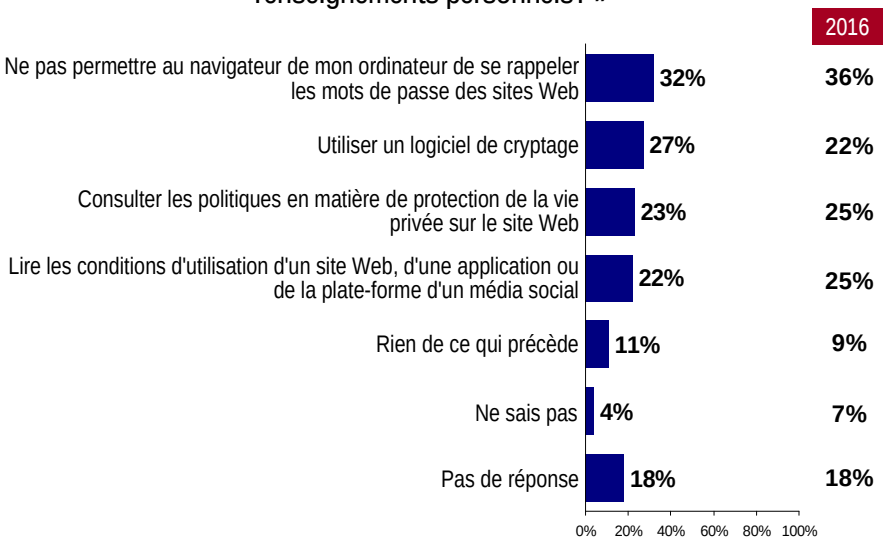
Les Associés de recherche EKOS

n=533

Sondage de SP sur la cybersécurité, 2018

Graphique 52b : Instructions de sécurité précises à l'intention des employés

« Quelles instructions parmi les suivantes fournissez-vous aux employés pour protéger l'organisation contre les menaces en ligne et pour protéger vos renseignements personnels? »



Les Associés de recherche EKOS

n=533

Sondage de SP sur la cybersécurité, 2018

- Les grandes organisations ont tendance à être plus précises lorsqu'elles indiquent à leurs employés de ne cliquer que sur les pièces jointes provenant de sources sures, d'utiliser des mots de passe complexes, de modifier les mots de passe par défaut, de ne pas partager de mots de passe sans effectuer une vérification et de consulter les politiques en matière de protection de la vie privée. Les organisations qui comptent de onze à vingt employés demandent également à leurs employés d'utiliser des mots de passe complexes, de faire preuve de prudence lorsqu'ils répondent à des demandes de sources inconnues et de télécharger uniquement du contenu provenant de sources sures.
- Les entreprises comptant une personne responsable des TI sont également plus susceptibles d'indiquer qu'elles demandent à leurs employés de procéder à chacune de ces procédures. Celles qui externalisent ce service sont les plus enclines à demander à leurs employés de télécharger ou de cliquer que sur les pièces jointes provenant de sources de confiance, de faire preuve de prudence lorsqu'ils répondent à des sollicitations et de ne pas partager de mots de passe sans effectuer une vérification.

10.4 RENSEIGNEMENTS UTILES

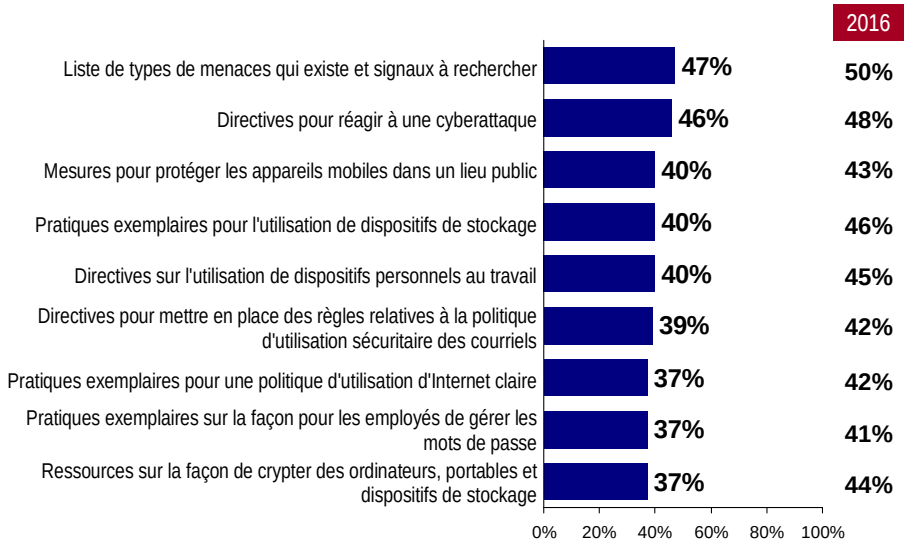
Le classement des éléments d'information susceptibles d'être bénéfiques fait ressortir le fait que les entreprises canadiennes aiment mieux recourir à des solutions dont peuvent s'occuper un service des TI ou un énoncé politique qu'à des solutions en vertu desquelles elles doivent informer leurs employés. Par exemple, en tête de liste, les organisations croient qu'elles devraient tirer profit de renseignements sur les types de menaces qui existent (47 p. cent), de directives sur la façon de réagir à des cyberattaques (46 p. cent), de pratiques exemplaires en matière de dispositifs de stockage, de mesures de protection d'appareils mobiles dans un environnement public et de directives sur l'utilisation d'appareils personnels pour le travail (40 p. cent chaque), ainsi que de directives permettant l'établissement de règles relatives à des politiques d'utilisation sécuritaire de courriels (39 p. cent).

Un peu plus bas dans la liste apparaissent les pratiques exemplaires sur les façons dont les employés devraient utiliser les mots de passe, les directives relatives à l'établissement d'une politique solide en matière de médias sociaux, les pratiques exemplaires relativement à l'utilisation d'Internet, de même que les ressources sur les méthodes de chiffrement d'ordinateurs, de portables et de dispositifs de stockage (37 p. cent dans chaque cas). La demande est semblable en ce qui concerne les conseils visant les logiciels et le matériel servant à sécuriser des réseaux (36 p. cent) et les pratiques exemplaires relatives à l'utilisation sécuritaire de services infonuagiques (35 p. cent). Un peu moins de répondants cernent un besoin d'information sur les mesures à prendre lorsque des employés quittent l'organisation (33 p. cent) et sur les conseils concernant la communication de l'importance de suivre les politiques de cybersécurité (32 p. cent).

En comparaison avec les résultats de 2016, les demandes d'information semblent légèrement à la baisse en 2018 dans certains domaines, y compris en ce qui a trait à l'utilisation de dispositifs de stockage et d'appareils personnels, à la clarté des politiques relatives à l'utilisation d'Internet, à la façon de chiffrer des appareils, aux types de logiciels et de matériel permettant de sécuriser des réseaux, à l'utilisation sécuritaire de services infonuagiques, à la marche à suivre lors du départ d'employés et à l'importance de l'adoption de politiques sécuritaires en matière de cybersécurité.

Graphique 53a : Renseignements requis

« De quels types de renseignements parmi les suivants croyez-vous que votre organisation tirerait profit si elle se protégeait contre les menaces en ligne? »



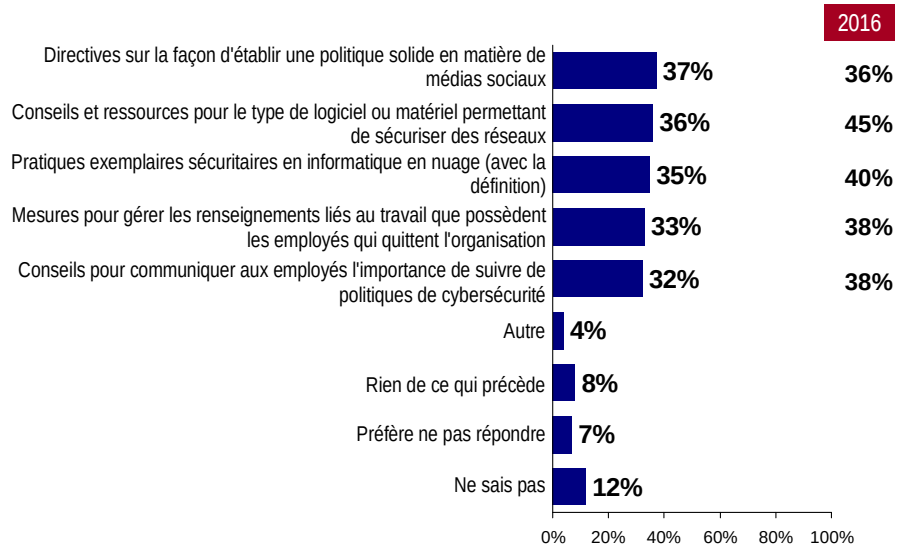
Les Associés de recherche EKOS

n=533

Sondage de SP sur la cybersécurité, 2018

Graphique 53b : Renseignements requis

« De quels types de renseignements parmi les suivants croyez-vous que votre organisation tirerait profit si elle se protégeait contre les menaces en ligne? »



Les Associés de recherche EKOS

n=533

Sondage de SP sur la cybersécurité, 2018

- Les entreprises comptant une personne responsable des TI, ainsi que celles qui externalisent cette tâche, sont également plus susceptibles d'indiquer qu'elles demandent à leurs employés de procéder à chacune des procédures mentionnées.

11. Résultats des groupes de discussion

11.1 Connaissance d'enjeux de sécurité

Les participants des groupes de discussion croient principalement qu'il existe des enjeux de sécurité en lien avec des activités en ligne. Plusieurs personnes sont préoccupées par les vols de nature financière lors de transactions en ligne, ou par le vol d'identité à la suite de saisie d'informations, de vol de données, de piratage d'institutions où des renseignements personnels sont stockés, ou de piratage d'ordinateurs personnels. Certaines personnes sont préoccupées par des enjeux de protection de la vie privée, ce qui comprend un éventail d'appréhensions, comme les prédateurs qui ont accès à des webcams ou les gens qui se procurent des données à des fins de marketing.

11.2 Confiance dans la capacité de se protéger

La plupart des participants des groupes de discussion affirment prendre des mesures pour se protéger contre les risques que supposent certaines activités en ligne. Ces participants croient que, bien qu'il soit impossible d'éliminer totalement les risques, ils prennent des mesures raisonnables pour assurer leur sécurité lorsqu'ils communiquent en ligne, effectuent des transactions électroniques ou protègent leurs documents ou photos. Sinon, les participants de certains groupes de discussion ont une confiance extrême dans leur capacité à mener en toute sécurité des activités en ligne, déclarant bien connaître les risques et être méticuleux dans les mesures qu'ils prennent pour se protéger. Quelques participants disent se sentir protégés contre les menaces en ligne, car ils minimisent leur présence ou leurs activités sur le Web. En évitant des interactions sociales ou financières en ligne, ils ont l'impression d'atténuer les risques.

