

Réduisez les risques du travail à distance

Guide élémentaire
de protection des
renseignements
personnels sur votre
ordinateur portable
(Restez sur vos gardes)



Commissaire à l'information et à la
protection de la vie privée / Ontario

BMO  ^{MD} Groupe financier

Aujourd'hui, vous pouvez vous connecter au réseau de votre entreprise de presque partout dans le monde.

Le travail à distance, loin du bureau, implique toutefois que vous travaillez en dehors des couches de sécurité habituelles. Vous devez donc réévaluer les risques pour la protection des renseignements personnels et la sécurité associés au travail à distance, que ce soit à la maison ou en déplacement. Vous devez prendre les mesures nécessaires pour protéger les renseignements confidentiels, qu'il s'agisse de renseignements vous concernant, concernant votre employeur ou, surtout, concernant vos clients.

Dans le présent document, nous examinons certains risques associés à la technologie « portable » (spécialement celle qu'on utilise hors du bureau) et donnons des conseils sur la façon de réduire ces risques. Ces conseils peuvent aider les voyageurs de commerce, les fournisseurs de soins à domicile, les spécialistes qui offrent des consultations sur place, les pigistes ou les employés qui apportent du travail à la maison ou dans leurs déplacements.

1 | Usurpation d'identité

L'usurpation d'identité consiste dans le vol de renseignements permettant d'identifier quelqu'un et l'utilisation de ces renseignements avec l'intention de commettre une fraude ou d'autres crimes au nom de la victime. Cela peut arriver encore plus facilement lorsque vous êtes en transit.

Voici certains des moyens habituels qu'utilisent les usurpateurs d'identité pour obtenir des renseignements :

1. **Vol d'équipement** : ordinateurs portables, assistants électroniques ou cellulaires – dans les voitures, les transports en commun, les chambres d'hôtel, les lieux publics, les aéroports, etc. Si l'équipement contient des renseignements non chiffrés, vos clients peuvent subir une usurpation d'identité et votre employeur pourrait faire l'objet d'une publicité négative, attirer l'attention des médias et risquer des poursuites et d'autres sanctions juridiques.
2. **Fouille de poubelles** : dans les poubelles de votre chambre d'hôtel ou dans tous les endroits où vous jetez des documents qui contiennent des renseignements personnels, comme les relevés de carte de crédit ou les reçus d'achat.
3. **Piquage de mot de passe** : lorsque vous utilisez votre carte de débit ou de crédit, à un guichet automatique ou lorsque vous travaillez sur votre ordinateur portable ou votre assistant électronique dans des lieux publics.
4. **Logiciel espion** : peut être facilement installé lorsque vous connectez votre ordinateur portable ou votre assistant électronique non protégé à un réseau public.
5. **Hameçonnage ou pêche aux données personnelles** : courriels qui, par ruse, peuvent vous amener à divulguer des renseignements vous concernant.

2 | Cultivez un état d'esprit axé sur la protection des renseignements personnels et la sécurité

Des gens essaieront de voler, de détruire ou d'utiliser à mauvais escient des données personnelles ou commerciales importantes en votre possession, qu'elles soient sur papier ou sous forme numérique. Ne devenez pas leur cible! Apprenez comment vous protéger, vous et votre entreprise.

3

Protégez vos clients, votre entreprise et vous même

Pour protéger vos clients, votre entreprise et vous même, nous vous recommandons ce qui suit :

1. Ne prenez aucun renseignement sur des clients dans le réseau de votre entreprise sans l'autorisation de votre superviseur et sans, au moins, la protection d'un bon mot de passe et, de préférence, un chiffrement des données.
2. Utilisez seulement des ordinateurs personnels ou de gestion pour les opérations confidentielles. N'utilisez pas d'ordinateurs ni de réseaux publics et ne faites aucune opération dans des lieux publics.
3. Ne donnez pas de renseignements confidentiels par cellulaire dans des lieux publics.
4. Dans votre voiture, gardez hors de la vue les renseignements confidentiels ou les appareils qui en contiennent. Mettez vos objets de valeur dans le coffre avant de partir et non dans le stationnement à votre arrivée.
5. N'oubliez aucun de vos effets personnels lorsque vous quittez un taxi, une chambre d'hôtel, une salle de réunion, un avion ou un restaurant.
6. À moins que vous n'en ayez vraiment besoin, laissez à la maison les pièces d'identité non nécessaires (carte d'assurance sociale, acte de naissance, carte d'assurance maladie, etc.). En voyage, conservez-les dans les coffres-forts d'hôtel.
7. Mettez tous les reçus dans votre portefeuille, non dans des sacs à provisions, et ne laissez aucun reçu dans les chambres d'hôtel ou les voitures.
8. Gardez la clé magnétique de vos chambres d'hôtel, vos cartes d'embarquement et tout ce qui peut contenir des renseignements vous concernant jusqu'à ce que vous puissiez les déchiqueter ou les détruire de façon sécuritaire.

