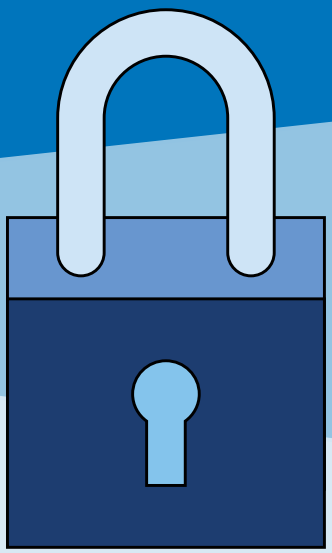
Trousse de cybersécurité

Protégez votre entreprise des cybermenaces



ASSOCIATION DES BANQUIERS CANADIENS

En partenariat avec

PENSEZCYBERSECURITE.CA

Une trousse préparée par l'Association des banquiers canadiens en vue d'aider les propriétaires et les gestionnaires de petites entreprises à comprendre les menaces à leur cybersécurité et à adopter des mesures efficaces pour se protéger et protéger leurs employés.

Nous sommes tous concernés. Les banques au Canada ne ménagent aucun effort pour détecter et éviter les cybermenaces. Elles collaborent étroitement entre elles, ainsi qu'avec les organismes de réglementation, les forces de l'ordre et tous les niveaux de gouvernement afin de protéger leurs clients, de même que le système financier dans son ensemble, contre le cybercrime. En tant que propriétaire ou gestionnaire d'une petite entreprise, vous pourrez adopter de simples mesures vous permettant de déceler les cybermenaces et de vous en protéger.

Contenu

Fondements de la cybersécurité

pour petites entreprises

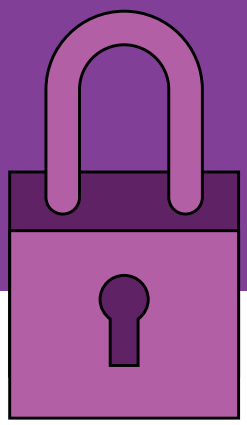
La prépondérance du numérique dans l'économie d'aujourd'hui signifie que les entreprises, petites ou grandes, utilisent Internet pour gérer leurs opérations, servir leurs clients et poursuivre leur croissance.

Les cybercriminels visent les petites entreprises vu qu'elles n'auraient pas nécessairement les moyens de mettre en place de solides mesures de sécurité. En tant que propriétaire d'une petite entreprise, vous devez être toujours conscient des mesures de cybersécurité afin de réduire les risques, surtout qu'il n'est pas nécessaire d'être un expert en informatique pour adopter des pratiques de cyberhygiène efficaces.

Que doit comporter un plan de cybersécurité?

Un plan de cybersécurité doit inclure :

- Des procédures de protection pour les données, les ordinateurs et les réseaux de l'entreprise contre les cyberattaques.
- La formation obligatoire des employés sur les principes de sécurité et la détection des escroqueries qui visent particulièrement les petites entreprises.
- Des processus de réaction aux enjeux de cybersécurité et un plan pour mettre à jour et calibrer les mesures de sécurité selon les changements dans les vulnérabilités de l'entreprise.



Qu'est-ce que la cybersécurité?

La cybersécurité est un ensemble de procédures établi dans l'objectif de protéger les réseaux, les systèmes, les employés et les données de votre petites entreprises contre les cybermenaces. Les cybercriminels visent les petites entreprises afin de récolter des données qu'ils pourront utiliser pour lancer des attaques dont l'objectif est de voler des renseignements ou de l'argent propres à l'entreprise ou à ses clients.

Liste de vérification de la cyberhygiène

protection des données, des ordinateurs et des réseaux de votre entreprise contre les cyberattaques

Pour que le risque de cybermenaces envers votre entreprise diminue, votre plan de cybersécurité devra inclure ces cinq étapes.

1. Installation des outils de sécurité adéquats

Installez un antivirus, un antimaliciel et un pare-feu sur tous les réseaux et les appareils connectés de votre entreprise. Ces programmes doivent être régulièrement activés et maintenus à jour pour veiller à la protection de vos données contre les maliciels.

2. Création de mots et de phrases de passe distincts et compexes

Utilisez des mots de passe distincts et complexes pour tous vos comptes et vos services Internet. Incitez vos employés à faire de même. Vous trouvez des conseils sur la création de phrases de passe sur le site de l'ABC : https://cba.ca/choose-a-better-password?l=fr.