> « Je sais que ces risques ne peuvent pas être complètement éliminés. » (Toronto)

> « Peut-être que je devrais être plus inquiet, particulièrement en ce qui concerne le vol d'identité. » (Toronto)

> « Je me sens plutôt à l'aise par rapport à mon niveau de sécurité. » (Calgary)

> « Il y a un certain risque. Je crois que lorsqu'on pense à toutes les entreprises qui sont victimes de piratage, la question est plus de savoir quand, et pas si. Puisque ça

se produit si souvent, nous savons que c'est un risque sur lequel nous n'avons pas vraiment de contrôle. Je ne m'empêcherai pas d'acheter quelque chose en ligne juste parce qu'il y a un risque, mais je vais faire plus attention aux gens avec qui je conclus des transactions. » (Montréal)

« Je ne magasine pas en ligne. Voilà pourquoi j'ai confiance. » (Halifax)

11.3 MESURES PRISES POUR ATTÉNUER LES RISQUES

La plupart des participants croient être conscients de l'existence de plusieurs des risques et prennent des mesures de précaution contre toutes les situations négatives. Parmi les domaines dans lesquels les participants se sentent protégés sans avoir à déployer d'efforts figurent les situations où sont impliqués les banques ou les fournisseurs de services Internet. Ces participants remarquent (grâce à leur expérience personnelle ou à celle d'autres personnes) que les banques surveillent les transactions financières et peuvent prendre des mesures pour cerner ou renverser des transactions frauduleuses. Certains participants se fient aussi à la protection qu'offrent les logiciels antivirus et d'autres fonctions de sécurité de leurs ordinateurs pour atténuer les conséquences du piratage, la réception de fichiers corrompus ou d'autres formes de données, ou le vol d'identité.

« Selon moi, la prise de conscience joue un grand rôle. Je vérifie religieusement mes relevés bancaires. » (Toronto)

« Je trouve que l'utilisation de PayPal constitue la meilleure façon de simplifier les choses, car vous ne voulez pas donner vos informations financières à un éventail d'entreprises différentes lorsque vous pouvez les donner à une seule d'entre elles. C'est un seul point vulnérable plutôt que plusieurs. » (Calgary)

« Je ne donnerai jamais mon numéro de carte de crédit à un site Web qui me le demande pour m'inscrire à quoi que ce soit, mais je sais que si j'informe ma banque que je n'ai pas procédé à une transaction, elle l'annulera, raison pour laquelle j'ai l'impression que ma banque me protège. » (Montréal)

Certains participants nomment les mesures qu'ils prennent pour se protéger contre des problèmes de sécurité en ligne, comme le fait de savoir comment reconnaître des courriels frauduleux (épellations erronées, liens vers des sites non officiels), de ne pas utiliser un réseau public ou non sécurisé, de ne pas saisir une date de naissance ou des renseignements personnels en ligne, et de modifier leurs mots de passe régulièrement ou de choisir des mots de passe complexes.

> « Je n'utilise pas mon téléphone pour des activités financières, car je me fie davantage à mon portable. Je ne sais pas si c'est valable ou non, mais je ne m'occupe pas de finances sur mon téléphone. » (Calgary)

> « Ils aiment prendre le nom et l'adresse de courriel de quelques-uns de vos amis, puis changer seulement une lettre avant de vous envoyer un pourriel. C'est une technique plus récente. Je me demande vraiment comment ils peuvent avoir le nom d'amis. Ça me préoccupe. S'ils peuvent obtenir le nom de mes amis, qu'est-ce qu'ils peuvent obtenir de plus? » (Toronto)

> « Je ne fais rien de nature délicate sur un réseau sans fil public. » (Halifax)

11.4 À QUEL POINT LA MENACE EN LIGNE EST-ELLE RÉELLE?

La plupart des participants des groupes de discussion croient que la nécessité de se protéger en ligne est tout aussi réelle que le besoin de se protéger contre des menaces tangibles. Par exemple, une personne qui vole un bien personnel ou qui commet une violation de même type se sent tout aussi menaçante qu'une personne qui commet un vol d'identité en ligne. Pour certains, la menace de vol en ligne est plus préoccupante que la menace de vol d'un bien personnel. Ces participants affirment qu'avec les articles tangibles, une personne peut surveiller ses biens, et l'ampleur des conséquences du vol est immédiatement connue. Quelques-uns expliquent qu'un vol dans « la vraie vie » est plus facile à comprendre que les menaces en ligne. Pour d'autres, il semble plus probable qu'une menace tangible se produise qu'une menace en ligne. Ces participants mentionnent qu'avec toutes les cibles potentielles dont peuvent profiter les pirates (comme les grandes organisations ou les gouvernements), il est improbable que quelqu'un les cible personnellement.

> « Je les considère plus ou moins au même niveau. En fait, je suis un peu moins préoccupée par mes biens physiques parce qu'ils ne peuvent accomplir qu'un certain nombre de choses dans une courte période. Cependant, des dizaines de milliers de dollars peuvent être virés en un instant en ligne. » (Toronto)

> « À mon avis, c'est plus une violation quand c'est numérique. Par exemple, si quelqu'un essaie de me voler, je réplique et ça finit là. Si quelqu'un accède à mes comptes en ligne et fait quelque chose de sournois, ça se peut que je ne m'en rende pas compte immédiatement, vous savez? Le temps de vous apercevoir de ce qui s'est passé et le malfaiteur est déjà parti et s'en prend à quelqu'un d'autre. » (Calgary)

> « Le hasard penche plus en ma faveur en ligne. Quelles sont les probabilités que quelqu'un cherche à accéder à mon ordinateur au moment même où je fais cette chose en particulier. Il me semble que les possibilités que ça arrive sont moins élevées, alors que si je sors mon portefeuille et que dix personnes m'entourent, ce

sont dix possibilités réelles. » (Halifax)

« Je pense que le risque est moindre en ligne, mais ça ne veut pas dire que rien de mal ne peut se produire, même si c'est moins risqué. » (Montréal)

« [Le vol de biens physiques représente davantage une menace, car...] tous mes documents importants, comme mon passeport, sont à la maison, et pas en ligne. » (Montréal)

11.5 Obstacles à la prise de mesures

Quelques participants des groupes de discussion cernent les raisons précises pour lesquelles ils n'ont pas à prendre des mesures supplémentaires pour se protéger en ligne. Certains croient déjà prendre des précautions suffisantes. Quelques-uns affirment prendre des mesures pour se protéger en général, reconnaissant toutefois qu'ils prennent parfois des risques (comme faire des transactions sur un appareil branché à un réseau sans fil public). D'autres déclarent prendre des mesures pour se protéger, mais croient qu'il est improbable qu'ils soient la cible d'intentions malveillantes.

Quand même, quelques-uns d'entre eux ignorent ce qu'ils devraient faire pour se protéger dans leurs activités en ligne et croient qu'il leur manque de temps, de directives ou d'information sur ce qu'ils devraient faire pour améliorer leur cybersécurité. Certains disent se sentir incapables de prendre des précautions parce que même si des mesures de sécurité sont en place, les activités en ligne riment quand même avec des menaces.

« Je ne sais pas si nous savons quoi faire. Je veux dire, vous pensez que vous contrôlez tout, mais vous lisez dans les manchettes des journaux "Un pirate fait des siennes" et vous voyez que de grandes sociétés sont victimes de piratage informatique. Je regarde mon téléphone cellulaire et je me demande à quoi je peux bien m'attendre. J'espère seulement ne pas être assez important pour les intéresser. » (Calgary)

« Si même l'ARC s'est fait pirater, que peuvent bien faire de simples particuliers? » (Calgary)

« La raison pour laquelle je possède tous ces appareils alors que je connais les risques est le côté pratique, et j'accorderai toujours plus d'importance à cet aspect qu'au risque qui y est associé. » (Toronto)

« J'ai recherché des conseils sur la façon de me rappeler différents mots de passe, mais c'est une question de facilité. Oui, je pourrais les modifier, mais je ne veux pas faire l'effort. C'est différent au travail, mais quand c'est personnel, j'imagine que ma vie est sans intérêt et que les pirates ne vont pas se déranger pour moi. » (Montréal)

11.6 CARACTÈRE ADÉQUAT DE L'INFORMATION

La plupart des participants des groupes de discussion indiquent ne pas posséder suffisamment d'informations pour prendre des mesures de protection adéquates pour eux et leur famille contre les menaces en ligne. Principalement, la plupart des participants disent posséder des informations de base ou très partielles. Selon certains d'entre eux, puisque la technologie utilise Internet et que les risques qui y sont associés évoluent constamment, il peut être ardu de se tenir à jour. De même, quelques-uns indiquent qu'il n'est pas possible de comprendre toutes les menaces potentielles en ligne et que certains risques sont inhérents à la plupart des activités.

> « Non, j'ai l'impression de ne pas disposer d'assez d'information, car les menaces changent. » (Calgary)

> « Selon ce que je sais, les Canadiens n'ont nulle part où aller pour connaître les risques qui existent, la prochaine menace qui se présentera et la principale menace qui pesait la semaine passée. Ça serait rassurant d'avoir ces renseignements. » (Halifax)

> « Je ne crois pas posséder toutes les informations, mais dans une certaine mesure, il n'est pas possible d'obtenir toute l'information. Je peux prendre une décision en m'inspirant des renseignements dont je dispose, mais il n'y a aucune garantie que ma banque ne sera pas victime de piratage demain et qu'elle perde tous les renseignements. » (Montréal)

Certains participants ont l'impression que des segments de la population (aînés, jeunes, nouveaux arrivants) n'ont pas accès à des renseignements sur les menaces qui existent en ligne et sur les mesures à prendre pour se protéger contre ces menaces. Quelques-uns déclarent avoir recherché de l'information pour protéger des membres de leur famille, comme des enfants ou des parents vieillissants. Parmi ces gens, personne n'a fait allusion à des renseignements qu'ils ont trouvés pour aider un segment en particulier.

> « J'ai tenté de trouver un site, mais il n'y a rien qui pourrait fournir à mes parents une liste de vérification disant : "Avez-vous vu ça?", "À quoi ressemble le courriel?", "À quoi ressemble le lien URL?" Il n'y a rien à leur disposition. Tout est éparpillé. » (Toronto)

> « Le fait d'être bientôt un aîné et de travailler avec des aînés me fait réaliser qu'il s'agit du groupe le plus ciblé et qu'il ne possède pas les connaissances pour y faire face. » (Toronto)

Les participants qui croient posséder suffisamment d'information comprennent généralement les gens qui se disent convaincus de savoir quelles mesures prendre pour atténuer les risques que posent les menaces en ligne. Ces participants ont l'impression de posséder les

connaissances techniques requises pour savoir quelles mesures prendre afin de se protéger en ligne et croient qu'aucun renseignement supplémentaire ne pourrait améliorer leur compréhension. Toutefois, comme l'a mentionné un participant, vous pouvez vous fier aux renseignements que vous possédez quand vous ne connaissez pas la nature du problème ou ce qui fait défaut.

> « En passant du temps à lire sur Internet, vous apprenez comment ces choses fonctionnent. Une fois que vous savez plus ou moins comment ça fonctionne, il est plus difficile de mordre à l'hameçon. » (Halifax)

11.7 Fiabilité perçue de l'information

La plupart des participants ont l'impression d'être sensibles aux risques en raison de différentes sources qu'ils ont consultées. Plusieurs d'entre eux ne recherchent pas activement de l'information sur les risques en ligne, mais sont passivement exposés à des renseignements qui leur sont communiqués par le bouche-à-oreille ou par les médias. Un participant souligne : « C'est si fréquent, que je connais très bien la plupart des mesures communes que je peux prendre parce que les médias nous les rappellent constamment. » Quelques participants qui commencent à réfléchir à ces mesures d'atténuation des risques que présentent les menaces en ligne lorsqu'eux ou des membres de leur famille sont touchés par des problèmes de sécurité sur le Web.

