PENSEZCYBERSECURITE.CA

Protégez-vous en ligne.

Connaissez les risques.

Protégez-vous.

Protégez vos appareils.

TROUSSE D'INFORMATION

Canada

Contenu de la trousse d'information

Au sujet de la trousse d'information

Merci de l'intérêt que vous portez à la cybersécurité!

Octobre est le Mois de la sensibilisation à la cybersécurité, mais il est bon de promouvoir la sécurité en ligne en tout temps.

En jouant un rôle actif dans votre collectivité, vous aidez à instaurer une culture de cybersécurité au Canada. Alors que tous les ordres de gouvernement consacrent des efforts considérables à la protection des Canadiens contre les menaces en ligne, la cybersécurité est une responsabilité partagée entre les Canadiens, les gouvernements, le secteur privé et les partenaires internationaux.

L'enjeu

Chaque jour, les Canadiens entendent des histoires sur la vulnérabilité des ordinateurs aux virus, la nécessité pour tout le monde de protéger ses renseignements personnels en ligne et la persistance des manœuvres frauduleuses dans le monde virtuel. Nous pouvons perdre de l'argent, des biens, des souvenirs personnels, même notre propre identité d'un simple faux clic sur l'ordinateur ou l'appareil mobile.

Les recherches

Les liens ci-dessous mènent vers des recherches sur les croyances et les comportements des Canadiens quant à l'utilisation d'Internet et à la sécurité en ligne.

2012

Commissariat à la protection de la vie privée du Canada : Sondage auprès des Canadiens sur les enjeux liés à la protection de la vie privée, publié en 2012.
http://www.priv.gc.ca/information/por-rop/2013/por_2013_01_f.asp

2011

Étude préliminaire sur la cybersécurité, rapport publié par Sécurité publique Canada en 2011.
http://epe.lac-bac.gc.ca/100/200/301/pwgsc-tpsgc/por-ef/public_safety_canada/2011/index.html

2010

Enquête canadienne sur l'utilisation d'Internet, rapport publié par Statistique Canada en mai 2010.
http://www.statcan.gc.ca/daily-quotidien/100510/dq100510a-fra.htm

2009

Les Canadiens et la vie privée, rapport publié par le Commissariat à la protection de la vie privée du Canada en mars 2009.
http://www.priv.gc.ca/information/por-rop/2009/ekos_2009_01_f.asp

La campagne

Pensez cybersécurité est une campagne nationale de sensibilisation publique qui vise à informer les Canadiens de la sécurité sur Internet et des simples étapes à suivre pour se protéger en ligne. La campagne a pour objectif de rassembler tous les ordres de gouvernement, les secteurs public et privé et la communauté internationale afin d'aider les Canadiens à naviguer en toute sécurité en ligne.

Au sujet de la trousse d'information

Dirigée par Sécurité publique Canada, au nom du gouvernement du Canada et de ses partenaires, la campagne vous encourage, ainsi que tous les Canadiens, à jouer un rôle actif et judicieux pour vous protéger en ligne, ainsi que pour protéger votre famille, votre collectivité et votre pays contre la cybercriminalité.

La trousse d'information

La trousse d'information a été créée pour vous aider à promouvoir la cybersécurité par vos propres moyens et dans le cadre de vos activités, dans le monde réel aussi bien que dans le monde virtuel. Si vous avez des questions au sujet du contenu de la trousse ou de son utilisation, n'hésitez pas à communiquer avec nous, à l'adresse : **info@PensezCybersecurite.gc.ca**.

Le site Web

La pierre angulaire de la campagne est le site Web : **PensezCybersecurite.ca**.

Non seulement il fournit des renseignements pour aider les internautes à connaître les risques, à se protéger en ligne et à protéger leurs appareils, mais le site Web les encourage également à visionner des vidéos, consulter des infographies, lire des articles de blogues et encore plus.

Consultez le site Web tout au long de l'année pour demeurer au fait des plus récentes mesures en matière de sécurité en ligne.