3. Mises à jour des systèmes d'exploitation et des applications

Utilisez la version la plus récente du système d'exploitation de vos ordinateurs et de vos appareils connectés. Chaque nouvelle version comporte d'importants correctifs de sécurité pour vous faire éviter les failles connues. L'automatisation des mises à jour du système d'exploitation, des applications et des périphériques veillera à l'installation des importants correctifs de sécurité qui vous protègeront des récentes menaces.

4. Programmation des sauvegardes régulières des données

Sauvegardez fréquemment vos fichiers sur des plateformes externes. Également, instaurez des procédures claires pour récupérer les fichiers ainsi sauvegardés et prévoyez une liste de vérification de ces sauvegardes régulières. Le guide Pensez cybersécurité pour les petites et moyennes entreprises, conçu par le gouvernement du Canada, présente à la section 7.1 plusieurs options de sauvegarde et de restauration pour les données et les fichiers de l'entreprise.

Liste de vérification de la cyberhygiène (Suite)

5. Désactivation des réseaux de partage de fichiers

Les réseaux de partage de fichiers, appelés aussi « pair à pair », sont populaires parce qu'ils permettent aux utilisateurs de télécharger toutes sortes de fichiers et de programmes informatiques entre des réseaux mondiaux. Toutefois, l'utilisation de ces réseaux est considérée comme une activité à risque élevé. En effet, ces réseaux sont régulièrement utilisés par des criminels pour distribuer des fichiers répréhensibles ou illégaux, de même que des virus insérés dans des téléchargements qui semblent autrement inoffensifs, comme des chansons populaires, des films, etc.

6. Installation d'un coupe-feu

Installez un coupe-feu pour protéger le système de votre entreprise du trafic malveillant sur Internet.

Le coupe-feu balaie le trafic sur votre réseau et bloque les mouvements indésirables. Le site Pensez cybersécurité du gouvernement fédéral explique le rôle du coupe-feu dans le processus de sécurité.

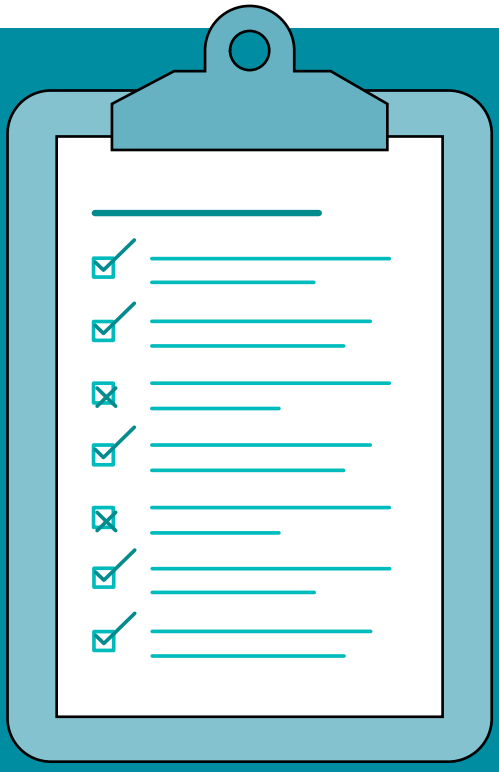
7. Utilisation d'une passerelle RPV

Prévoyez une passerelle RPV (réseau privé virtuel) pour que vous et vos employés ayez un accès à distance sécurisé et chiffré au réseau de l'entreprise. Le site Web du Centre canadien de cybersécurité explique comment fonctionnent les RPV et liste les divers genres de RPV.

8. Éducation des employés

L'une des principales lignes de défense contre les cyberattaques est une main-d'œuvre sensibilisée à la cybersécurité.

Veillez à l'adoption de politiques et de procédures destinées à la gestion des données propres à votre entreprise et offrez à vos employés des conseils sur la cybersécurité qui soient simples, pratiques et facilement applicables. En cas d'atteinte à la cybersécurité de votre entreprise, vos employés devraient être fin prêts à agir.



Votre liste de vérification de la cyberhygiène

- [ ] Installation des outils de sécurité adéquats
- [ ] Création de mots et de phrases de passe distincts et compexes
- [ ] Mises à jour des systèmes d'exploitation et des applications
- [ ] Programmation des sauvegardes régulières des données
- [ ] Désactivation des réseaux de partage de fichiers
- [ ] Installation d'un coupe-feu
- [ ] Utilisation d'une passerelle RPV
- [ ] Éducation des employés

Survol des escroqueries les plus fréquentes

Les propriétaires et administrateurs de petites entreprises doivent savoir identifier et garder à l'œil un ensemble d'arnaques destinées principalement aux petites entreprises. Notamment :

- Hameçonnage
- Rançongiciel
- Fraude du courriel d'entreprise compromis

Il est utile de connaître les tactiques utilisées par les cybercriminels pour vous leurrer, vous et vos employés, en vue de leur révéler des renseignements importants sur l'entreprise.