> « Je ne voulais rien en savoir jusqu'à ce que ça m'arrive et j'en suis maintenant très conscient. » (Halifax)

La plupart des participants des groupes de discussion croient que les renseignements sur la cybersécurité sont plus fiables et dignes de confiance lorsqu'ils proviennent de sources « officielles », comme leur banque ou leur fournisseur de services internet. D'autres sources d'information fiables peuvent être le bouche-à-oreille d'amis ou de membres de la famille, et des articles en ligne. Plusieurs participants nomment également toute source ou donnée pouvant faire l'objet d'une vérification par le biais d'autres forums.

> « Je dirais que c'est une question de récurrence de l'information. Si je vois une vidéo sur des médias sociaux sur un sujet chaud ou sur une histoire de piratage, et que je ne la revois pas ailleurs, ce n'est pas une vidéo digne de confiance. Mais si elle a été partagée et que des gens que je connais en parlent, je peux commencer à croire qu'il s'agit de quelque chose de véridique. » (Montréal)

11.8 RESPONSABILITÉ DES PARTENAIRES

La plupart des participants sont d'avis que les gens devraient être responsables de leur propre protection contre les menaces en ligne. Néanmoins, d'autres entités sont considérées comme de possibles sources d'information pouvant aider les gens à s'informer des risques et à prendre des mesures pour se protéger. Les principales sources comprennent les fournisseurs de services Internet et les banques (aussi considérées comme des sources fiables). Certains participants croient que lorsqu'ils se procurent un logiciel de sécurité, il est de la responsabilité du fournisseur du logiciel de protéger les consommateurs contre les menaces en ligne. D'autres personnes nomment aussi la police ou des organismes non gouvernementaux comme des sources potentielles pouvant avoir la responsabilité de fournir des renseignements et de veiller à ce que les Canadiens soient prêts à se protéger contre des menaces en ligne. Quelques-uns nomment sans aide les gouvernements provinciaux et fédéral.

> « Les Canadiens devraient eux-mêmes s'en occuper. Chaque fois que vous êtes confrontés à une nouveauté, vous devriez essayer d'apprendre à la connaître, tout comme les risques qui y sont associés. » (Toronto)

> « Si je paie pour qu'un service de sécurité s'occupe de moi, je crois que c'est sa responsabilité. J'utilise Shaw et je crois que Shaw devrait aussi mettre en place un certain type de tri pour être aux aguets de ces intrusions. Nous payons aussi pour Norton, McAfee ou d'autres entreprises. Ces organisations devraient veiller à ma sécurité. » (Calgary)

Plusieurs participants croient que les écoles devraient fournir des informations aux étudiants afin de les sensibiliser aux risques que présentent Internet et qu'elles devraient créer une fondation pour se protéger. Bien que des efforts soient déployés pour éduquer les jeunes sur la cyberintimidation, cette éducation pourrait être élargie pour aborder des thèmes comme la quantité de renseignements personnels fournis en ligne, les menaces de piratage et les transactions financières.

> « Je crois que ça devrait faire partie du système d'éducation. Pas à l'école secondaire, mais plus tôt encore, comme à l'école primaire, car certains enfants de sept ans utilisent Facebook. » (Toronto)

> « Selon moi, puisque le Web est en constante évolution, il est de la responsabilité du gouvernement de mettre en œuvre des programmes de formation, particulièrement pour les nouvelles générations. » (Toronto)

> « Ne devrait-on pas implanter tout cela dans les programmes d'études des écoles, dans le système d'éducation? » (Halifax)

11.9 RÔLE DU GOUVERNEMENT

Plusieurs participants des groupes de discussion sont d'avis que le gouvernement du Canada a un rôle à jouer pour aider les Canadiens à trouver de bons renseignements sur les menaces en ligne et sur les mesures à prendre pour se protéger. Ces participants considèrent le gouvernement comme une source d'information digne de confiance et croient que l'information que partagerait le gouvernement du Canada serait examinée minutieusement et confirmée comme étant fiable. En outre, quelques-uns croient que le gouvernement a la responsabilité de protéger les Canadiens et qu'il a la possibilité de rejoindre tous les gens. D'autres font remarquer que le gouvernement peut contribuer à ce que des renseignements soient fournis aux particuliers et aux entreprises, et que cela est dans son propre intérêt. Certains croient que le rôle du gouvernement devrait être de contrer les cybermenaces par le biais de politiques, de normes ou de lois.

> « Il devrait sensibiliser les entreprises à un certain point de façon à ce qu'elles adoptent des mesures et informent les utilisateurs. » (Montréal)

> « Le gouvernement devrait imposer des sanctions aux malfaiteurs. C'est un problème mondial, ce qui constitue ma plus grande préoccupation, et les gouvernements devraient pouvoir agir à l'échelle mondiale. » (Montréal)

> « Il serait bien que des normes gouvernementales (pour les industries) disent : "Vous devez offrir au minimum ce niveau de protection et diffuser ce type de publicité". » (Toronto)

> « Je crois qu'il devrait y avoir des règles et règlements pour les grandes sociétés qui se procurent des données, qu'elles manipulent et qu'elles nous vendent par la suite. » (Calgary)

Certaines personnes ont des préoccupations par rapport à la capacité du gouvernement à fournir de l'information de façon efficace. Ces participants ont l'impression que le gouvernement fédéral peut être excessivement bureaucratique et qu'il ne serait pas en mesure de produire des renseignements à l'intention des Canadiens en temps opportun ou de façon rentable, particulièrement si l'on tient compte de la vitesse à laquelle les risques en ligne évoluent. D'autres participants soulignent également que, selon eux, il incombe aux individus de se protéger contre les menaces en ligne et sont mal à l'aise à l'idée que le gouvernement s'occupe de la façon dont la technologie est utilisée. La crédibilité du gouvernement quant à sa capacité à transmettre de l'information sur la cybersécurité préoccupe aussi quelques participants. Ces gens évoquent des brèches dans les données de ministères fédéraux ainsi que l'incapacité du gouvernement fédéral à prévenir des manœuvres frauduleuses en ligne, notamment celles qui semblent provenir de l'ARC, pour expliquer pourquoi ils ne se fieraient pas à des renseignements sur les menaces en ligne émanant du gouvernement.

> « Combien est-ce que ça nous coûterait en fin de compte? Voilà la question. » (Toronto)

> « C'est une question de réputation. Le gouvernement et plusieurs directions gouvernementales ont été victimes de piratage. » (Calgary)

> « Les gens doivent réfléchir et assumer leurs responsabilités, car ce sont eux qui utilisent la technologie. Nous en sommes au point où le gouvernement frappe à nos portes pour nous dire d'être prudents. Il y a des limites à tout. » (Montréal)

Quelques personnes disent qu'un modèle efficace pourrait être que le gouvernement du Canada fournisse du financement à des organisations tierces qui se spécialiseraient dans la communication de renseignements fiables en matière de cybersécurité afin d'aider les Canadiens à se protéger en ligne. Ces organisations seraient considérées comme plus efficaces et concentrées que le gouvernement fédéral et comme des sources d'information impartiales.

> « J'aime l'idée qu'un groupe sans but lucratif qui a obtenu du financement de différentes sources, d'un groupe qui n'agirait pas dans son propre intérêt, mais pour le bien de tous. » (Halifax)

> « Je crois que le rôle du gouvernement consiste à donner à des établissements des outils pour veiller à la sécurité de certaines choses et qui ne se contentent pas de nous informer directement. » (Montréal)

11.10 Mise à l'essai du site Web

Quelques participants des groupes de discussion connaissant des campagnes ou programmes du gouvernement du Canada dont l'objectif est de promouvoir la cybersécurité affirment se rappeler vaguement avoir vu quelque chose, sans pouvoir apporter de détails. D'autres disent se rappeler que le gouvernement du Canada a produit des « conseils cybernétiques » sur la cyberintimidation, notamment un énoncé précisant que tout ce qui est publié dans des médias sociaux reste à tout jamais, ou encore l'image d'un pirate avec un capuchon. Certains mentionnent d'autres souvenirs qui leur viennent à l'esprit, comme une loi antipourriel sur le site Web du commissaire à la protection de la vie privée. D'autres se rappellent une annonce informant que « l'organisme responsable de la cybersécurité » embauchait de nouveaux employés.

Très peu de participants ont entendu parler de la campagne Pensez cybersécurité, hormis une personne qui se rappelle avoir vu quelque chose sur Pensez cybersécurité sur un site de réseautage social. Quelques participants affirment avoir peut-être vu des images de Pensez cybersécurité dans des médias sociaux, mais se disent habitués à ignorer les publicités sur Internet. « Je ne les remarque même plus. »

Apparence générale du site Web

Les participants des groupes de discussion ont eu différentes premières réactions lorsqu'ils ont vu le site Web. En grande majorité, la plupart étaient surpris et ravis d'apprendre qu'il y avait un site Web Pensez cybersécurité et ont demandé s'il était actuellement à la disposition du grand public.

La première réaction de la plupart des participants est que le site Web semble contenir beaucoup de renseignements ainsi qu'une allure « officielle » ou gouvernementale. Selon de nombreux participants, l'apparence « gouvernementale » du site Web donne confiance. Plusieurs d'entre eux étaient curieux et enthousiastes à l'idée d'explorer plus en profondeur le site Web.

> « Oui, je prévois réellement de jeter un coup d'œil au site Web, mais j'ignorais qu'il existait. » (Toronto)
>
> « Est-il en état de marche à l'heure actuelle? » (Calgary)
>
> « Il vous laisse une impression positive lorsque vous y accédez. » (Calgary)
>
> « Puisque c'est un site Web du gouvernement, les gens savent qu'il est sécuritaire et fiable. » (Halifax)
>
> « Je n'avais aucune idée de son existence et je vais le montrer à ma mère. » (Halifax)
>
> « Quand je vois un site Web qui se termine par gc.ca, je sais que je peux m'y fier. » (Montréal)

Quelques participants, particulièrement ceux de Toronto, n'ont pas aimé l'apparence générale du site Web, affirmant qu'il a l'air démodé, qu'il semble plutôt normal avec aucun élément qui se démarque, et qu'il ne donne pas l'impression d'être convivial pour les appareils mobiles. Ces participants aimeraient d'une approche qui soit plus interactive, qui utilisent plus de symboles et qui adopte l'approche d'un fil de nouvelles avec beaucoup de renseignements, comme les « Cinq actualités locales à ne pas rater ».

> « C'est comme Internet en 2010. » (Toronto)
>
> « Puis-je partager ma première impression? La façon dont est fait le site Web me prouve qu'ils ne peuvent pas me transmettre des renseignements sur la cybersécurité parce qu'il a l'air complètement démodé. » (Toronto)
>
> « L'interface utilisateur n'est pas très attrayante. De nombreuses entreprises conçoivent des sites Web avec des interfaces super attrayantes qui fournissent des renseignements aux gens. Ça ressemble à un typique site Web du gouvernement. Il

n'y a pas d'images personnalisées. » (Montréal)

Quelques personnes croient que le site Web pourrait être amélioré si la page d'accueil était simplifiée. Ces participants sont d'avis qu'en raison des nombreux menus et contenus se trouvant sur la première page, il n'est pas évident de savoir par où commencer lorsqu'on recherche de l'information. Certains déclarent que la quantité de renseignements peut être accablante pour une personne qui ne sait pas par où commencer. D'autres veulent d'entrée de jeu savoir s'il y a un glossaire des termes utilisés.