Publications

Vous trouverez également dans la section Ressources du site Web **PensezCybersecurite.ca**, des produits qui vous permettront de transmettre les messages associés à la cybersécurité, notamment :

- Une brochure imprimable
- Une affiche

Affiche : Protégez-vous en ligne

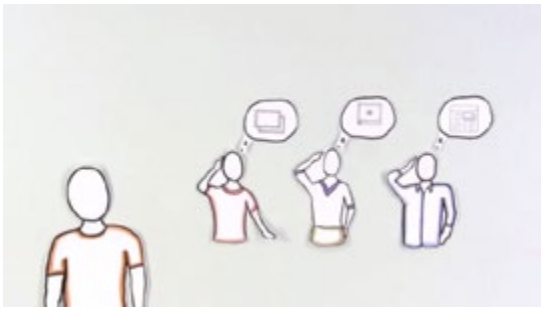
Une affiche faisant la promotion du site Web PensezCybersecurite.ca ainsi que les trois étapes à suivre pour naviguer sur le Web en toute sécurité : Connaissez les risques, Protégez-vous, Protégez vos appareils (11” x 17”).

Brochure : Protégez-vous en ligne — Mesures à prendre pour assurer la sécurité en ligne

Une brochure qui résume les trois étapes à suivre pour naviguer sur le Web en toute sécurité : Connaissez les risques, Protégez-vous, Protégez vos appareils.

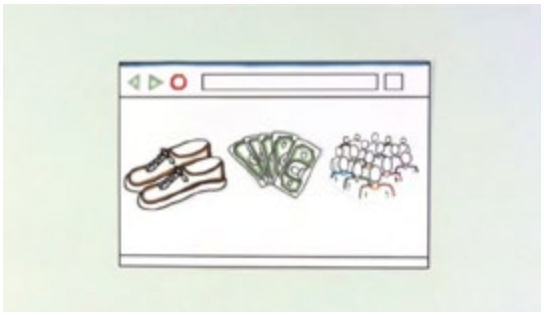
Vidéos

Toutes les vidéos peuvent être visionnées sur **PensezCybersecurite.ca** dans la section « Ressources ».



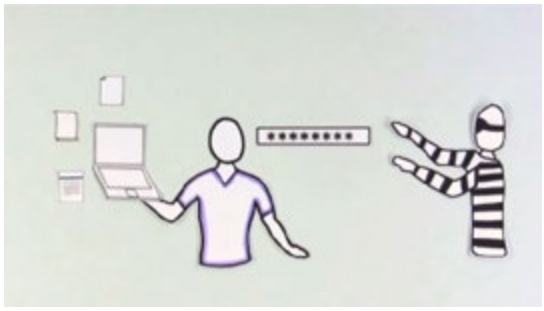
La protection de la cyber-réputation

Avant l'ère d'Internet, commettre un geste embarrassant n'occasionnait pas vraiment de conséquences. On en riait sur le moment et puis on passait à autre chose. Aujourd'hui, ces moments embarrassants peuvent être immédiatement partagés sur Internet et ils peuvent rester gravés à jamais, entachant ainsi votre réputation et celle de vos amis.



Les sites Internet sécurisés

Que ce soit pour l'achat de chaussures, la gestion de vos comptes ou le réseautage avec vos amis, les sites Internet font partie de notre vie. Or, il existe aujourd'hui de nombreux sites frauduleux conçus pour détourner votre argent ou transmettre vos données sensibles aux criminels.

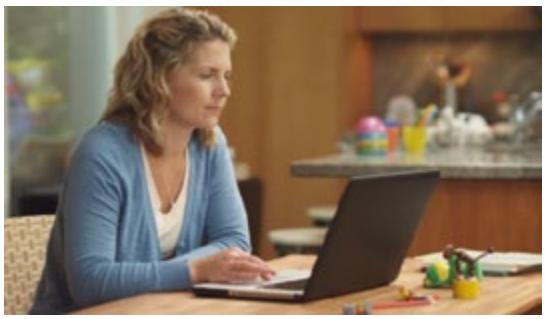


Les mots de passe sécurisés

Les mots de passe font partie de notre vie. Si nous ne les protégeons pas correctement, nous prenons de gros risques. En comprenant ces risques et en rendant nos mots de passe plus forts, nous serons en mesure de nous sentir plus en sécurité.

