Commissariat
à la protection de
la vie privée du Canada

Notes d'allocution pour le programme de sensibilisation des personnes âgées

Protection de vos renseignements personnels

DIAPOSITIVE 1 – Titre : Protection de vos renseignements personnels en ligne

Présentez-vous.

DIAPOSITIVE 2 – Titre : CE QUE NOUS VERRONS AUJOURD'HUI

- Aujourd'hui, nous verrons trois secteurs clés liés au respect de la vie privée qui préoccupent les aînés canadiens. Nous aborderons tout d'abord le vol d'identité, ensuite nous passerons à la protection de la vie privée en ligne et nous finirons par la protection de la vie privée pour les applications mobiles.
- Cette présentation vise à vous fournir des renseignements et des solutions faciles à mettre en œuvre pour assurer votre protection.

DIAPOSITIVE 3 – Points clés

Qu'est-ce que le vol d'identité?

- Le vol d'identité, c'est quand une personne prend vos renseignements personnels et se fait passer pour vous à des fins frauduleuses.
- Chaque année, des milliers de personnes sont victimes de vol d'identité. Votre nom, date de naissance, adresse, numéro de carte de crédit, numéro d'assurance sociale (NAS) et vos autres numéros d'identification personnels peuvent servir à obtenir une carte de crédit, ouvrir des comptes bancaires, réacheminer le courrier, établir un service de téléphone cellulaire, louer un véhicule, de l'équipement ou une chambre, ou même obtenir un emploi.

- Si vous êtes victime d'un vol d'identité, les répercussions sont graves. Par exemple, on peut refuser de vous octroyer un permis de conduire ou un service de téléphone cellulaire, et il faut parfois plusieurs années pour réparer les dommages causés par ce vol d'identité, sans parler de toute la paperasserie qu'il faut préparer.

DIAPOSITIVE 4 – Points clés

Comment vous protéger contre le vol d'identité :

- **Divulguez le moins de renseignements personnels possible.** Si on vous demande votre date de naissance, votre adresse courriel réelle ou d'autres détails, demandez la raison. Ne donnez pas de renseignements personnels si vous n'avez pas à le faire.

Facultatif : Réfléchissez à combien de fois on vous demande votre adresse courriel. On me la demande toujours – à l'épicerie, au magasin de vêtements. Parfois, on vous offre un rabais de 15 % si vous fournissez votre adresse courriel. Comme vous le savez sans doute, dès que vous donnez votre adresse courriel, vous commencez automatiquement à recevoir un plus grand nombre de courriels dans votre boîte de réception; pensez-y donc deux fois avant de divulguer votre adresse courriel. Il peut être difficile de repérer les pourriels et les courriels importants. Pour vous faciliter la tâche, vous pouvez utiliser une adresse courriel principale pour vos contacts de confiance et créer des adresses supplémentaires pour vos activités en ligne, comme remplir des formulaires ou adhérer à des communautés. Ces adresses sont faciles à changer si elles sont recueillies et vous commencez à recevoir beaucoup de pourriels.

- **Divulguez seulement des renseignements personnels de nature délicate (dont les renseignements financiers comme les numéros de carte de crédit et les numéros de compte bancaire) par l'entremise de moyens sûrs.** Si vous remplissez un formulaire en ligne, repérez le cadenas dans le coin inférieur droit de votre écran. N'envoyez jamais vos renseignements personnels de nature délicate dans un courriel.
- **Portez une attention particulière à votre numéro d'assurance sociale (NAS).** Votre identité est étroitement liée à cette pièce d'information qui donne accès à vos rapports de crédit et aux bases de données informatisées.
- **Assurez-vous de connaître les fins auxquelles vos renseignements personnels sont destinés**. Si vous ne les connaissez pas, demandez-les.

DIAPOSITIVE 5 – Points clés

Vos renseignements personnels sont importants; en quoi consistent-ils et comment les gens/entreprises peuvent-ils les trouver et les utiliser?

- Les renseignements personnels sont des renseignements qui vous concernent, par exemple votre nom, votre âge, l'adresse de votre domicile, votre adresse électronique, votre numéro de téléphone et votre date de naissance.
- Les renseignements personnels peuvent également s'agir de photos ou de vidéos de vous, et de ce que vous écrivez en ligne.
- À peu près tout ce que vous faites en ligne peut révéler quelque chose sur vous.
- Vous laissez des empreintes partout sur Internet. Les mots que vous tapez, les sites Web que vous visitez et les photos que vous affichez en ligne laissent des empreintes. Si quelqu'un d'autre affiche des éléments portant votre nom ou votre photo, il s'agit également de vos empreintes.
- Ce n'est pas seulement en ligne non plus. Les voleurs d'identité peuvent ramasser votre courrier ou vous demander des renseignements personnels par téléphone. Il est important de déchiqueter les documents de nature sensible que vous n'avez plus besoin de conserver. De plus, vous ne devez jamais divulguer de renseignements personnels par téléphone.