Des participants suggèrent de déployer des efforts pour améliorer la première page du site Web afin de créer un « message principal », à offrir un fil de nouvelles ou une liste bien en vue des menaces actuelles. Certains n'aiment pas la quantité d'informations présentes sur la première page. Quelques participants n'aiment pas les images qui clignotent sur la première page, alors que d'autres personnes les aiment, car elles donnent un ton personnel au site (en raison de la présence d'humains) tout en attirant l'attention. Bien que quelques personnes remarquent le pavé « Avertissement » de la page d'accueil, certaines d'entre elles sont déçues que le lien ne mène pas à une page qui énumère des menaces de cybersécurité actuelles. Quelques participants n'aiment pas le symbole et le pavé d'avertissement, car cela donne l'impression qu'il y a une erreur sur le site Web ou qu'il n'est pas possible d'y accéder.

> « Je crois qu'il ne parvient peut-être pas à véhiculer le message principal. Ainsi, lorsque vous ouvrez la page, quelle impression cela laisse-t-il à l'utilisateur? Je crois que le problème du site Web est peut-être qu'il faut un seul message qui dise aux gens qu'ils devraient avoir peur d'Internet. » (Toronto)

> « Si vous ne connaissez pas les termes, comment pouvez-vous savoir où cliquer? » (Toronto)

> « Ça ressemble plus à un message de mise en garde qu'à un avertissement sur des problèmes de cybersécurité. On dirait un message d'erreur. » (Montréal)

> « Selon moi, la bannière supérieure prend trop de place. Vous devez défiler vers le bas pour trouver de l'information sur la page. » (Montréal)

Contenu

La plupart des participants des groupes de discussion croient qu'il y a suffisamment de contenu pertinent sur le site Web Pensez cybersécurité. La plupart d'entre eux affirment qu'il est généralement important de proposer des renseignements sur la cybersécurité et que le site Web semble en avoir beaucoup. Ils sont également d'avis que la barre de menus et les menus déroulants constituent une caractéristique positive du site Web. Les participants indiquent que la quantité d'enjeux abordés sur le site Web est une caractéristique très positive et que le site Web couvre la plupart des sujets recherchés.

> « J'aime la barre supérieure. J'aime les mentions sur la cybersécurité et sur les façons de se protéger, ainsi que les menus déroulants. » (Calgary)

> « Je trouve que c'est une idée géniale parce qu'on dirait que ça couvre le thème en général. Le site aborde aussi la cyberintimidation et de possibles fraudes. Vous couvrez donc toute la base de ce que vous pouvez retrouver sur le Web. Différentes personnes sont touchées par différentes choses. » (Halifax)

> « On dirait qu'il y a des conseils sur la façon de faire preuve de prudence avec [tous les éléments mentionnés]. » (Montréal)

> « Je pense que tout est là si vous prenez le temps de bien consulter le site. » (Montréal)

Certains participants déclarent que même si le contenu du site Web semble abondant, certains renseignements sont de nature trop générale. Ces participants aimeraient avoir des renseignements plus précis sur les diverses menaces en ligne. De l'information, par exemple, sur les courriels d'hameçonnage pourrait utiliser une image d'un courriel et mettre en évidence les éléments à rechercher pour détecter si le courriel est « vrai » ou non, ainsi que les mesures à prendre lors de la réception d'un tel courriel.

> « J'ai un problème avec tous les sites Web du gouvernement du Canada. Ils vous donnent un texte de présentation comme celui-là, mais il n'y a pas moyen d'aller plus en profondeur. » (Calgary)

> « Lorsque vous parlez de piratage, il devrait y avoir une illustration qui dit "voici ce à quoi ressemble le piratage", "voici ce à quoi ressemble un pourriel", "voici ce à quoi ressemble un courriel d'hameçonnage". Au lieu de simplement y aller d'une description, vous devez parler aux gens, pas seulement leur montrer. » (Halifax)

Certains participants affirment qu'ils seraient préoccupés par le fait que l'information du site Web ne soit pas mise à jour. Plus particulièrement, certains d'entre eux font remarquer que la dernière modification sur des pages date de plusieurs années, ce que suscite leur scepticisme par rapport à la pertinence de l'information. Compte tenu de la vitesse à laquelle les technologies évoluent, les participants croient que le contenu du site Web devrait être constamment modifié et qu'ils ne retourneraient sur le site Web que s'il était évident que le contenu avait fait l'objet d'une mise à jour.

> « Les gens le visiteront plus souvent s'il est précis et actualisé, même sur une base hebdomadaire. Si je savais que le site est actualisé toutes les semaines, je le consulterais dès que j'entendrais parler de nouvelles arnaques ou fraudes. S'il ne contient que des renseignements généraux, les gens le visiteront une fois, peut-être deux, pour apprendre ce qu'ils peuvent, puis ils n'y retourneront plus jamais. » (Calgary)

> « Le site est-il à jour? Pouvons-nous croire que les gens qui ont conçu le site ont fait toutes les recherches nécessaires pour s'assurer que l'information est actuelle? » (Montréal)

Quelques participants aimeraient qu'il y ait quelque chose comme « Le coin des enfants » avec des renseignements destinés aux enfants et aux jeunes. Il pourrait y avoir un symbole un peu plus attrayant sur lequel cliquer avec des images et du contenu qui s'adresse particulièrement aux enfants. Comme nous l'avons souligné plus haut, certains participants des groupes de discussion croient qu'il existe un besoin particulier en ce qui concerne les renseignements de cybersécurité à l'intention des enfants et des jeunes adultes.

> « Particulièrement maintenant pour les plus jeunes enfants, les choses vont empirer et il va toujours y avoir de nouvelles arnaques. Vous devez être en mesure de les préparer à cette réalité. » (Toronto)

> « Il pourrait y avoir un petit jeu pour les enfants. » (Montréal)

Quelques participants n'aiment pas le slogan de la campagne, « Pensez cybersécurité ». Même s'ils sont nombreux à ne pas aimer la formulation, des participants ont spontanément indiqué (dans les groupes en anglais et en français) que le message devrait être plus proactif et inciter les gens à assurer leur cybersécurité. Si une personne pense à la cybersécurité, peut-être qu'il est déjà trop tard pour se protéger contre les menaces en ligne.

11.11 INFOGRAPHIE

Les opinions sont mitigées en ce qui concerne l'infographie, bien qu'elles soient en grande partie positive quant à l'intention du produit. Plusieurs personnes affirment que les renseignements sont utiles et qu'ils suscitent la réflexion, ou qu'il s'agit d'un outil de communication efficace et facile à suivre. Quelques autres, cependant, croient que le site serait plus évocateur s'il avait recours à une activité en ligne qui est plus universelle. Par exemple, certains participants déclarent que cela ne s'applique peut-être pas aux gens qui ne font pas de magasinage en ligne. Un faible nombre de participants sont également d'avis qu'ils connaissent déjà les éléments dont ils doivent se méfier lorsqu'ils font du magasinage en ligne et qu'ils n'auraient donc pas besoin de ce type de rappels.

> « Il fait ce qu'il doit faire. Il attire l'attention. Il n'y a pas beaucoup de lecture, mais il vous donne les renseignements dont vous avez besoin pour avoir le goût d'en savoir plus. » (Calgary)

> « Je serais curieux de voir ce qu'on nous invite à faire, comme d'aller à un site #moquelquechose pour voir ce qui se passe. » (Halifax)

> « C’est très visuel, donc j’aime ça. Je n’ai pas tendance à lire un texte complet, alors ça attire mon attention. » (Montréal)

> « Je suggèrerais aussi un produit un peu plus commun qu’un drone. En fait, qui d’entre nous a déjà utilisé un drone? » (Calgary)

> « J’ai tendance à penser que je n’achèterais jamais quelque chose seulement avec une adresse de courriel. » (Halifax)

Une grande préoccupation par rapport à l’infographie est le temps qu’il faut pour que le message apparaisse, y compris le nombre de tableaux ou de secondes qu’il faut pour accéder au message principal. Plusieurs participants affirment qu’il ne devrait y avoir qu’un seul tableau ou qu’il faut aborder le thème principal au cours des dix premières secondes. De nombreux participants considèrent le court temps d’attention des utilisateurs de médias sociaux comme une préoccupation alors que plusieurs autres croient que si le contenu et le style ne captivent pas immédiatement le public, la publicité sera ignorée.

> « Je n’ai pas compris l’objectif de l’infographie avant la troisième fois, cependant. » (Calgary)

> « J’ai l’impression que l’utilisation de trois plans où il serait possible de voir l’ensemble du contenu, comme une bande dessinée, serait plus percutante. Cela aiderait un peu plus les gens à faire le lien. » (Halifax)

> « Dans ce format, trente secondes c’est beaucoup trop long, ce qui est dommage, car dans le monde d’aujourd’hui c’est tout simplement trop. » (Halifax)

> « C’est la façon de faire les choses de nos jours. Créer quelque chose qui peut se résumer à une vidéo de dix secondes, mais aussi une vidéo de trois minutes et ensuite un fichier balado d’une heure. » (Toronto)

La deuxième préoccupation de participants de la plupart des villes (à l’exception de Toronto) est qu’il n’est pas évident, ou à tout le moins pas assez tôt, qu’il s’agit d’un produit du gouvernement du Canada. Le contraire rendrait immédiatement légitimes l’information et le message. Pour certaines personnes, il ne possède pas une apparence typique du gouvernement et elles suggèrent de mettre davantage en évidence la marque du GC. Parmi les suggestions de modifications figure l’utilisation de marqueurs communs, comme le slogan « Une présentation du gouvernement du Canada » sur la dernière diapositive du refrain publicitaire « Oh Canada ».

> « C’est une question de familiarité. » (Calgary)

> « Lorsque j’utilise une application comme Instagram, si je vois le logo du gouvernement du Canada, je suis plus susceptible de voir ce que la vidéo a à dire. » (Halifax)

> « Les gens sont conditionnés à ignorer les publicités. Si ça ressemble trop à une annonce publicitaire, les gens vont l'ignorer. » (Calgary)

> « Aussitôt que vous quittez la première page, vous n'avez aucune idée que ça vient du gouvernement du Canada. Si vous ne voyez pas le petit symbole au bas de l'écran, ça peut avoir l'air de provenir de n'importe qui. » (Halifax)

> « Je trouve que publier des annonces du gouvernement du Canada sur Instagram et Facebook est très novateur, raison pour laquelle j'ai tendance à me demander : "Pourquoi veulent-ils que je regarde ces choses". Je sais qu'ils n'essaient pas de me vendre quoi que ce soit. » (Halifax)

Certaines personnes trouvent l'absence d'une conclusion agaçante, énervante même. Ils sont d'avis que les conclusions devraient être claires et que les gens ne devraient pas aller à une autre source pour voir la fin de l'histoire. Comme le dit un des participants : « De la façon dont c'est monté, ça pourrait être de l'hameçonnage ».