L'hameçonnage

L'hameçonnage est une menace en forte croissance sur Internet. Si vous connaissez les escroqueries, vous pourrez faire confiance aux entreprises avec qui vous faites affaire en ligne.



Publicité en ligne de Pensez cybersécurité

Protégez-vous contre les cybercriminels... c'est aussi simple qu'un clic.

Vidéos
(lancement en 2013-2014)

Moyens simples pour vous protéger sur les réseaux Wi-Fi publics

Une courte vidéo qui présente les étapes faciles que peuvent prendre les Canadiens pour se protéger lorsqu'ils utilisent des réseaux Wi-Fi publics.

Des moyens simples pour vous protéger lorsque vous utilisez votre appareil mobile

Cette vidéo explique comment utiliser votre appareil mobile en toute sécurité.

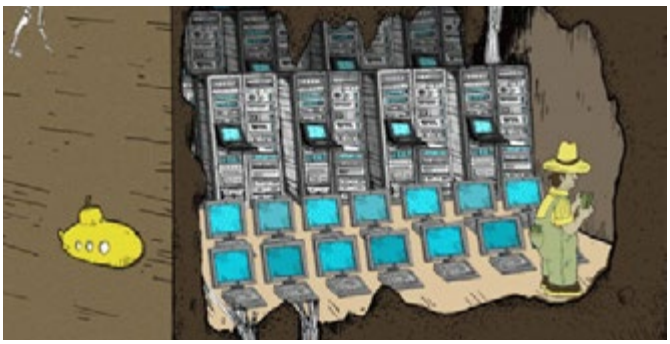
Des moyens simples pour vous protéger lorsque vous naviguez sur les réseaux sociaux

Cette vidéo offre des conseils pour profiter en toute sécurité des réseaux sociaux.

Infographies

Les infographies sont des représentations visuelles graphiques d'informations qui décrivent rapidement et clairement un sujet. Vous trouverez les infographies suivantes sur le site Web de PensezCybersecurite.ca, dans la section Ressources.

Vous trouverez toutes les infographies sur le site Web de **PensezCybersecurite.ca**, dans la section Ressources.



L'économie clandestine : les cybercrimes démasqués

Cette infographie expose littéralement le monde des cybercriminels et la façon dont ils utilisent nos renseignements personnels. L'illustration représente la cybercriminalité comme étant un monde douteux qui existe sous nos pieds.

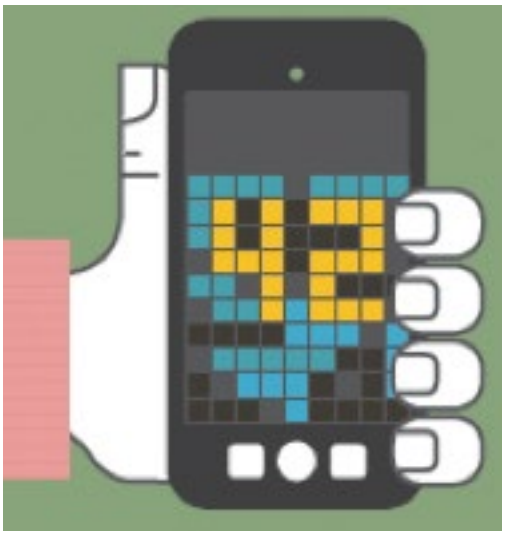
La cybercriminalité. Pourquoi les petites entreprises peuvent perdre beaucoup

Cette infographie amène le lecteur sur une route sinueuse qui s'étend à travers de petits villages, de grandes villes et de paysages ruraux pour les éduquer sur la façon dont la cybercriminalité peut toucher les petites entreprises.

Infographies

L’hameçonnage : combien de personnes en sont victimes?