INGÉNIERIE SOCIALE : ne vous laissez pas duper

L'ingénierie sociale est le processus par lequel des criminels exploitent la nature humaine – et notre soif de répondre aux demandes urgentes, d'être utiles ou d'aider un ami dans le besoin – afin de leurrer leurs victimes dans la perspective d'obtenir des renseignements personnels qui seront utilisés aux fins de fraude financière.

Lorsqu'il s'agit de cybersécurité, les systèmes de sécurité informatique les plus performants ne peuvent rien contre le fait que des utilisateurs dupés révèlent leurs coordonnées de connexion ou autres renseignements personnels.

Au lieu d'utiliser les techniques de piratage et mener une cyberattaque, les criminels utilisent l'ingénierie sociale pour manipuler psychologiquement, dans l'espoir de faire croire leurs histoires.

3 signaux d'ingénierie sociale

01 **Usage de la peur comme motivation.** Les courriels, les appels et les textos menaçants ou intimidants sont des techniques d'ingénierie sociale utilisées afin de motiver le receveur à accéder aux demandes de renseignements personnels ou de fonds.

02 **Courriels ou textes suspects.** Ces messages, qui contiennent des demandes urgentes pour des renseignements personnels, sont une flagrante indication qu'on essaie de vous arnaquer.

03 **Offres impossibles à croire ou comportant des demandes inhabituelles.** Attention, si un de vos contacts en ligne vous offre un accès gratuit à une application, à un jeu ou à un programme en échange de vos coordonnées de connexion! Également, les offres gratuites en ligne comportent souvent une logique malveillante.

Hameçonnage : détectez ces arnaques

Les courriels frauduleux existent depuis qu'il est possible de taper et de cliquer pour envoyer un message sur Internet. Ce qui a changé, c'est la capacité des fraudeurs à cibler leur arnaque pour vous tromper davantage et vous pousser, vous et vos employés, à leur virer de l'argent ou à leur divulguer des données financières.

Voici quelques signes que le courriel reçu est un hameçon :

Exigences et menaces

La demande de renseignements est-elle justifiée? Votre banque ne vous enverra jamais de courriel menaçant ni ne vous téléphonera pour exiger la divulgation de renseignements personnels, comme votre mot de passe, le numéro de votre carte de débit ou de crédit ou le nom de jeune fille de votre mère.

Expéditeur douteux

Vérifiez l'adresse électronique de l'expéditeur. Le texte dans le champ de l'expéditeur peut sembler celui de l'organisation, mais l'adresse électronique qui y est rattachée ne l'est pas nécessairement. Pour vérifier, il suffit de placer votre curseur au-dessus du nom, sans cliquer.

Pièces jointes et liens douteux

Les courriels hameçons contiennent souvent des liens qui ont l'air légitimes, mais conduisent plutôt à des sites frauduleux. Là également, il suffit de placer le curseur au-dessus du lien pour voirsi l'adresse du site vers lequel il mène correspond au nom affiché. Par ailleurs, n'ouvrez jamais des pièces jointes auxquelles vous ne vous attendez pas.

Avertissements

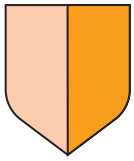
Avertissements que votre compte sera fermé ou l'accès à votre compte sera limité si vous ne répondez pas aux demandes dans le courriel.

Testez vos habiletés et celles de vos collègues à reconnaître une arnaque, avec les questionnaires de l'ABC : https://abccybersecurite.ca

Rançongiciels : protégez vos fichiers

Un rançongiciel est un logiciel malveillant, ou maliciel.

Une fois que le maliciel est installé sur votre ordinateur, rien n'arrivera jusqu'à ce que des pirates informatiques s'en emparent et cryptent vos fichiers. Lorsque les fichiers sont cryptés (verrouillés), les fraudeurs exigeront le paiement d'une rançon pour les décrypter et les déverrouiller. Rappelez vous, toutefois, que rien ne garantit le déverrouillage de ces fichiers une fois la rançon payée ni la vente des données ou leur divulgation en ligne.