> « Si je dois cliquer sur autre chose, je ne vais pas le faire. » (Calgary)

> « Cela tient pour acquis d'entrée de jeu que je suis sur Twitter, ce qui signifie que je dois faire quelque chose pour en savoir plus, et je ne fais jamais ça quand je suis en ligne. » (Halifax)

> « Je déteste vraiment les choses qui font ça, qui montre deux parties d'une histoire et qui te demande de cliquer pour voir le reste. Racontez-moi l'histoire. Ça ne m'importe pas assez pour me rendre à cette page. » (Halifax)

> « Personne ne visite #moetsesamis. » (Toronto)

Selon quelques participants, le format et l'approche sont trop enfantins et exercent un attrait limité. D'autres affirment qu'ils préfèreraient voir un peu de texte ou des puces dans l'infographie.

> « Selon moi, les gens le prendraient plus au sérieux s'il avait une apparence un peu plus professionnelle. » (Calgary)

> « Je comprends qu'on cherche à proposer quelque chose d'accueillant, mais c'est trop bébé. » (Montréal)

> « J'aime. C'est attrayant pour les adolescents et les jeunes adultes qui font du magasinage en ligne. » (Montréal)

> « Je pense à du contenu bref et concis, comme des puces. N'importe quoi qui le rende accrocheur et intéressant pour que je sache en cinq secondes ce que ça signifie et si c'est pertinent pour moi. » (Halifax)

« En règle générale, ça me semble trop chargé. Ça doit être réduit à l'essentiel. » (Toronto)

11.12 Publication Facebook

Certains participants aiment la publication et la trouvent utile, bien que certains d'entre eux affirment également qu'ils ne la remarqueraient pas. Ils aiment aussi les conseils rapides qui y apparaissent, tout comme le titre accrocheur, qu'ils considèrent comme des attributs positifs.

> « C'est bien. Si ce type d'information m'intéressait, c'est de cette manière que je voudrais qu'elle soit présentée. » (Calgary)
>
> « L'introduction est accrocheuse. » (Halifax)
>
> « Je trouve que ces mascottes sont plutôt jolies. » (Toronto)
>
> « Je trouve que c'est bien. Ce n'est pas tout le monde qui comprend la technologie ou son fonctionnement; ça rejoindrait donc bien des gens. » (Montréal)

Quelques personnes moins favorables à la publication semblent préoccupées par la grande quantité de texte et le manque de clarté du message. Plusieurs d'entre elles réitèrent le commentaire concernant l'approche enfantine formulé à l'égard de l'infographie.

> « Elle semble s'adresser davantage à des enfants de cinq ans qu'à des adultes. » (Calgary)
>
> « Le jargon me paraît bizarre. » (Calgary)
>
> « Les gens qui ne savent pas ce qu'est l'hameçonnage n'ont aucune idée du thème dont traite la publication. Personne ne sait ce que c'est. » (Toronto)
>
> « Je vois la photo, ça attire mon attention, puis je vois trois paragraphes. Je me demande alors si la photo me captive suffisamment pour lire trois paragraphes d'information. » (Calgary)
>
> « Il doit y avoir quelque chose comme quatre mots. » (Toronto)
>
> « Les messages ne ressortent pas et ne m'incitent pas à poursuivre la lecture. » (Montréal)

Comme dans le cas de l'infographie, plusieurs participants affirment que ce n'est pas évident qu'il s'agit d'un produit du gouvernement du Canada, ce qui devrait être une priorité. En ce qui concerne cet aspect, de nombreuses personnes déclarent qu'elles hésiteraient à cliquer sur un lien à moins que la source soit clairement légitime. Certains participants suggèrent que la campagne ait recours à une adresse URL complète (c.-à-d. avec gc.ca bien en vue), car les URL

courtes suscitent la méfiance et sont typiques des tentatives d'hameçonnage.

> « Vous voulez que je suive le lien d'un expéditeur inconnu avec une photo et un lien court? Non merci, ça va. » (Calgary)
>
> « Si ça vient du gouvernement du Canada, je me sens plus à l'aise de cliquer sur le lien. » (Calgary)
>
> « Le logo du gouvernement du Canada ajoute du poids s'il est clairement visible. » (Halifax)
>
> « Certaines personnes évitent les URL courtes. Puisqu'il s'agit du gouvernement du Canada, ils n'ont pas besoin d'en utiliser une. Je préfèrerais que ce soit gc.ca. » (Halifax)
>
> « Il manque le logo du gouvernement du Canada, alors je ne suis pas susceptible de m'y fier. » (Montréal)

ANNEXE A
QUESTIONNAIRE DU SONDAGE

APPENDIX A: Survey Instrument

INTRO

WEB INTRO

EKOS Research Associates is surveying people across the country on behalf of the federal Government about issues related to the use of internet-enabled devices (e.g. personal computers, cell phone, smart phones, smart TVs, tablets, etc). The survey should take approximately 20 minutes to complete. Your participation is voluntary and your responses will be kept completely confidential and anonymous. Any information you provide will be administered in accordance with the Privacy Act and other applicable privacy laws. This survey is registered with the National Survey Registration System. **A few reminders before beginning: -** On each screen, after selecting your answer, click on the "Continue" button at the bottom of the screen to move forward in the questionnaire. **-** If you leave the survey before completing it, you can return to the survey URL later, and you will be returned to the page where you left off. Your answers up to that point in the survey will be saved. **-** If you have any questions about how to complete the survey, please call Prob*it* at 866.211.8881 or send an email to online@ekos.ca. Thank you in advance for your participation.

D2

Which of the following categories best describes your current employment status? Are you ... ?

Working full-time (35 or more hours per week)	1
Working part-time (less than 35 hours per week)	2
Self-employed	3
Student attending full time school (not working)	4
Unemployed, but looking for work	5
Not in the workforce (for example, unemployed, but not looking for work, a full-time homemaker or parent)	6
Retired	7
Other (please specify)	77
No response	99
ON DISABILITY PENSION	8
MATERNAL/PATERNAL LEAVE	9

QEMP

Employed, D2

How many employees are there at all locations in your organization, including those working full and part-time?

Please specify	77
None	98
Don't know/ No response	99

QEMPB [1,2]

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

Do you have any of the following responsibilities:

Please select all that apply

Employees who report to you/ you oversee work of other employees	1
Involvement in decisions about processes and procedures followed by employees in your organization	2
None of these	99

D5

Are there any children under the age of 18 currently living in your household?

Yes	1
No	2
No response	9

D4

In what year were you born?

Year	1
No response	9

B1 [1,8]

What kinds of devices do you use to access the internet for **personal use**?

Please select all that apply

Desktop computer or laptop	1
Smart phone capable of accessing data, video, etc (e.g. iPhone, Android)	2
Tablet/ ereader/iPod (e.g. iPad, Amazon Kindle)	3
Home gaming system (e.g. Sony PlayStation, Microsoft Xbox)	4
Streaming service (e.g. Apple TV, Chromecast)	5
Smart TV	6
Smart watch/wearable technology	7
Smart home devices (e.g. Nest, smart locks, smart baby monitor, etc.)	8
Voice activated assistive devices (e.g., Google Home, Amazon Echo, etc.)	9
Do not know	98
No response	99

B2 [1,20]

Where do you typically access the internet?

Please select all that apply

Home using wired connection only	1
Home using wifi	2
At work	3
Public Wifi (e.g. libraries, coffee shops, malls, airports, etc.)	4
On your provider's cellular network (LTE, 3G, etc.)	5
At school	6
At the home of friends or relatives	7
Other	77

No response	99

B2B

Home wifi, B2

Do you secure your home wifi with a password?

Yes	1
No	2
Do not know	98
No response	99

B3 [1,20]

Which of the following activities have you done over the internet in the past year?

Please select all that apply

Used email	1
Financial transactions (making payments, other, banking, investments, etc.)	2
Purchased at an online store or an auction site (such as eBay)	3
Used your credit card online	4
Browse websites	5
Used social network sites/apps (Facebook, Myspace, Twitter, Snapchat, Instagram, LinkedIn, Pinterest, etc.)	6
Used app-based services (Uber, Lyft, Just Eat, Airbnb, etc)	7
Telephone or video calls via Skype or other similar applications	8
Accessed government information services	9
Viewed videos or movies (YouTube, Netflix, etc.)	10
Played online games	12
Streamed or downloaded music, podcasts, or other content	13
Participated in an online contest	14
Participated in online training course	15
Participated in blogs/discussion groups/message boards	16
Submitted applications (e.g. for employment) online	17
Read news, watched television, listened to radio	18
Downloaded software	19
No response	99

B3B [1,7]

Financial transactions, B3

How do you usually do these transactions?

Please select all that apply

From your computer at home	1
From your smartphone using a secure payment app	2
From your smartphone from your Internet browser	3
Using a voice activated device (e.g., Google Home, Amazon Echo)	4
Escrow services (e.g. Paypal)	5
Other	77
No response	99

B11 [1,8]

To your knowledge, have you ever done any of these things?

Please select all that apply

Opened an email attachment from an unknown source	1
Clicked on a link from an unknown email or text	2
Entered personal details on a computer that you did not know was secure	3
Forwarded an email or text attachment from an unknown source	4
Entered bank account or credit card information on a site that you did not know was secure	5
Replied to spam mail unknowingly	6
Replied to spoof or phishing email unknowingly	7
Entered financial information while using public Wi-Fi	8
None of these	97
Do not know	98
No response	99

K1

Canadians have expressed a wide range of views regarding their ability to protect their personal information when going online. Some are quite concerned and others are not concerned. How ***concerned*** would you say that you are about your personal information being fraudulently obtained online and used for purposes of illegal activities?

Not at all	1
Not very	2
Fairly	3
Very	4
Do not know	8
No response	9

B5

Some people take precautions to protect their computer and other devices they use to access the internet, while others do not. Do you take precautions to protect your devices?

Yes	1
No	2
Do not know	8
No response	9

B5A [1,20]

Which of the following precautions do you take, if any, to protect your devices?

Please select all that apply

Keep security software up-to-date	1
Only download files from trusted sources	2
Use spam filters	3
Verify the source before clicking on URL links or opening attachments	4
Lock the device using a password or PIN	5
Change the default password right away	14
Turn off the device when not using it	6
Back up information on my device	7
Store information in an account in the cloud	8

Use encryption software	9
Do not use administrator account when accessing the web	10
Use a password or user authentication for wireless and remote access	11
Use caution when responding to solicitations from strangers	12
Use two-step or two-factor authentication	13
None of these	97
Do not know	98
No response	99

B5B [1,20]

Which of the following precautions do you take to protect yourself against online threats and to protect your personal information?

Please select all that apply

Use passwords that contain random numbers, letters and symbols that are difficult to guess	1
Check privacy policies or terms of use on the website	2
Change my device's default password	3
Do not share passwords	4
Use caution when giving out real name, address and phone number	5
Use additional email accounts under a pseudonym/false name for organizations you don't trust	6
Do not allow my computer browser to remember passwords for websites	7
Use caution when responding to solicitations from strangers	8
Do not use administrator account when accessing the web	9
Use of encryption software	10
None of these	97
Do not know	98
No response	99

B4 [1,6]

Desktop computer or laptop, B1

Do you have anti-virus software on your computer, smartphone or tablet?

Select all that apply

Yes, for computer	1
Yes, for smartphone	3
Yes, for tablet	4
No	2
Do not know	8
No response	9

B4C

Computer, B4

How often is the anti-virus software on your computer, smartphone or tablet updated (by you or automatically) to the latest version?