Grâce à de faux courriels et des astuces, les hameçonneurs ratissent la cyber haute mer afin d’obtenir vos renseignements de comptes bancaires, numéros de carte de crédit et mots de passe. Environ 156 millions de courriels d’hameçonnage sont envoyés chaque jour partout dans le monde. Même si seulement une petite proportion des gens se fait prendre, les hameçonneurs frappent fort.



Rentrée scolaire – Conseils pour vos appareils

La nouvelle année scolaire vient avec plusieurs nouveautés : des appareils, des devoirs, des amis, mais aussi des risques. Soyez prudents, les criminels pourraient gâcher votre rentrée scolaire.

Fiches-conseils sur la cybersécurité

Ces fiches-conseils accompagnent à merveille vos nouveaux appareils électroniques. Elles présentent les étapes à suivre pour vous protéger et protéger votre nouvel appareil, et ce, dès son activation.

Jeu en ligne

Practical tips for online gaming.

Téléphone intelligent

Conseils pratiques pour un nouveau téléphone intelligent.

Portable

Conseils pratiques pour un nouveau portable.

Bannières Web
Pensez cybersécurité

Nos bannières Web sur lesquelles vous pouvez cliquer apparaissent sur notre page d'accueil. Vous les trouverez immédiatement en dessous du logo de Pensez cybersécurité et ils vous mèneront vers différentes sections du site Web qui comprennent de l'information pertinente.

Quelques exemples :

Boutons Web
Pensez cybersécurité

La présente trousse d'information contient aussi des boutons Web que vous pouvez placer bien en évidence sur les sites intranet et Internet de votre organisation afin de promouvoir la campagne **Pensez cybersécurité**.

Pour télécharger les boutons, veuillez consulter le site Web : **PensezCybersecurite.ca**

Boutons Web

Boutons pour le Mois de la sensibilisation à la cybersécurité :

Des boutons d'autres formats et de couleurs différentes sont disponibles.

Pour de plus amples renseignements, communiquez avec nous à l'adresse : **info@PensezCybersecurite.ca**.

Codes QR

Le concept des codes QR (Quick Response) s'apparente à celui des symboles CUP (codes universels des produits) qu'on voit sur les produits emballés. Avec son appareil mobile, un utilisateur peut balayer le code QR grâce à une application gratuite pour ouvrir la page Web en question.

Ainsi, vous pouvez vous connecter instantanément au site Web dont le code QR est indiqué sur une affiche ou une brochure.

Les codes QR suivants mènent au site Web, **PensezCybersecurite.ca**, et peuvent être inclus dans des documents imprimés.

Français

Anglais

Remarque : Lire un code QR équivaut à cliquer sur un lien Web; vous devez donc être vigilant lorsque vous lisez un code QR provenant d'une source peu fiable. Vous pouvez également faire en sorte que l'application qui lit le code QR affiche en même temps l'adresse URL et qu'elle vous demande si vous désirez vous connecter sur le site le site Web, plutôt que de le faire automatiquement. **Note : Soyez prudent lorsque vous téléchargez un code QR. Assurez-vous d'en connaître la source.**

Échanger sur les médias sociaux

La meilleure façon de véhiculer le message sur la cybersécurité est d'utiliser les modes de communication en ligne, où les utilisateurs font souvent face à des cybermenaces.

Utilisation des médias sociaux pour suivre et promouvoir la campagne PensezCybersecurite.ca

- Suivez **@cyber_securite** sur Twitter et encouragez les autres à faire de même (des microbillets sur la cybersécurité y sont diffusés quelques fois par semaine).
- « Aimez » Pensez cybersécurité sur Facebook : www.facebook.com/pensezcybersecurite
- Affichez le contenu pertinent du site Web **PensezCybersecurite.ca** sur votre page Facebook, sur vos tableaux Pinterest ou sur Twitter (voir ci-dessous un exemple de contenu d'un microblogue).
- Communiquez des renseignements pertinents à un blogueur dont le domaine de la cybersécurité intéresse.
- Affichez le contenu pertinent du site Web **PensezCybersecurite.ca** sur votre blogue.
- Soumettez une histoire, un incident ou des pratiques exemplaires liés à la cybersécurité au site Web **PensezCybersecurite.ca** (par courriel à l'adresse : **info@PensezCybersecurite.ca**).