Comment protéger votre entreprise des rançongiciels

Installez des logiciels de protection antivirus et anti-maliciels sur votre réseau, et gardez ces logiciels à jour.

Prenez le temps d'installer la plus récente version de vos systèmes d'exploitation et de vos applications.

Sauvegardez fréquemment vos fichiers sur des systèmes de stockage externes, comme un disque dur externe ou une plateforme infonuagique, qui ne sont pas reliés à votre ordinateur. S'ils le sont, vos données ainsi sauvegardées pourraient être verrouillées également.

Faites preuve de prudence! Ne cliquez pas sur des liens ni n'ouvrez des pièces jointes provenant d'adresses inconnues et désactivez les macros – vous pourriez par inadvertance télécharger des maliciels en activant des macros, et en cliquant sur une pièce jointe, un lien ou une fenêtre contextuelle en ligne.

Sensibilisez vos employés à l'importance de l'usage responsable d'Internet.

Que faire si vous en êtes victime?

Il serait bien difficile de déverrouiller vos fichiers et de supprimer le rançongiciel de votre système informatique. Si votre entreprise est victime d'un rançongiciel, envisagez les actions suivantes :

Consultez votre fournisseur de logiciel antivirus.
Si vous vous connaissez en récupération de données, vous pourrez essayer de supprimer les logiciels malveillants vous-même. Certains fournisseurs peuvent déceler ce maliciel et offrir des instructions et des logiciels pour remédier au problème.

Consultez un spécialiste de la sécurité informatique.
Un professionnel peut être en mesure de vous aider à supprimer le rançongiciel et à restaurer vos fichiers si vous les avez sauvegardés.

Changez vos mots de passe.
Changez tous vos mots de passe en ligne, en particulier ceux qui donnent accès aux comptes bancaires en ligne de l'entreprise. Ainsi, les criminels ne pourront pas accéder à vos comptes s'ils arrivent à récupérer vos mots de passe.

Signalez la fraude.
Informez-en le service de police local et le Centre antifraude du Canada.

Fraude du courriel d'entreprise compromis

La fraude du courriel d'entreprise compromis se présente sous divers types de fraude avancés et vise autant les petites entreprises que les grandes.

Voici comment identifier les fraudes visant votre entreprise :

Faux dirigeants

Des courriels frauduleux semblent provenir du chef de la direction ou du chef des finances de l'entreprise – ou d'un autre dirigeant –, adressés à un employé du service de la comptabilité ou des finances. Dans ces courriels, le supposé haut dirigeant intime au récipiendaire de virer des fonds à une tierce partie, dans l'immédiat et en toute confidentialité.

Hameçonnage des fournisseurs

Des courriels frauduleux semblent provenir d'un fournisseur avec lequel votre entreprise entretient une longue relation de travail. Dans ces courriels, le prétendu fournisseur vous demande d'effectuer le paiement d'une facture par transfert électronique de fonds à un compte frauduleux.

Vol de renseignements

Des criminels font des demandes, légitimes en apparence, pour des renseignements financiers essentiels, comme des déclarations fiscales, ou autres renseignements confidentiels au sujet de l'entreprise. Ces renseignements serviront à commettre des actes frauduleux.

Comment éviter les fraudes par courriel visant l'entreprise

Éducation

Apprendre aux employés à rester vigilants, car les comptes électroniques de l'entreprise peuvent être compromis, et leur montrer comment détecter ces arnaques. Le signal d'alarme le plus retentissant pour ce genre de fraude est la demande urgente d'un transfert électronique de fonds.

Vérification

Dans le cas de transferts électroniques de fonds, le Centre antifraude du Canada recommande aux entreprises d'établir un processus de vérification à deux étapes afin qu'il y ait un second responsable qui pourra confirmer la validité de la demande.

Prudence

Les renseignements qui seront affichés en ligne ou dans les médias sociaux au sujet des déplacements des hauts dirigeants de l'entreprise pourront être utilisés par des criminels. Il faut toujours être méfiant durant ces périodes.

Protection

Les logiciels de protection – antivirus et autres – doivent, en tout temps, être à jour et fonctionnels sur tous les ordinateurs, appareils informatiques et serveurs de l'entreprise. Vous devez également protéger le domaine de courriel. Utilisez un logiciel contre l'hameçonnage qui correspond au protocole DMARC.

Si votre entreprise est victime...

Aussitôt que vous apprenez qu'un transfert de fonds a été fait à la suite d'une demande frauduleuse, communiquez avec votre banque et signalez l'incident à la police.