DIAPOSITIVE 6 — Points clés

Protection de votre boîte de réception, de votre ordinateur et de vos appareils mobiles

- Vous devriez commencer par installer des logiciels antivirus et d'autres logiciels de protection sur votre ordinateur et vous assurer de les mettre à jour régulièrement.
- La bonne nouvelle, c'est que votre navigateur Internet (Internet Explorer ou Google Chrome) est doté d'outils intégrés qui aident à protéger vos renseignements personnels. Prenez le temps de découvrir les paramètres de sécurité et de protection de la vie privée de votre navigateur et tenez-les à jour.
- Lorsque vous utilisez des réseaux Wi-Fi publics, évitez d'effectuer des opérations sensibles, en particulier des opérations bancaires en ligne. La connexion n'est pas sécurisée et des tiers pourraient intercepter les données que vous transmettez.
- Il est important de choisir un mot de passe sûr. Lorsque vous choisissez un mot de passe, résistez à l'envie d'opter pour le nom de jeune fille de votre mère, le nom de l'un de vos enfants ou de votre animal de compagnie ou toute autre référence que quelqu'un pourrait deviner à partir de renseignements que vous avez publiés ailleurs. Créez des mots de passe d'au moins huit caractères. Utilisez un mot de passe différent pour chaque site Web et chaque compte. Ne les partagez jamais avec les autres.

Facultatif : Combien d'entre vous avez de la difficulté à vous rappeler de vos mots de passe? Si vous avez besoin d'écrire vos mots de passe pour ne pas les oublier, assurez-vous de les conserver dans un endroit secret, sécuritaire et verrouillé.

- Méfiez-vous de quiconque vous demande par courriel ou par téléphone des renseignements liés à vos cartes bancaires et à vos cartes de crédit, et utilisez uniquement des sites sécurisés lorsque vous faites des achats en ligne. L'icône de cadenas, le

protocole HTTPS et la barre d'adresse affichée en vert ne sont pas à toute épreuve, mais ils signifient tous que le site est probablement sécurisé.

Options facultatives aux fins de discussion : Vous avez acheté un nouveau chandail en ligne et peu après, vous recevez un courriel vous demandant d'envoyer vos renseignements de paiement une autre fois, car ils n'ont pas bien été transmis. Devriez-vous envoyer vos renseignements de carte de crédit au vendeur?

Réponse : N'envoyez jamais vos renseignements de carte de crédit par courriel.

DIAPOSITIVE 7 – Points clés

Réduire le risque de pourriels.

- Combien d'entre vous recevez des pourriels dans votre boîte de réception? Les pourriels peuvent être agaçants, car ils congestionnent votre boîte de réception et dans certains cas, ils peuvent même constituer une véritable menace à votre vie privée.
- Les pourriels peuvent introduire des logiciels espions et d'autres types de logiciels malveillants qui peuvent compromettre votre ordinateur et vos appareils mobiles, et s'emparer de vos renseignements personnels à votre insu. La bonne nouvelle, c'est que vous pouvez prendre des mesures afin de réduire les risques que votre adresse courriel soit recueillie et ciblée par les polluposteurs.

DIAPOSITIVE 8 – Points clés

Conseils pour éviter les pourriels.

- **N'ouvrez pas les courriels** provenant d'une personne ou d'une organisation que vous ne connaissez pas. Si vous supprimez les courriels des expéditeurs que vous ne connaissez pas, cela vous permettra d'éviter un éventail de problèmes à l'avenir.
- Si vous ouvrez un de ces messages, **ne répondez pas aux pourriels**, car cela peut confirmer que votre adresse est active et vous recevrez ensuite encore plus de pourriels. Pour la même raison, ne cliquez jamais sur un lien de retrait ou de désabonnement qui se trouve dans un pourriel douteux. En cliquant sur ce lien, il se peut que vous vous abonniez involontairement à recevoir davantage de pourriels.
- **Ne cliquez jamais sur les liens ou les pièces jointes** d'un courriel si le message est douteux. Ils peuvent renfermer des logiciels malveillants (maliciels) qui pourraient mettre en péril vos renseignements personnels ou compromettre votre appareil s'ils sont déclenchés.

DIAPOSITIVE 9 – Points clés

Ne vous faites pas hameçonner!