Exemples de microbillets

Composez des mots de passe difficiles. Mémorisez-les et changez-les souvent. **PensezCybersecurite.ca** #cybersecurite #conseils

Mettez à jour vos paramètres de confidentialité sur vos sites de réseautage social. Consultez **PensezCybersecurite.ca** #cybersecurite #conseils

Renseignez-vous sur logiciels malveillants qui attaquent appareils mobiles/mesures pour les prévenir. **PensezCybersecurite.ca** #cybersecurite

Demeurez au fait des risques du magasinage et des enchères en ligne. Pensez cybersécurité : **PensezCybersecurite.ca** #cybersecurite

Messages sur Facebook ne devraient être lus que par ceux autorisés. Vérifiez paramètres de confidentialité : **PensezCybersecurite.ca**

Prenez l'habitude de créer des copies de sauvegarde. Consultez les nombreuses solutions affichées sur le site Web : **PensezCybersecurite.ca**

Vous envisagez d'installer un pare-feu? Recherchez les programmes d'entreprises fiables et lisez les critiques : **PensezCybersecurite.ca**

Vous utilisez réseau Wi-Fi à la maison? N'oubliez pas paramètres protection pour ne pas que d'autres en profitent : **PensezCybersecurite.ca**

Échanger sur les médias sociaux

Institution bancaire ne demandera jamais no carte de crédit/mot de passe dans un courriel : **PensezCybersecurite.ca** #cybersecurite #conseils

Parents peuvent aider enfants/ados à utiliser outils de réseautage social de façon sécuritaire, grâce aux conseils de **PensezCybersecurite.ca**

Utilisez-vous plus d'un navigateur Internet? Assurez-vous que paramètres de sécurité sont bien configurés. **PensezCybersecurite.ca**

Connaître menaces en ligne vous aide à vous protéger, et à protéger votre famille, contre cyberattaques. **PensezCybersecurite.ca**

Afin d'accroître nos connaissances sur la cybersécurité,octobre est le Mois sensibilisation cybersécurité au #Canada : **PensezCybersecurite.ca**

Durant le Mois sensibilisation cybersécurité, revoyez vos pratiques en ligne pour assurer votre sécurité : **PensezCybersecurite.ca**

Mois sensibilisation cybersécurité : Rappelez à vos amis/membres famille la nécessité de se protéger en ligne : **PensezCybersecurite.ca**

Mois sensibilisation cybersécurité : Renseignez-vous au sujet des cybermenaces courantes, en consultant **PensezCybersecurite.ca**.

Mois sensibilisation cybersécurité : Votre appareil mobile comporte-t-il des risques? Étapes pour le sécuriser : **PensezCybersecurite.ca**

Mois sensibilisation cybersécurité :Fermons la porte aux cybercriminels. Voici ce qu'il faut faire : **PensezCybersecurite.ca**

Échanger sur les médias sociaux

Utilisation de mots clics

Un mot clic est un mot ou une expression (sans espace) précédé d'un dièse (#) utilisé pour désigner un microbillet qui porte sur un sujet d'intérêt particulier. Ajoutez le mot clic #cybersecurite à vos microbillets lorsque vous participez à une conversation en ligne dont le sujet est la cybersécurité. L'utilisation du mot clic permet aux autres internautes de trouver plus facilement vos microbillets lorsqu'ils recherchent des messages sur le thème de la cybersécurité.

Facebook

Lancée en 2013, notre page Facebook **www.Facebook.com/PensezCybersecurite** fournit de l'information pour aider les Canadiens à en apprendre davantage sur la cybersécurité et les mesures à prendre, individuellement, pour se protéger. Notre contenu est également destiné à être utilisé et partagé par d'autres organisations.