Protection des données personnelles des clients

Souvent, les petites entreprises sont visées par les cybercriminels qui croient que ces entreprises n'ont ni les ressources ni les connaissances nécessaires pour adopter les mesures de cybersécurité pertinentes.

À titre de petite entreprise, deux de vos plus importants atouts sont votre personnel et les renseignements financiers de vos clients qui sont en votre possession. Vos clients ont confiance que vous garderez leurs données en sécurité et que vous disposez des procédures et des processus adéquats à la protection de leurs renseignements personnels contre les cybercriminels.

À cette fin, vous devrez suivre une méthode de classification des renseignements de nature délicate et émettre des lignes directrices pour vos employés pour savoir comment traiter de tels renseignements.

1. Classifiez et étiquetez correctement vos données sensibles

La première mesure de protection des données de nature délicate que votre entreprise détient est la classification et l'étiquetage adéquats de ces données. La section 7.3 du Guide Pensez cybersécurité pour les petites et moyennes entreprises donne les recommandations suivantes pour un simple modèle de classification :

Renseignements publics

Ces données sont accessibles à tous dans votre entreprise aussi bien qu'à l'extérieur et n'exigent pas de protection, de marquage ou de traitement particuliers; par exemple, articles publiés sur le site Web de votre entreprise.

Renseignements restreints

Ces renseignements ne sont pas publics, doivent être étiquetés et doivent être protégés. Cette catégorie comprend les fichiers et les données qui ne sont accessibles que par vos employés et vos fournisseurs; par exemple les dossiers des clients.

Renseignements confidentiels

Ces renseignements étant de nature délicate, seuls peuvent y accéder les employés désignés. Les renseignements confidentiels doivent être étiquetés et protégés, et des restrictions doivent être imposées sur la façon dont ils peuvent être traités; par exemple, les renseignements financiers propres à votre entreprise et à vos clients.

Protection des données personnelles des clients (Suite)

2. Développer un processus de traitement

Ensuite, élaborez un processus pour le traitement des renseignements de nature délicate (restreints et confidentiels) relatifs à votre entreprise et à vos clients. Votre protocole doit comprendre des mesures pour conserver adéquatement les renseignements personnels et préciser quels employés dans votre entreprise peuvent y avoir accès.

3. Vérifier les politiques et procédures

Assurez-vous d'avoir des politiques et des procédures en place au cas où des renseignements restreints ou de nature délicate tombent entre de mauvaises mains. Veillez à ce que vos employés sachent quoi faire dans le cas d'un incident de cybersécurité et organisez régulièrement une formation sur les procédures de cybersécurité.

4. Mettre en place des systèmes de désinfection et de destruction

Enfin, mettez en place un système pour détruire les dossiers lorsque vous n'en avez plus besoin. Assurez-vous que ce système réponde aux dispositions de la politique de gestion des renseignements de votre entreprise. Ainsi, vous empêcherez l'accès non autorisé aux renseignements personnels ainsi que leur communication illicite.

Ressources pour protéger les renseignements personnels de vos clients

Centre canadien de cybersécurité

Sécurité pour les petites et moyennes organisations

Protection de l'information de grande valeur : Conseils pour les petites et moyennes organisations (ITSAP.40.001)

Contrôles de cybersécurité de base pour les petites et moyennes organisations

Pensez cybersécurité

Sections 7.3 et 7.4 du Guide Pensez cybersécurité pour les petites et moyennes entreprises

Commissariat à la protection de la vie privée du Canada

Guide sur la protection de la vie privée à l'intention des entreprises

Cybersécurité :
conseils pour vos employés

ASSOCIATION DES BANQUIERS CANADIENS

Il est important de prévoir, dans le plan de cybersécurité, une formation de base continue et formelle pour vos employés. En effet, les employés sont très souvent le premier rempart contre les incidents qui menacent la cybersécurité.

Commencez par des conseils simples, pratiques et faciles à appliquer. La prévention des cybermenaces est un sport d'équipe auquel tout le monde participe. Prenez note de ces simples renseignements...

Votre première ligne de défense

Utilisez une phrase ou un mot de passe exclusif pour accéder au réseau de l'entreprise et modifiez-le régulièrement.