Please select only one response

Daily	1
Weekly	2
Monthly	3
Yearly	4

It is not updated	5
Do not know	8
No response	9

B4D [1,20]

Smartphone, B4

People have a number of different reasons for not having anti-virus software. What is the reason that you don't have anti-virus software?

Please select all that apply

I do not know what it is	1
It would cost too much	2
I haven't had time to install it	3
I don't believe I need it for a smartphone or tablet	10
I thought my computer does it automatically	4
I don't know what to buy or how to install and run it	5
I don't go online with my computer very often	6
I only go to websites I know are safe	7
I only do activities online that I know are safe	8
I don't think I need it	9
Other (please specify)	77
Do not know	98
No response	99
Operating system not susceptible to viruses, use mac/apple/linux, do not use windows/microsoft	11
Impedes performance, slows down system, uses too many system resources	12
Antivirus software ineffective/insufficient, attracts additional viruses	13
I can take care of viruses easily myself	14
My isp (internet service provider) has an antivirus component to it	15
Other	97

B4E

No need, B4D

Why don't you feel that you need it?

Response	77
No response	99
Operating system not susceptible to viruses, use mac/apple/linux, do not use windows/microsoft	1
I only go to trusted websites, secure sites, careful user, exercise caution	2
I know how to get rid of viruses	3
Not effective, invasive, do not trust anti virus	4
Other	97

K5 [1,20]

Below is a list of some of the threats individuals can face when using the internet. Which of the following were you already aware of?

Please select all that apply

Computer/mobile devices get viruses, spyware, malware	1
Identity theft	2
Privacy violations	3
Personal data erased or changed or lost	4

Financial loss	5
Seeing or receiving information of a criminal nature	6
Device unknowingly taken over or used in other crimes	7
Destruction of computer	8
Loss of files/information (music, photos, etc.)	9
Being a victim of an online scam or fraud	10
Personal data held for ransom (i.e., locked by ransomware)	11
None of these	97
No response	99

K7 [1,7]

Which of the following have the potential of being affected by an online threat?

Select as many as apply

PC/Laptop	1
Tablet/ereaders/iPod	2
Smartphones	3
Wearable devices (e.g. fitbit, smart watch)	4
Smart TV	5
Smart home devices	6
Voice activated devices (e.g., Google Home, Amazon Echo, Apple HomePod)	7
None of these	97
Do not know	98
No response	99

QATT1

Please rate the degree to which you agree or disagree with the following statements.

QA12A2

Parents only

I can't keep up with technology/apps/games that young people are using.

Strongly disagree	1
2	2
3	3
Neither	4
5	5
6	6
Strongly Agree	7
Do not know	8
No response	9

QA12A3

Parents only

I am confident that I have the information I need to help navigate my child's online world

Strongly disagree	1
2	2
3	3
Neither	4
5	5
6	6

Strongly Agree	7
Do not know	8
No response	9

QA13

It's up to individuals to protect their own personal privacy.

Strongly disagree	1
2	2
3	3
Neither	4
5	5
6	6
Strongly Agree	7
Do not know	8
No response	9

QA15

The security of your computer could be compromised without you even knowing it.

Strongly disagree	1
2	2
3	3
Neither	4
5	5
6	6
Strongly Agree	7
Do not know	8
No response	9

QA117

Half-sample

As long as the anti-virus software that came with my computer isn't more than a couple years old, it should be good enough to protect me from online threats.

Strongly disagree	1
2	2
3	3
Neither	4
5	5
6	6
Strongly Agree	7
Do not know	8
No response	9

QA110

I am confident that businesses and other organizations have adequate security safeguards to protect my personal information.

Strongly disagree	1
2	2
3	3
Neither	4
5	5

6	6
Strongly Agree	7
Do not know	8
No response	9

QA111

Half-sample

Taking steps on how to protect myself and my family from online threats is something that everyone knows how to do and regularly does these days

Strongly disagree	1
2	2
3	3
Neither	4
5	5
6	6
Strongly Agree	7
Do not know	8
No response	9

K8

How ***likely*** is it that you or a family member will be affected by an online threat in the next 2 years?

Not at all	1
2	2
3	3
Moderately likely	4
5	5
6	6
Extremely likely	7
Do not know	8
No response	9

K8A [1,5]

Unlikely, K8

Why don't you think that it is likely that you or your family will be affected by an online threat?

Please select all that apply

Take steps to protect ourselves online	1
Do not do anything risky online	2
Think the chances are just very small	3
Online threats only apply to businesses and people with a lot of money	4
Other (please specify)	77
No response	99
Stay up to date/knowledgeable/educated about information/viruses, work in computer/information technology, educate/teach family/friends to protect themselves	5
Use apple/mac/linux which not as susceptible to viruses, do not use microsoft network	6
OTHER	97

PK2

How ***important*** do you think each of the following are:

K2A

For the average Canadian to take steps to protect **their *personal information* online**?

Not at all	1
2	2
3	3
Moderately important	4
5	5
6	6
Extremely important	7
Do not know	8
No response	9

K2B

For Canadians to take steps to protect the **security of *home computers or mobile devices, like smartphones, tablets, and other smart devices***?

Not at all	1
2	2
3	3
Moderately important	4
5	5
6	6
Extremely important	7
Do not know	8
No response	9

K6B

How ***common*** is it for Canadians to be affected by online threats?

Not at all	1
2	2
3	3
Moderately common	4
5	5
6	6
Extremely common	7
Do not know	8
No response	9

K10A

Half-sample

How familiar are you with the practice of purchasing crypto currency that can be used for online purchasing or trading?

Not at all familiar	1
2	2
3	3
Moderately familiar	4
5	5

6	6
Very familiar	7
Do not know	8
No response	9

K10B

Familiar, K10A

Have you ever purchased, traded or used crypto currency for online purchases/activities?

Yes	1
No	2
Uncertain	9

K11 [1,13]

Below is a list of steps to reduce the chances of experiencing an online threat. Some people are aware of these steps, while others are not. Which of the following were you already aware of?

Please select all that apply

Only doing banking on a computer you know is safe	1
Not sharing your passwords with others	2
Using different passwords for different accounts and websites	3
Using longer/more complex passwords	4
Not opening email attachments from people you do not know	5
Being selective in the sites you use for online shopping	6
Limiting the personal information you share online	7
Using antivirus/anti-spyware software on your computer, tablet or smartphone	8
Using firewalls and passwords to protect computers and other web-enabled devices	9
Password protecting your wireless home network	10
Avoiding using open, public wifi to do shopping or banking	11
None of these	97
No response	99

K11A [1,20]

Banking on safe computer, K11

How can you tell if a website is secure?

Please select all that apply

HERE	
Know the site well	1
Site belongs to a trustworthy source (e.g. well known internet Service Provider or software provider, government, etc)	2
The site has an "https" address	3
The site has a checkmark or VeriSign authentication	4
Other (please specify)	77
Do not know	98
No response	99
Displays security lock symbol	5
Impossible, cannot fully know/know for sure, difficult to guarantee, any site can be hacked	6
Will get a warning message about security, security warnings from browser/software/computer, will say if not encrypted/if has security ticket, green/red certificate in browser	7

Go directly to site, type it in, do not use third party links/hyperlinks, avoid redirects/email links	8
Check independently through web (web of trust) or site advisor	9
Conduct research as to whether site is legitimate/safe, check url (see if registered/secured properly), use whois, check spelling of url, read comments about privacy/reputation	10
Other	97

B6

Have you ever had a *virus, spyware or malware* on your devices

(Please note - when we ask about *virus, spyware or malware* we mean: Viruses, spyware, and malware are designed to destroy data, monitor your computer use and report it back to a third party without your knowledge, or allow a third party to take control of your computer).

Yes	1
No	2
Do not know	8
No response	9

B8A

Yes, B6

How much of an impact did this *virus, spyware or malware* have on you or your family?

No impact at all	1
2	2
3	3
Moderate impact	4
5	5
6	6
Very large impact	7
Do not know	8
No response	9

B7A

Have you ever suffered financial loss or been the victim of financial fraud as a result of your online activity?

Yes	1
No	2
Do not know	8
No response	9

B8B

Yes, B7A

How much of an impact did the *financial fraud as a result of your online activity* have on you or your family?

No impact at all	1
2	2
3	3

Moderate impact	4
5	5
6	6
Very large impact	7
Do not know	8
No response	9

B7B

Have you ever been a victim of *identity theft* a result of online activity?

(Please note - when we ask about *identity theft* we mean: The unauthorized collection and fraudulent use of your personal information, usually for criminal purposes.

Yes	1
No	2
Do not know	8
No response	9

B8C

Yes, B7B

How much of an impact did your *identity theft* have on you or your family?

No impact at all	1
2	2
3	3
Moderate impact	4
5	5
6	6
Very large impact	7
Do not know	8
No response	9

PB13

Half-sample

Many people use the same passwords for different accounts and devices, and many keep the same passwords over time. How often would you say you change a password in each of the following:

B13A

Half-sample

Your social media accounts

Never	1
Every few years	2
Once a year	3
A few times a year	4
More often than a few times a year	5
Whenever I am prompted to	6
Whenever I think of it no set pattern	7
When I learn about a security breach	10
Not applicable (don't have any)	8
No response	9

B13B

Half-sample

Your online shopping accounts

Never	1
Every few years	2
Once a year	3
A few times a year	4
More often than a few times a year	5
Whenever I am prompted to	6
Whenever I think of it no set pattern	7
When I learn about a security breach	10
Not applicable (don't have any)	8
No response	9

B13D

Half-sample

Your email accounts

Never	1
Every few years	2
Once a year	3
A few times a year	4
More often than a few times a year	5
Whenever I am prompted to	6
Whenever I think of it no set pattern	7
When I learn about a security breach	10
Not applicable (don't have any)	8
No response	9

B14 [1,20]

Which of the following do you do, if any?

Please select all that apply

Share a password with your friends	1
Write down your passwords	2
Use the same passwords for multiple accounts	3
Use a password keeper	4
Allow your browser to remember your passwords	5
Make your passwords complex with a combination of letters, numbers and symbols	6
Keep your passwords simple and easy to remember	7
Use a multi-step or multi-factor authentication	8
Use a biometric protection (e.g. fingerprint lock, facial recognition)	9
Other	77
None of these	97
No response	99

B16

Half-sample

How likely are you to take precautions against online threats as you are to take precautions against "in-person" threats? As an example, how likely are you to avoid posting vacation pictures and information on social media while you are away as you are to cancel deliveries or ask neighbours to watch your home while you are away?

Not nearly as likely as in-person 1	1
2	2
3	3
As likely as in-person 4	4
5	5
6	6
Much more likely than in-person 7	7
No response	99

IC5A [1,20]

Which of the following types of online threats have you looked for information on, if any?

Please select all that apply

Protecting devices with anti virus software	1
How to know if an email is a scam	2
Things you can do to protect your computer files	3
Steps you can take to use public wifi safely	4
Steps you can take to use social networking sites safely	5
PARENT = 1	
Internet safety for your children	6
Internet safety for seniors	7
Things you can do to protect your mobile devices	8
Definition of terms (glossary) about internet safety or cyber security	9
Cyberbullying, online harassment	10
Securing home networks/wifi	11
Steps you can take to protect other internet connected devices (e.g. smart TVs, home security systems, fitness monitors, voice activated devices such as Google Home and Amazon Echo)	12
Other	77
None of these	97
No response	99

IC5B [1,15]

1-8, IC5A

Where did you go for that information?