9. Examinez toujours vos relevés bancaires ou de cartes de crédit aussitôt que vous les recevez pour voir s'il y a eu des opérations inhabituelles.

Principe clé :

1. Réduisez au minimum la quantité de données personnelles ou commerciales que vous transportez avec vous; assurez-vous que vous en avez vraiment besoin.
2. Ne partez pas du bureau avec des données personnelles ou commerciales sans autorisation.
3. Utilisez tous les moyens matériels et techniques pour protéger les données que vous transportez avec vous. Au moins, utilisez un bon mot de passe pour protéger les données. Pour une plus grande protection, vous devriez utiliser le chiffrement.

4 | Ordinateurs portables, assistants électroniques, cellulaires

Pour les voleurs d'information, les ordinateurs portables, les assistants électroniques et, plus récemment, les cellulaires sont des poules aux œufs d'or. Prenez les précautions suivantes pour réduire les risques au minimum :

1. Veillez à ce qu'un mot de passe contrôle l'accès à tous vos appareils : mots de passe pour mise sous tension, mots de passe pour protection d'écran, mots de passe pour les comptes.
2. Les bons mots de passe comprennent au moins huit caractères, des majuscules et des minuscules, des chiffres et des caractères spéciaux. Le mot de passe ne doit pas être un mot qu'on peut trouver dans un dictionnaire.
3. Protégez vos mots de passe et vos clés de chiffrement en ne les mettant pas par écrit.

Remarque : Pour les assistants électroniques, il existe des programmes novateurs (exigeant une signature ou une pression sur un point d'une image) qui vous évitent de retaper votre mot de passe.

4. Mettez en service le dispositif de verrouillage automatique de votre appareil après cinq minutes d'inactivité.
5. Évitez de transporter des données confidentielles sur votre appareil portable, à moins que vous n'en ayez absolument besoin.
6. Chiffrez vos données conformément aux politiques approuvées de votre entreprise. Cela est essentiel si vous transportez des données personnelles ou confidentielles sur vos clients – n'acheminez jamais de données non chiffrées.
7. Si vous n'en avez plus besoin, retirez toutes les données confidentielles de vos appareils à l'aide d'un bon programme de nettoyage numérique. Ne vous fiez pas à la fonction de suppression pour enlever les données confidentielles.
8. Utilisez un porte-documents ou un sac pour portable verrouillable et ne portant aucun logo d'entreprise ou d'association connue.
9. À l'intérieur de votre porte-documents, mettez une carte portant l'indication « Si vous trouvez ce porte-documents, veuillez appeler au numéro [numéro de téléphone]. », et n'ajoutez rien d'autre.
10. Protégez vos appareils portables en tout temps. Utilisez un câble de sûreté muni d'une alarme sonore lorsque vous travaillez avec ces appareils, ou mettez-les sous clé lorsque vous ne les utilisez pas.

Si vous utilisez des appareils portables dotés du dispositif Bluetooth, protégez-vous de la façon suivante :

1. Fermez le Bluetooth lorsque vous n'en avez pas besoin.
2. Réglez vos appareils sur le mode non-découvrable.
3. Utilisez autant de caractères que possible comme numéro d'identification personnel Bluetooth.
4. Effectuez ces réglages en privé.

5

Renseignements confidentiels et financiers

Si vous traitez des renseignements confidentiels en ligne ou effectuez des opérations financières, votre ordinateur portable (et parfois votre assistant électronique) doit au moins avoir un pare-feu personnel, un antivirus et un anti-logiciel espion. Suivez le cycle I-C-M : **I**nstaller tôt, **C**onfigurer adéquatement, **M**ettre à jour fréquemment.