- Les escroqueries en ligne peuvent être dissimulées de nombreuses façons. Il existe de nombreuses escroqueries montées dans le but de vous inciter à divulguer vos renseignements personnels, en particulier ceux qui concernent votre compte bancaire ou votre carte de crédit, dans une intention frauduleuse.
- Un des exemples les plus courants de ces types d'escroqueries est l'hameçonnage. L'hameçonnage est une forme d'escroquerie qui se sert du courrier électronique pour vous attirer sous de faux prétextes sur des sites Web en apparence bien légitimes où vous serez incité à fournir vos renseignements personnels. Ces courriels semblent parfois provenir de sources qui vous sont familières, comme des banques ou des organismes de secours en cas de catastrophe, mais ils sont en fait liés à des sites Web frauduleux.
- Pour éviter d'être victime d'un hameçonnage, méfiez-vous des courriels non sollicités et des pourriels provenant de sources inconnues ainsi que des hyperliens suspects insérés dans les messages diffusés sur les médias sociaux. Ils pourraient contenir des logiciels malveillants (maliciels) susceptibles d'endommager votre ordinateur et peut-être même de voler vos renseignements personnels. Méfiez-vous aussi des messages bizarres, même s'ils semblent avoir été envoyés par une personne de votre connaissance, puisque son compte pourrait avoir été piraté.
- Voici la règle d'or à suivre : n'ouvrez jamais de courriels ou de pièces jointes et ne cliquez pas sur les liens douteux si vous ne reconnaissez pas l'expéditeur du message. Et ne divulguez aucun renseignement personnel sur le Web à moins d'être certain de savoir à qui vous avez affaire. Vous pouvez aussi tenter d'authentifier le message en communiquant avec la personne ou l'organisation qui vous l'a supposément expédié.
- Enfin, vous avez raison de vous méfier des courriels provenant d'institutions financières, de fournisseurs de services Internet ou d'autres organisations qui vous demandent de leur fournir des renseignements personnels en ligne. Les entreprises dignes de confiance ne demandent jamais de renseignements personnels de cette manière.
- Si vous avez le moindre doute au sujet d'une organisation, vérifiez son numéro de téléphone dans l'annuaire ou utilisez le numéro inscrit au dos de la carte de crédit ou sur le relevé de compte et appelez-la. L'absence de salutations personnalisées, la menace de supprimer un compte si vous ne prenez pas de mesures particulières et la présence d'erreurs d'orthographe ou de grammaire sont des indices d'un courriel frauduleux.

Options facultatives aux fins de discussion : Vous recevez un courriel d'une banque que vous reconnaissez; ce courriel vous demande d'ouvrir une session afin de réactiver votre compte. Que devez-vous faire?

Réponse : Méfiez-vous toujours des courriels qui vous demandent d'ouvrir votre compte. Ne saisissez pas de renseignements personnels si vous avez des doutes. Communiquez avec votre banque par téléphone pour vérifier si le courriel est valide.

DIAPOSITIVE 10 – Points clés

Sécurité des réseaux sociaux

- Combien d'entre vous ont un compte Facebook ou d'un autre réseau social? Ces types de sites Web sont de plus en plus utilisés afin de garder contact avec ses amis et sa famille. Cet usage est formidable!
- Toutefois, avant de créer un profil, de publier une photo ou de dire ce que vous êtes en train de faire au monde entier, prenez le temps d'apprendre comment le site fonctionne en lisant les politiques relatives à la vie privée ainsi que les conditions d'utilisation, et pensez à ce que vous pouvez faire pour assurer votre sécurité en ligne.
- Si vous utilisez un site de réseau social, vous divulguez probablement des renseignements personnels en ligne. Et une fois qu'ils se trouvent dans le cyberespace, il se peut que vous perdiez tout contrôle sur ce qu'il en advient. Cela peut présenter un risque lié à la protection de vos renseignements personnels ou même vous exposer au vol d'identité ou à la fraude.

DIAPOSITIVE 11 – Points clés

Conseils de prudence sur les sites de réseautage social :

- **Assurez-vous de lire et de comprendre les politiques de protection de la vie privée.** Elles vous informent de ce qui advient de vos renseignements personnels et des options de confidentialité qui vous sont offertes.
- **Utilisez les contrôles de protection de la vie privée disponibles.** Les sites comme Facebook vous permettent de contrôler dans une certaine mesure vos renseignements personnels. Par exemple, vous pouvez limiter le nombre de personnes qui ont accès à votre profil et à vos photos ainsi que celles qui peuvent trouver votre profil par une recherche. Mettez-les à l'essai afin de déterminer lesquels vous conviennent. Lorsque vous publiez quelque chose en ligne, n'oubliez pas que cette publication peut être quasi permanente. Les gens peuvent prendre des photos ou des captures d'écran de ce que vous publiez, et ils peuvent continuer à le partager (avec des personnes qui ne font même pas partie de votre liste d'amis) même après que vous l'ayez supprimé. Il est important de réfléchir au contenu que vous publiez avant de le partager en ligne.
- **N'acceptez pas les demandes « pour devenir amis » de gens que vous ne connaissez pas dans la vraie vie.** Comment pouvez-vous savoir que ces personnes en ligne sont réellement qui elles disent être?
- **Quand vous affichez de l'information en ligne, soyez discret.** Réfléchissez bien au type de renseignements que vous affichez et à leurs implications. Une photo de vous et de vos amis, par exemple, peut en dire long : où vous habitez, l'école que vous fréquentez ou la voiture que vous conduisez.