Blogage

Si vous avez un blogue personnel ou organisationnel, il est facile de véhiculer le message de la cybersécurité aux personnes qui suivent votre blogue. Vous pouvez rédiger votre propre article, en vous inspirant des renseignements affichés sur le site Web **PensezCybersecurite.ca**, ou vous servir du modèle suivant en l'adaptant à vos besoins.

Modèle de billet d'un blogue

Conseils simples qui vous aident à naviguer en toute sécurité en ligne

Lorsque vous êtes en ligne, que ce soit pour des transactions bancaires, du réseautage avec les amis ou pour des activités de travail, d'apprentissage ou de divertissement, vous n'êtes jamais seul. Lorsque vous êtes dans une place publique très fréquentée, vous assurez la protection de vos arrières, de votre famille, de votre portefeuille et de vos effets personnels; vous devriez être tout aussi prudent quand vous naviguez dans le monde virtuel achalandé.

Vous pouvez facilement apprendre à vous protéger en ligne, tout comme vous l'avez appris pour « circuler en toute sécurité » dans la rue, si vous considérez la cybersécurité comme une priorité et que vous consacrez du temps pour vous renseigner des risques et menaces les plus courants dans le monde virtuel.

Le site Web de Sécurité publique Canada, **PensezCybersecurite.ca**, présente trois étapes simples que vous pouvez suivre pour assurer votre propre sécurité en ligne, ainsi que la sécurité de votre famille et de vos biens :

- Connaissez les risques
- Protégez-vous
- Protégez vos appareils

Le site fournit des conseils très faciles à suivre qui vous aident, par exemple, à créer et à protéger des mots de passe, à faire des transactions et des achats en ligne de façon plus sécuritaire, à ne pas être victime de pourriels et de manœuvres frauduleuses, et à protéger votre identité, vos renseignements et votre famille.

Pensez cybersécurité est une campagne nationale de sensibilisation publique qui vise à informer les Canadiens de la sécurité sur Internet et des simples étapes à suivre pour se protéger en ligne. La campagne a pour objectif de rassembler tous les ordres de gouvernement, les secteurs public et privé et la communauté internationale afin d'aider les Canadiens à naviguer en toute sécurité en ligne.

Dirigée par Sécurité publique Canada, au nom du gouvernement du Canada et de ses partenaires, la campagne vous encourage, ainsi que tous les Canadiens, à jouer un rôle actif et judicieux pour vous protéger en ligne, ainsi que pour protéger votre famille, votre collectivité et votre pays contre la cybercriminalité.

Apprenez en plus sur **PensezCybersecurite.ca**! Vous pouvez également suivre Pensezcybersecurite sur Twitter (@cyber_securite) et sur Facebook pour connaître les plus récents conseils de sécurité.

Le téléphone intelligent change tout

Conseils de sécurité simples pour utilisateurs de téléphone intelligent

Le réveil vient de sonner. Vous appuyez encore une fois sur le bouton de rappel d'alarme pour voler un petit peu plus de sommeil à la nuit. Puis, vous vous réveillez et vous vous rendez compte que vous allez être en retard au travail. Vous sautez précipitamment du lit, courez vous doucher et vous brosser les dents, buvez en vitesse ce café dont vous aviez désespérément besoin, puis vous passez la porte, à temps. Dans l'autobus, vous cherchez votre téléphone intelligent, histoire de commencer votre journée du bon pied. À votre grand désespoir, vous ne le trouvez nulle part. Tout à coup, vous vous sentez mal et vous vous demandez comment vous allez faire pour survivre toute la journée sans cet appareil.

Cela vous rappelle quelque chose? Soyons honnêtes, nous sommes constamment branchés à nos appareils mobiles. Ils sont devenus tellement essentiels que nous nous sentons perdus sans eux.

En relativement peu de temps, les téléphones cellulaires se sont transformés. Nous sommes passés du téléphone traditionnel à un appareil qui compte maintenant plus de fonctions qu'un ordinateur personnel. Nous nous en servons pour recevoir nos courriels, fréquenter les réseaux sociaux, prendre des photos et conserver les coordonnées de toutes nos connaissances. L'appareil nous sert aussi à accéder aux sites bancaires mobiles, à naviguer sur Internet, à utiliser des applications, et bien plus encore.