De plus, installez les mises à jour et les retouches de sécurité les plus récentes sur vos appareils portables, y compris votre cellulaire.

Si vous vous connectez à un réseau radiotéléphonique public ou à HotSpots dans les aéroports, les hôtels, les cafés, les bibliothèques publiques, etc., n'oubliez pas que ces réseaux sont peu sûrs par nature. N'oubliez pas l'essentiel :

1. Surveillez ce qui se passe autour de vous.
Quelqu'un pourrait regarder discrètement votre écran d'ordinateur.
2. Ne vous connectez jamais à deux réseaux distincts en même temps (comme Wi Fi et Bluetooth).
3. N'effectuez pas d'opérations confidentielles à moins d'utiliser un lien chiffré (comme un réseau privé virtuel, ou RPV) avec le réseau d'accueil.

À moins qu'elle ne soit chiffrée, toute l'information sur Internet circule bien en vue et est accessible à tous. Cela s'applique à la navigation sur le Web, aux courriels et à la messagerie instantanée.

Principe clé :

Si vous ne savez pas comment utiliser les mesures de protection technique exposées dans le présent document et ne pouvez pas les mettre en œuvre vous même, demandez qu'on le fasse pour vous avant de sortir des renseignements personnels de votre bureau.

6

Si vous êtes victime d'une usurpation d'identité

Le plus important est d'agir rapidement et avec assurance pour réduire au minimum les dommages possibles.

1. Notez toutes vos conversations avec les autorités et les institutions financières, y compris les dates et les heures, les noms et les numéros de téléphone.
2. Signalez immédiatement le crime au service de police (et éventuellement à PhoneBusters) et remplissez un rapport d'événement.
3. Muni de votre rapport d'événement, communiquez avec les agences d'évaluation du crédit énumérées plus loin dans la section « Coordonnées » et demandez qu'un avertissement de fraude soit attaché à votre dossier.
4. Communiquez par téléphone et par écrit avec tous les créanciers chez qui votre nom a été utilisé frauduleusement.
5. Dites aux agents de recouvrement qui vous appellent ultérieurement que vous êtes victime d'une usurpation d'identité et que vous n'êtes pas responsable des factures impayées sur des comptes frauduleux. Obtenez les renseignements pertinents sur ces comptes pour remplir votre rapport aux autorités.
6. Signalez immédiatement la perte ou le vol de votre passeport à la police locale et au bureau des passeports le plus proche (http://www.ppt.gc.ca/can/lost_stolen.aspx?lang=f). Si vous êtes à l'extérieur du Canada, signalez la perte ou le vol à l'ambassade ou au consulat canadien le plus proche.

Principe clé :

Si vous perdez des données confidentielles, en particulier des renseignements personnels sur des clients, informez-en immédiatement votre superviseur et le responsable de la protection des renseignements personnels de votre entreprise.

AIDE-MÉMOIRE

Avant de quitter le bureau en emportant des renseignements personnels et confidentiels sur quelqu'un, revoyez la liste suivante :

1. Avez-vous la permission de votre superviseur ou la politique de l'entreprise vous y autorise-t-elle?
2. Emportez vous le moins de renseignements personnels possible et, de préférence, aucun numéro d'assurance sociale?
3. Si vous emportez des renseignements électroniques
 - a. Sont-ils protégés par un mot de passe?
 - b. Sont-ils chiffrés?
4. Votre porte-documents ou votre sac pour ordinateur portable est-il verrouillé et non identifié?
5. Savez-vous quoi faire en cas de vol ou de perte de données?

À NE PAS OUBLIER :

Verrouillage; mot de passe; protection.

Coordonnées

Agences d'évaluation du crédit

Equifax :	1 800 465-7166 www.equifax.ca
TransUnion :	1 866 525-0262
Résidents du Québec :	1 877 713-3393 www.tmac.ca (en anglais)
PhoneBusters :	1 888 495-8501 www.phonebusters.com

GRC – Usurpation d'identité :

RCMP

www.rcmp.ca/scams/identity_theft_f.htm

Gouvernement de l'Ontario – Usurpation d'identité :

www.cbs.gov.on.ca/MGS/fr/ConsProt/050438.htm

BMO Groupe financier

bmo.com



Commissaire à l'information et à la
protection de la vie privée/Ontario

www.ipc.on.ca

Ann Cavoukian, Ph.D.

Commissaire

Août 2006