Please select all that apply

Web site of software or hardware vendor	1
Friends and family	2
Media	3
Web site of a non-profit group	4
Newsletter	5
Government web site	6
Employer IT dept	7

School	8
Search engine (e.g. Google, Bing, etc.)	9
Law enforcement website	10
Other (please specify)	77
Do not know	98
No response	99
Computer technician, it professional/consultant	11
Internet service provider	12
Discussion forums, blogs, message boards	13
Computer stores, staff at stores, stores that sold them the computer	14
Bank/financial institutions	15
Books, magazines, articles/journals	16
Sites specifically for security news/updates, independent sites of experts, specialized debunkers of misinformation (various, e.g.:: snopes.com)	17
Other	97

QATT2

Please rate the degree to which you agree or disagree with the following statements.

QA211

I feel I have enough information to know how new technologies might affect my personal privacy.

Strongly disagree	1
2	2
3	3
Neither	4
5	5
6	6
Strongly Agree	7
No response	9

QA211B

I feel I have enough information on how to take steps to protect myself and my computer against online threats.

Strongly disagree	1
2	2
3	3
Neither	4
5	5
6	6
Strongly Agree	7
No response	9

QA218

I am confident that I could protect myself online as long as I have basic and trustworthy information on steps to take.

Strongly disagree	1
2	2
3	3
Neither	4

5	5
6	6
Strongly Agree	7
No response	9

PQA22

Parents only

As a parent of a youth, how concerned are you, if at all, about each of the following:

QA22A

Parents only

Cyberbullying, online harassment

Not at all concerned	1
2	2
3	3
Moderately concerned	4
5	5
6	6
Extremely concerned	7
Do not know	8
No response	9

QA22B

Parents only

Your child's privacy

Not at all concerned	1
2	2
3	3
Moderately concerned	4
5	5
6	6
Extremely concerned	7
Do not know	8
No response	9

QA22C

Parents only

Legal implications of your child downloading copyrighted materials (e.g. music, books, movies)

Not at all concerned	1
2	2
3	3
Moderately concerned	4
5	5
6	6
Extremely concerned	7
Do not know	8
No response	9

QA22D

Parents only

Legal implications of your child sharing pictures or content of others under 18

Not at all concerned	1
2	2
3	3
Moderately concerned	4
5	5
6	6
Extremely concerned	7
Do not know	8
No response	9

QA22X [1,7]

Parents only; Not concerned, QA22D

Why is it that you are not concerned?

Please select all that apply

I never really thought about it	1
I don't know what the issues are to be concerned about	2
I have looked for information and talked with my child about these issues	3
My child has received information and instructions at school on these issues	4
My child has looked for information and told me about what they do to avoid risks	5
I just trust my child to know what to do	6
My child isn't online very much	7
Do not know	8
No response	9

IC6 [1,15]

Who would you trust to give you the best **technically reliable and up-to-date information** about online threats and steps you can take to protect yourself?

Please select all that apply

Friends or family	1
Internet Service Provider	2
Security Software company	3
Financial Institutions	4
Vendor website (e.g. online store where you are shopping, etc.)	5
Not-for-profit organization dedicated to electronic security	6
Government	7
Law enforcement organization	8
Other (please specify)	77
Do not know	98
No response	99
It personnel/computer/security technician, computer consultant, software programmers/experts (includes it staff from work)	9
Computer store/vendor, retail outlets/software vendor, geek squad from best buy	10
On line sources (e.g.: forums/blogs/podcasts/websites/online articles	11
Television, magazines, newspapers, radio	12
Computer manufacturer	13
Through work, my employer, work employees	14

Myself	15
No one, these sources are the problem, none of the above	16
Other	97

IC7 [1,15]

And who would you trust to give you the most **unbiased** information about online threats and steps you can take to protect yourself?

Please select all that apply

Friends or family	1
Internet Service Provider	2
Security Software company	3
Financial Institutions	4
Vendor website (e.g. online store where you are shopping, etc.)	5
Not-for-profit organization dedicated to electronic security	6
Government	7
Law enforcement organization	8
Other (please specify)	77
Do not know	98
No response	99
It personnel/computer/security technician, computer consultant, software programmers/experts (includes it staff from work)	9
Computer store/vendor, retail outlets/software vendor, geek squad from best buy	10
On line sources (e.g.: forums/blogs/podcasts/websites/online articles	11
Television, magazines, newspapers, radio	12
Computer manufacturer	13
Through work, my employer, work employees	14
Myself	15
No one, these sources are the problem, none of the above	16
Other	97

IC8

When someone talks about "fake news" in connection with information that people/consumers need to protect themselves, do you think that this typically refers to:

Information that is from a biased source (i.e., someone/individual/company/political party)	1
that stands to gain from misinformation consumer use)	2
Information from a source that is not transparent (i.e., hidden or falsely	3
attributed to a more reputable source)	4
Information that is falsely used to shape opinion or facts	5
Parodies intended as a joke, that are presented as factual (i.e., The Onion)	6
Other (specify)	77
Don't know	99

IC10

1-5, IC8

How can consumers tell that information about online threats is "fake news"?

Response :	77
Don't know	99

IC11

Half-sample

Who should play a role in helping Canadians recognize what is "fake news" when it comes to information about online threats and consumer protection?

Government	1
Not for profit organizations dedicated to electronic security	2
Software providers	3
Internet service providers	4
Manufactures of the devices	5
Retailers of devices (computers, mobile devices)	6
Teachers	7
Other (please specify):	77
Do not know	98
No response	99

B10 [1,20]

As far as you know, who is primarily responsible for ensuring that personal devices that Canadians use to access the internet with (e.g. computer, smart phone, tablet, other smart devices etc.) are safe and secure?

Please select all that apply

Individual owners of the devices	1
Private sector	2
Government	3
Not for profit organizations dedicated to electronic security	4
Software providers	5
Internet service providers	6
Manufactures of the devices	7
Retailers of devices (computers, mobile devices)	8
Other (please specify)	77
Do not know	98
No response	99
Nobody	9
Website owners where information should be protected (e.g.: bank websites...)	10
Other	97

GOCAD

Have you seen, heard or read any Government of Canada advertising or websites related to the use of internet-enabled devices and security of online activities?

Yes	1
No	2
Do not know	99

GOCEDU

The Government of Canada has a public education campaign in place to tell Canadians about the importance of taking steps to protect yourself from online threats, along with some steps to think about. Do you recall seeing, hearing or reading anything like this from the Government of Canada?

Yes	1
No	2
Do not know	99

DEMIN

These last questions are about you and will be used strictly for statistical purposes to understand the results of the survey.

D1C

How many hours do you spend online each day?

Enter number of hours	77
Do not know	98
Prefer not to say	99

D1B [1,3]

Thinking about data storage of information for personal use, do you save information on your computer hard drive, an external hard drive (i.e., extra storage / back up), or on a "virtual server" (i.e., cloud computing)?

Save files on computer hard drive	1
Save files to an external hard drive	2
Save files on a "virtual server"/in a cloud	3
Do not know	8
Prefer not to say	99

B5X

How often do you back up data/personal files stored on your computer, smartphone or tablet?

Never	1
Once or twice a year	2
Every few months	3
Once a month	4
A few times a month	5
Weekly or more often	6
Don't know	99

D11

Are you ...

Male	1
Female	2
Other	3

Prefer not to say	99

D3

What is the highest level of formal education that you have completed to date?

Elementary school or less	1
Secondary school	2
Some post-secondary	3
College, vocational or trade school	4
Undergraduate university program	5
Graduate or professional university program	6
Prefer not to say	99

D6

Which of the following categories best describes your total household income? That is, the total income of all persons in your household, before taxes?

Under $20,000	1
$20,000 to just under $40,000	2
$40,000 to just under $60,000	3
$60,000 to just under $80,000	4
$80,000 to just under $100,000	5
$100,000 to just under $150,000	6
$150,000 and above	7
Prefer not to say	99

D7

What is the language you first learned at home as a child and still understand?

English	1
French	2
Other	77
Prefer not to say	99

D9

Were you born in Canada?

Yes	1
No	2
Do not know	98
Prefer not to say	99

D5B

Parents only

How old is your oldest child still living at home?

Year(s)	1
Prefer not to say	99

D5C

Parents only, 11 or younger, D5B

Do any of your children use a computer or mobile device to access the internet?

Yes	1
No	2
Prefer not to say	99

BUS1 [1,20]

Responsible, QEMPB; Self-employed, D2

Turning to your work as a business owner/manager, which of the following steps has your business taken to protect itself against online threats?

Select all that apply

Keep security software up-to-date on all machines	1
Set spam filters	2
Require password protection on all devices	3
Back up information on all devices	4
Use encryption software	5
Do not use administrator account when accessing the web	6
Use a password or user authentication for wireless and remote access	7
Follow information removal protocols when employees leave the organization	8
None of these	97
Do not know	98
Prefer not to say	99

BUS2 [1,20]

Responsible, QEMPB; Self-employed, D2

Which of the following instructions do you provide to employees to protect the organization against online threats and to protect your personal information?

Select all that apply

To use passwords that contain random numbers and letters that are difficult to guess	1
To check privacy policies on the website	2
To read terms of service/use of a website, app or social media platform	3
To change my default password	4
Not to give out password without calling to verify that the request is legitimate	5
To only download from trusted sources	6
To only click on attachments or URLs from trusted sources	7
Not to allow my computer browser to remember passwords for websites	8
To use caution when responding to solicitations from strangers	9
To use of encryption software	10
None of these	97
Do not know	98
No response	99

BUS3 [1,20]

Responsible, QEMPB; Self-employed, D2

Which of the following types of information do you feel that your organization would benefit from having to protect itself against online threats?

Select all that apply

A list of the types of threats that exist and cues to look for	1
Tips on communicating the importance of following cyber security policies to employees	2
Best practices for a clear internet usage policy	3
Guidelines to establish rules for safe email usage policies	4
Guidelines on how to establish strong social media policy	5
Tips/resources for the type of software/hardware to make networks secure	6
Best practices for how employees on how to handle passwords	7
Steps to protect mobile devices in a public setting	8
Steps for handling work-related information possessed by departing employees	9
Guidelines for reacting to a cyber attack	10
Best practices for safe cloud computing (with definition of cloud computing)	11
Best practices for use of storage devices (e.g. USBs)	12
Resources on how to encrypt computers, laptops, and storage devices	13
Guidelines on use of personal devices for work	14
Other	77
None of these	97
Do not know	98
Prefer not to say	99

BUS4 [1,20]

Responsible, QEMPB; Self-employed, D2

Who is responsible for your company's IT?

Select all that apply

Me	1
Another employee (specify role in company) BOXBUS4	2
An employee of the organization dedicated to IT	3
Outsource to an IT firm	4
Other	77
None of these	97
Do not know	98
Prefer not to say	99

BUS5A

Responsible, QEMPB; Self-employed, D2

Thinking about the various concerns of daily operations of your organization, how worried would you say you are about work disruptions or financial loss as a result of online threats?

Not at all concerned	1
2	2
3	3
Moderately concerned	4
5	5
6	6

Extremely concerned	7
Do not know	98
Prefer not to say	99

BUS5B

Unconcerned, BUS5A

Why is this?