Signes que le courriel que vous venez de recevoir est un hameçon

Demandes inhabituelles de la part d'un fournisseur

Des cybercriminels peuvent envoyer des courriels similaires à ceux de l'un de vos fournisseurs fiables. Généralement de tels courriels vous demanderaient de transférer le paiement d'une facture électroniquement à un compte frauduleux. Vérifiez toujours l'adresse de l'expéditeur : il suffit de placer le curseur par-dessus sans cliquer; la vraie adresse électronique apparaîtra. Si le domaine de l'adresse ne correspond pas à l'organisation, vous saurez immédiatement qu'il s'agit d'une fraude.

Exigences et menaces

La demande de renseignements est-elle valable? La banque n'enverra jamais un courriel menaçant ni n'appellera pour demander des renseignements personnels, comme le mot de passe, le numéro de la carte de débit ou de crédit, ou encore le nom de famille de la mère.

Demandes irrégulières de renseignements

Aussi, les cybercriminels peuvent essayer d'obtenir des renseignements financiers confidentiels, comme les déclarations de revenus, qu'ils utiliseront afin de commettre des fraudes.

Avertissements

Des avertissements au sujet de la fermeture de votre compte ou de la restriction de votre accès au cas où vous ne répondez pas aux demandes faites dans le courriel sont un autre signal d'hameçonnage.

Pièces jointes ou liens douteux

Il faut toujours se méfier des pièces jointes et des liens inattendus ou en provenance d'expéditeurs inconnus. Les courriels frauduleux contiennent souvent des liens intégrés qui semblent légitimes. Or, si vous passez le curseur par-dessus, vous verrez la vraie adresse du lien qui, dans le cas de courriels frauduleux, serait autre que ce qui devrait figurer. Ne jamais cliquer sur une pièce jointe ou un lien douteux.

Demandes bizarres de la part du propriétaire de l'entreprise ou d'un membre de la haute direction

Les cybercriminels peuvent usurper les adresses électroniques des employés. Un signal flagrant d'une possibilité de fraude par courriel d'entreprise compromis est la demande d'un transfert électronique qui semble provenir de l'adresse du propriétaire ou d'un haut gestionnaire et qui incite à agir sans tarder.

Encore des recommandations...

- Soyez méfiants des appels et des visites de la part d'individus demandant des renseignements au sujet de l'entreprise ou des employés. Les criminels recherchent souvent des renseignements personnels sur les employés en vue lancer une cyberattaque.
- Dans le doute... consultez votre superviseur ou demandez l'aide d'un collègue.
- Signalez tout événement suspect à votre superviseur. Très souvent, c'est ainsi qu'on fait échouer une cyberattaque.
- Si vous croyez que de l'information bancaire a été communiquée, signalez immédiatement la fuite afin que l'institution financière puisse être avisée et que les comptes de l'entreprise soient protégés contre tout accès frauduleux.

Ressources additionnelles

Association des banquiers canadiens

Prévention de la fraude :
http://www.cba.ca/fraude?l=fr

Questionnaires de sensibilisation à la cybersécurité :
https://abccybersecurite.ca

Bulletin gratuit sur la prévention de la fraude : Abonnement en ligne.

Gouvernement du Canada

Pensez cybersécurité :
Pensez cybersécurité pour les petites et moyennes entreprises

Centre canadien pour la cybersécurité :
Cybersécurité pour les petites et moyennes organisations

CyberSécuritaire Canada :

Programme national de certification en cybersécurité, destiné aux petites et moyennes entreprises et administré par Innovation, Sciences et Développement économique Canada, qui contribue à l'amélioration des pratiques de cybersécurité en vue de limiter les risques posés par les cybermenaces. La série d'apprentissage gratuite comprend des modules et des guides pratiques. La certification est valide pour deux ans.

Votre banque pourrait avoir des ressources additionnelles. Voyez avec votre institution financière quels sont les services, les guides et les conseils en matière de sécurité offerts aux petites entreprises clientes.

ASSOCIATION DES BANQUIERS CANADIENS

L'Association des banquiers canadiens est la voix de plus de 60 banques canadiennes et étrangères qui contribuent à l'essor et à la prospérité économiques du pays. L'ABC préconise l'adoption de politiques publiques favorisant le maintien d'un système bancaire solide et dynamique, capable d'aider les Canadiens à atteindre leurs objectifs financiers. www.cba.ca

PENSEZCYBERSECURITE.CA

Pensez cybersécurité est une campagne nationale visant à informer les Canadiens sur les enjeux de la cybersécurité et à leur indiquer des façons simples de se protéger en ligne. Cette campagne est menée au nom du gouvernement du Canada par le Centre de la sécurité des télécommunications qui profite de l'expertise de son Centre canadien pour la cybersécurité. Pensezcybersecurite.ca