Avec tous ces accessoires et gadgets au bout des doigts, nous devons plus que jamais protéger notre appareil. Vous pouvez éviter les menaces potentielles en suivant ces conseils :

- Protégez votre téléphone par mot de passe. Tous les appareils mobiles peuvent être verrouillés par un mot de passe ou un code numérique. Voilà un conseil tout simple qui vous permettra de protéger vos renseignements personnels si votre appareil était perdu ou volé.
- Activez le verrouillage automatique de votre mot de passe de sorte que votre appareil se verrouille après une courte période d'inactivité.
- Évitez de vous connecter à des réseaux Wi-Fi inconnus ou non protégés par mot de passe, même s'ils sont privés. Un réseau sans fil non sécurisé peut compromettre vos renseignements, y compris la liste de vos connaissances, et peut même donner à quelqu'un d'autre l'utilisation de votre forfait de données.
- Interrogez-vous sur ce que vous devez absolument conserver sur votre appareil mobile, et supprimez tout le reste. Si votre appareil est perdu ou volé, vous risquez d'avoir donné sans le vouloir vos renseignements personnels à une autre personne.
- Réfléchissez avant de vous procurer une application. Avant de la télécharger, sachez à quels renseignements l'application peut accéder et si elle peut les partager.
- Utilisez un dispositif de recherche de téléphone : activez le service ou utilisez une application sûre qui vous permettra de rechercher votre téléphone. Ce type de dispositif vous permet de verrouiller ou de supprimer les données contenues dans le téléphone si l'appareil est perdu ou volé.

Plusieurs parmi nous ne peuvent plus se passer de leur appareil mobile. Protégez-vous en ligne. Pour en savoir davantage, consultez le site PensezCybersecurite.ca.

Apprenez la cybersécurité à vos enfants

Les jeunes Canadiens grandissent aujourd'hui dans un monde numérique. Toute leur enfance, ils sont appelés à utiliser des ordinateurs, des caméscopes, des téléphones cellulaires, des consoles de jeux en ligne et Internet. Les communications par voie numérique font partie intégrante de leur vie et bon nombre d'entre eux ont une adresse électronique et sont abonnés à des réseaux sociaux avant même d'entrer au secondaire. Leurs téléphones cellulaires servent à envoyer des messages textes, à prendre des photos et à envoyer le tout à des amis.

Les activités en ligne peuvent permettre aux enfants de vivre des expériences tout à fait enrichissantes. En fait, de nombreux avantages du point de vue éducatif sont associés à Internet, mais c'est aussi un outil qui peut être dangereux. Ce monde hyperconnecté est caractérisé par de nouvelles menaces qui apparaissent constamment, en particulier parce que les données enregistrées le sont de façon permanente. Ainsi, tout ce que vos enfants disent, affichent et partagent en ligne aujourd'hui peut refaire surface et leur causer toute une surprise à l'âge adulte.

Nous disons à nos enfants de regarder des deux côtés avant de traverser la rue et nous leur recommandons de ne pas parler aux étrangers, mais il faut aussi leur enseigner à utiliser Internet en toute sécurité, ce qui est aussi important. Souvent les parents ne connaissent pas les récents dangers liés à l'utilisation d'Internet ou ne savent pas vraiment ce que leurs enfants font lorsqu'ils sont en ligne. Rassurez-vous : il existe des endroits fiables où vous trouverez les renseignements dont vous avez besoin. Voici, pour commencer, quelques conseils pour faire en sorte que vos enfants soient informés et protégés :

- Apprenez à connaître les sites Web que vos enfants utilisent et montrez-leur ce qu'ils doivent faire s'ils tombent sur un contenu inapproprié.
- Discutez avec eux des répercussions d'un affichage de photos inappropriées, en leur mentionnant que la diffusion d'observations désobligeantes sur des personnes peut détruire une réputation ou mettre fin à une amitié.
- Rappelez-leur qu'Internet est un lieu public et que toutes les données sont conservées. Ce qu'ils font ou divulguent sur des sites peut avoir des conséquences plus tard.