I never really thought about it	1
I don't know what the issues are to be concerned about	2
We have researched this and taken steps to protect ourselves	3
The threat for a company like ours is very low	4
There are bigger issues to worry about than cyber attacks	5
You can't really protect yourselves against cyber attacks if it's going to happen, there's isn't much you can do	6
Other	77
None of these	97
Do not know	98
Prefer not to say	99

THNK

The Government of Canada, and EKOS, thank you very much for your time.

That concludes the survey. This survey was conducted on behalf of the Public Safety Canada. In the coming months, a report with the findings from this study will be available from Library and Archives Canada. Thank you very much for taking part. It is appreciated.

THNK2

Screened out

Thank you for your cooperation! Based on the information you have provided, unfortunately you are not eligible to complete the remainder of this survey.

ANNEXE B
SCÉNARIO DE RECRUTEMENT POUR LES GROUPES DE DISCUSSION

APPENDIX B: Focus Group Recruitment Script

Hello, my name is _____ from EKOS Research. We are conducting a series of focus group discussions with Canadians who are 16 years of age or older on behalf of the Government of Canada. The research is related to use of Internet-enabled devices and security issues of concern to all Canadians and we think that you'll find the topic interesting.

Your participation in the research is completely voluntary and your decision to participate or not will not affect any dealings that you may have with EKOS Research or the Government of Canada. The purpose of the research is to understand the opinions and experiences of Canadians not to sell any service or product.

The sessions will be audio and video recorded for research purposes. Representatives of the Government of Canada will also be observing the discussions. The information is being collected under the authority of the Privacy Act and other applicable privacy laws. The full names of participants will not be provided to the government or any other third party. Also, the results from the discussions will be grouped together in a report, which will contain non-identifying information. May I continue?

Yes	1
No	2

Q1

The session will last an hour and a half and an incentive is offered for participation. May we have your permission to ask you some further questions to see if you fit in our study?

Yes	1
No	2

QGENDR

Record gender of respondent (DO NOT ASK)[ELSE]Are you...>

Male	1
Female	2

QAGEX

May I have your year of birth, please?

RECORD YEAR :	77
REFUSED	99

QEDUC

What is the highest level of formal education that you have completed to date?

Grade 8 or less	1
Some high school	2
High school diploma or equivalent	3

Registered Apprenticeship or other trades certificate or diploma	4
College, CEGEP or other non-university certificate or diploma	5
University certificate or diploma below bachelors level	6
Bachelor's degree	7
Post graduate degree above bachelor's level	8
Don't know / No answer	9

QINCOME – ASK ONLY OF 19+

Which of the following categories best describes your total household income? That is, the total income of all persons in your household, before taxes?

Under $20,000	1
$20,000 to just under $40,000	2
$40,000 to just under $60,000	3
$60,000 to just under $80,000	4
$80,000 to just under $100,000	5
$100,000 to just under $120,000	6
$120,000 to just under $150,000	7
$150,000 and above	8
Don't know / No answer	9

D2

Which of the following categories best describes your current employment status? Are you ... ?

Working full-time (35 or more hours per week)	1
Working part-time (less than 35 hours per week)	2
Self-employed	3
Student attending full time school (not working)	4
Unemployed, but looking for work	5
Not in the workforce (for example, unemployed, but not looking for work, a full-time homemaker or parent)	6
Retired	7
Other (please specify)	77
No response	99

Q2

Are you or is any member of your household or immediate family employed in:

Q2A

Government of Canada

Yes	1
No	2

Q2B

An advertising agency

Yes	1
No	2

Q2C

A market research company

Yes	1
No	2

Q2D

The media (Print, Radio, TV, Internet)

Yes	1
No	2

NOTE: If a response of "YES" to any of the above (Q2a-Q2D) Thank and Terminate →THNK2

Q3

Participants in group discussions are asked to voice their opinions and thoughts. How comfortable are you in voicing your opinions in front of others, in English? Are you...

Very Comfortable	1
Comfortable	2
Fairly Comfortable	3
Not Very Comfortable	4
Very Uncomfortable	5

Q4

Have you ever attended a focus group or one to one discussion for which you have received a sum of money?

Yes	1
No	2

Q5

When did you last attend one of these discussions that was sponsored by the Government of Canada?

Please specify :	77
Months	1
Years	2
Never	999

Calculate:

Within last 6 months, thank and terminate	1
Continue	99

Q5B

Have you attended more than 6 of these discussions that were sponsored by the Government of Canada?

Yes	1
No	2

QEMP

How many employees are there at all locations in your organization, including those working full and part-time?

Please specify	77
None	98
Don't know/ No response	99

QEMPB [1,2]

Do you have any of the following responsibilities:

Please select all that apply

Employees who report to you/ you oversee work of other employees	1
Involvement in decisions about processes and procedures followed by employees in your organization	2
None of these	99

QFOCUS

The focus group is about an hour and 30 minutes in length, but we are asking that all participants arrive 10 minutes prior to the start time of the session. Are you able to be at the facility 10 minutes prior to the session time?

Yes	1
No	2

QTELE

We are providing each participant with a $85 cash incentive for their participation, although late arrival (i.e., more than a few minutes) may result in not being able to participate or receive the incentive. Replacements are not permitted and you will need to bring ID, which you may be asked to present on arrival for the discussion. If you usually use reading glasses you should bring those along as well because there may be a few short phrases to read throughout the discussion.

We will be giving you a reminder telephone call and sent an email or if you prefer, a text, a day or two prior to your group discussion. What is your preferred method of receiving a reminder?

Email

Text

Phone call

If phone/text:

Is this the best number at which to reach you?

If email, please provide your email address

FNAME

Please provide your first and last names.

NOTE TO INTERVIEWER: Confirm proper spelling. Ensure proper capitalization (IE: not all upper or lowercase).

Name : 1

THNK

If you have any questions or something comes up and you can no longer participate in the discussions, please let us know by calling us toll-free at XXXXXXXX or by sending an e-mail to XXXXXXX. Thank you for your cooperation and time.

ANNEXE C
GUIDE DU MODÉRATEUR POUR LES GROUPES DE DISCUSSION

APPENDIX C: Focus Group Moderator's Guide

1. INTRODUCTION

- I represent EKOS Research and these groups are being conducted for Public Safety Canada to explore perceptions regarding exposure to online threats and steps that Canadians can take to protect themselves online.
- This research will help the Government of Canada plan communications activities designed to make Canadians aware of various risk factors related to online activities, and steps they can take to reduce their risk.
- This group is part of a series of focus groups taking place across Canada. This session will last about an hour and a half and we can start by going over the format and "ground rules":
  - Discussion is being audio taped and video recorded so that I can listen closely to what you are saying and not be distracted by having to write things down.
  - There are observers from the Government of Canada.
  - All comments are confidential.
  - Please try to speak one at a time and be respectful of one another's opinions.
  - There are no right or wrong answers to the things we'll be talking about.
  - It's okay to disagree. Please speak up even if you think you're the only one who feels a certain way about an issue. Everyone may have different experiences and different points of view. And we want to hear everyone's opinions.
- Moderator's role: raise issues for discussion, watch for time and make sure everyone has a chance to participate. We do not work for the Government of Canada.
- Please make sure that your cell phones, notifications on smart watches, etc. are turned off. We ask for your full attention for this time, without distractions.

2. INTRODUCTION

1. Let's start by going around the table. Tell me your first name, and who you have in your household?

2. What kinds of devices do you and others in your household use to access the Internet?
   a. How many use voice activated assistance, like Google Home or Amazon "Echo" types of devices to do things online?

3. What kinds of activities do you and others in your household do online (e.g., financial transactions, online shopping, social media, app-based shared services like Uber/Airbnb, online games)?
   a. How many of you use phone-based apps to make payments on the go?

3. AWARENESS AND CONCERNS

4. Do you feel there are any security issues that pose a risk to you and your family when you are engaged in online activities?
   a. What are the nature of the risks that concern you (financial theft, identity theft, breach of privacy, loss of information/data, other?)

5. Do you currently take any action to prevent these risks?
   a. What kinds of actions do you take?
   b. Do you feel it works? Do you feel like you are making a difference?

6. How confident are you that you know how to protect yourself? How have you decided what steps you will take and what you won't?
   a. Is it about feeling you are aware of the risk and have information about steps you can take to protect yourself and your family from online threats?

7. For those of you not taking any steps or for those of you who think you could do more, what are the things that hold you back from taking steps or making changes to prevent risk?
   a. How much is it about knowing if something does pose a risk or not (i.e., recognizing the risk)? Or knowing what to do about it?
   b. Do you feel that it is up to others to address these things not you?

8. Does it feel just as "real" when it happens online or do you have to remind yourself about protecting yourself online? For example, does someone stealing your belongings feel more real or more like a real threat, than someone stealing your identify online?

4. INFORMATION & ROLE OF GOVERNMENT

9. Do you feel like you have enough information to adequately take steps to protect you and your family from online threats?

10. What got you started thinking about or taking steps to mitigate risk from online threats? Did you go looking for information or did you happen upon it or learn from friends and family?

11. Where have you looked for this information? Where have you found information that was useful to you?

12. How can you tell if the information you are getting is reliable and trustworthy? Unbiased?
    Is it hard to tell who/where information is coming from and whether it's a trusted source

13. Whose responsibility do you think it is to ensure that Canadians are prepared to protect themselves against online threats?

14. Do you feel it is the Government of Canada's responsibility to inform the Canadian public about the potential for online threats and steps everyone can take to protect themselves from online risks? Why or why not?

15. Could the GC have a role to play in helping Canadians find good information that helps them to know what steps to take?
    a. In what way would that be helpful?
        i. Finding information
        ii. Access to trustworthy and unbiased information
        iii. Easy to understand information? Tips sheets on things to thing about
        iv. Other?

16. Are you familiar with any Government of Canada campaigns or programs to promote cybersecurity?

17. Have you heard of Get Cyber Safe?

5. Website Testing

Now we are going to look at a Government of Canada website on cyber safety and get everyone's reaction to various elements of it. This is the Get Cyber Safe website that is part of the campaign.

18. Let's have a look at the website homepage. What do you think of the overall look and layout of the page?
    a. Is it appealing? Does it command attention / is it compelling (i.e., makes you curious to know what it's about and keep looking)?
    b. What stands out most on the page?
    c. Is there anything about it that turns you off right away (tone, images, information)?

19. Does it feel like this is a trustworthy site?
    Why do you feel that way (GC site, good information, look and feel of site?)

20. Does it seem like a site that you could get useful/informative information from? Would you visit it and read the information there?
    a. Is it the right kind of information (i.e., information Canadians should have)?
    b. Does it seem like the right level of detail for a public campaign? Why or why not?

21. Let's look at how the content is organized. There is a section for social media posts with added information. There are menus along the top. Let's have a look at the headings and a few of the topics under each.
    a. How do you feel about the organization of the page overall?
    b. How do you feel about the menus - how they are organized, topics under each?
    c. Is there anything that you feel should be changed, added or done differently? What and why?

22. Have a look at an infographic the Government is developing. What do you think of it?
    Is it clear?
    a. How about this FaceBook ad?

23. Overall, does the site encourage you to think carefully about the type of online threats you and your family may be exposed to, and the steps you take or need to take to protect yourself from online threats?
    a. Does it make you want to look for more information?

6. Wrap up

24. Is there anything that we haven't talked about or that you would like to add before we go?

THANK YOU