Options facultatives aux fins de discussion : Un Canadien reçoit un message d'un utilisateur Facebook lui annonçant qu'il a gagné un prix à la loterie. Lorsque cet homme communique avec le

site, on lui demande d'envoyer 2 000 $ afin de réclamer son prix. Que devriez-vous faire dans cette situation?

Réponse : Ne répondez pas à cette demande.

DIAPOSITIVE 12 – Points clés

Questions à vous poser lorsque vous effectuez une transaction en ligne.

- De nos jours, le magasinage en ligne est un moyen facile et pratique qui vous permet de recevoir vos articles à domicile. Ce service est formidable, en particulier pour les personnes à mobilité réduite. Toutefois, il y a certaines choses que vous devez garder à l'esprit.
- Lorsque vous effectuez des transactions en ligne, posez-vous toujours les questions suivantes :
    - Quels renseignements recueille-t-on?
    - À quelles fins sont-ils recueillis? Ces renseignements sont-ils nécessaires à la transaction?
    - Sont-ils partagés avec quelqu'un d'autre?
    - Quelles seront les conséquences pour moi? Quels sont les risques?
- Vous devriez trouver des réponses à ces questions dans le site Web ou dans la politique de confidentialité de votre fournisseur de services de courriel, ou dans l'entente sur les modalités d'utilisation ou autres documents sur la protection des renseignements personnels qui doivent expliquer les politiques de l'entreprise en matière de collecte, d'utilisation, de divulgation et de protection de ces renseignements.
- Si vous avez toujours des doutes, adressez-vous directement au responsable de la protection des renseignements personnels de l'organisation. Si les politiques du site ne vous inspirent pas confiance, refusez de communiquer vos renseignements personnels, surtout les renseignements de nature sensible comme ceux qui ont trait à votre santé ou à vos finances.

DIAPOSITIVE 13 – Points clés

Protégez vos appareils mobiles avec des mots de passe solides.

- Un appareil mobile constitue un téléphone cellulaire, un iPod, un appareil de jeux portatif, une tablette ou tout autre appareil électronique que vous apportez avec vous.
- Si vous en avez un, vous avez probablement des renseignements personnels précieux enregistrés dans votre appareil, comme des photos, des messages textes, vos coordonnées et les coordonnées de votre famille et de vos amis.
- Si vous oubliez votre appareil mobile quelque part (comme au gymnase) et que l'écran n'est pas verrouillé par un mot de passe, n'importe qui peut le ramasser et accéder à vos

renseignements qui se trouvent sur l'appareil. Ensuite, cette personne peut facilement transmettre vos renseignements à d'autres personnes. Elle pourrait même se faire passer pour vous.
- Protégez toujours vos appareils mobiles qui contiennent vos renseignements par un mot de passe. Ainsi, si vous le perdez ou l'oubliez quelque part, vos données personnelles seront mieux protégées et vous courez moins de risque que quelqu'un essaie de se faire passer pour vous en ligne.

DIAPOSITIVE 14 – Points clés

- Réfléchissez avant de cliquer!
- Gardez à l'esprit que tout ce que vous affichez pourrait devenir permanent.
- Rappelez-vous que les choses que vous affichez ne sont pas nécessairement privées.
- Connaissez vos amis.
- Réglez vos paramètres de confidentialité.

DIAPOSITIVE 15 – Points clés

- Ne dites jamais où vous vous trouvez lorsque vous êtes en ligne.
- Ne partagez pas vos mots de passe et faites en sorte qu'ils soient toujours sûrs.
- Ne donnez pas vos renseignements financiers par courriel.
- Faites attention aux escroqueries.
- Protégez votre vie privée et celle des autres.

DIAPOSITIVE 16 – Points clés

- Cette présentation a été réalisée par le Commissariat à la protection de la vie privée du Canada. Le Commissariat a pour mission de protéger et de promouvoir le droit des Canadiens à la vie privée.
- Pour obtenir d'autres conseils sur la protection de vos renseignements personnels, veuillez consulter le site www.priv.gc.ca.