Montrez l'exemple et enseignez à vos enfants comment utiliser Internet en toute sécurité.

Protégez-vous en ligne. Pour en savoir davantage, consultez le site PensezCybersecurite.ca.

Promotion à l'interne

Vous pouvez également promouvoir le *Mois de la sensibilisation à la cybersécurité*, en octobre, en mobilisant vos collègues ou vos employés.

Voici un modèle de courriel :

> Le mois d'octobre est le Mois de la sensibilisation à la cybersécurité; c'est également le temps d'aider les Canadiens à se protéger et à protéger leurs familles contre un éventail de menaces en ligne.
>
> Dirigée par Sécurité publique Canada, la campagne Pensez cybersécurité vise à sensibiliser les Canadiens aux menaces qui les guettent en ligne, et à les informer des mesures simples à prendre pour réduire les risques autant que possible.
>
> Nous avons tous un rôle important à jouer pour assurer la sécurité de nos ordinateurs, de nos appareils personnels et de nos entreprises contre les cybermenaces. De simples mesures sont requises :
>
> - savoir reconnaître les courriels suspects
> - créer des mots de passe sécuritaires pour tous les appareils
> - savoir reconnaître les sites Web non fiables
> - ne pas oublier d'éteindre l'ordinateur la nuit
>
> De simples mesures de protection comme celles-ci peuvent nous aider à ne pas être la prochaine victime d'un cybercriminel.
>
> Je vous encourage fortement à en apprendre davantage à ce sujet, en visitant le site Web : PensezCybersecurite.ca, et à en parler aux autres.
>
> Parce que vous pouvez tout perdre. Ou vous pouvez tout protéger. C'est si simple.
>
> [Signature]

Utilisez le bloc-signature suivant dans tous vos courriels pour faire la promotion du Mois de la sensibilisation à la cybersécurité. Vous pouvez le télécharger sur le site **PensezCybersecurite.ca**

Si vous avez un site intranet, vous pouvez également utiliser les boutons Web Pensez cybersécurité pour faire la promotion du *Mois de la sensibilisation à la cybersécurité* et utiliser un lien menant à **PensezCybersecurite.ca**.

Personnes-ressources

Avez-vous besoin de plus de renseignements sur la sécurité en ligne?

Les demandes de renseignements généraux sur la Stratégie de cybersécurité du Canada ou la Campagne peuvent être soumises à Sécurité publique Canada, aux numéros de téléphone : 613-944-4875 ou 1-800-830-3118, ou par courriel à l'adresse : **info@PensezCybersecurite.ca**.

Nota : Les avis d'escroquerie, de fraude ou de vol d'identité ne devront pas être soumis à Sécurité publique Canada. Les enquêtes sur les cybercrimes sont la responsabilité des organismes d'application de la loi.

Autres ressources :

Stratégie de cybersécurité du Canada : http://www.securitepublique.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/index-fra.aspx

Centre canadien de réponse aux incidents cybernétiques : http://www.securitepublique.gc.ca/cnt/ntnl-scrt/cbr-scrt/ccirc-ccric-fra.aspx

Centre antifraude du Canada : 1-888-495-8501 http://www.antifraudcentre-centreantifraude.ca/

La Loi canadienne anti-pourriel : http://fightspam.gc.ca/eic/site/030.nsf/fra/accueil

Commissariat à la protection de la vie privée du Canada : http://www.priv.gc.ca/index_f.asp

Ressources internationales (sites disponibles en anglais seulement) :

STOP. THINK. CONNECT. (États-Unis) : http://stopthinkconnect.org/

Get Safe Online (Royaume-Uni) : http://www.getsafeonline.org/

Stay Smart Online (Australie) : http://www.staysmartonline.gov.au/

Security Central (Nouvelle-Zélande) : http://www.securitycentral.org.nz/

No de cat. : PS9-2/2013F-PDF
ISBN : 978-0-660-21293-7