CONFORMITÉ

LIGNE DIRECTRICE I APPAREILS MOBILES

Ce document s'adresse à :
Tous courtiers individuels ou incorporés autorisés avec le Centre Financier Optimal Inc.

JANVIER 2017

425 NOTRE-DAME ST, DIEPPE NB E1A 9G4 | COMPLIANCE@OPTIMALCENTRE.CA | OPTIMALCENTRE.CA

APERÇU - OBJECTIF

Le Bureau de la sécurité informatique a établi la présente ligne directrice afin de vous aider à comprendre comment sécuriser les appareils mobiles *gérés personnellement* qui sont utilisés à des fins professionnelles

La compagnie représente le Centre Financier Optimal Inc et ses filiales ainsi que les compagnies d'assurance et d'investissement dont nous avons des ententes contractuelles.

Le but ainsi visé est d'assurer que l'utilisation de tels appareils mobiles n'entraîne pas la perte, le vol ou la compromission de renseignements et qu'elle n'ait pas d'effet défavorable sur l'infrastructure de la Compagnie.

La présente décrit les dispositifs de sécurité les plus courants dont sont dotés les appareils mobiles. Elle ne traite pas de tous les dispositifs possibles, de la même façon que ce ne sont pas tous les appareils mobiles qui incluent l'ensemble des dispositifs décrits.

PORTÉE

La présente ligne directrice vise les appareils mobiles *gérés personnellement* (c'est-à-dire, les appareils mobiles généralement achetés par les courtiers), pour accomplir des tâches d'affaire.

Elle aborde précisément l'utilisation d'appareils mobiles *gérés personnellement*, y compris les téléphones cellulaires, les téléphones intelligents et les tablettes. Elle ne vise pas les portatifs, même si ceux-ci pourraient être dotés de certains de ces dispositifs; si tel est le cas, la ligne directrice devrait alors s'appliquer.

PERSONNES VISÉES

La présente ligne directrice s'applique aux personnes suivantes :

- Tous les courtiers (sans distinction de situation professionnelle)
- Les consultants, conseillers, courtiers, et autres entrepreneurs indépendants et de leurs employés
- Les tierces parties qui ont signé un contrat de service avec le courtier
- Toutes les personnes autorisées à accéder aux ressources d'information du courtier

Par « **vous** », on entend, dans la présente ligne directrice, toute personne parmi les personnes susmentionnées qui utilise un appareil mobile géré personnellement à des fins professionnelles.

INTRODUCTION

Les renseignements de la Compagnie sont précieux non seulement pour celle-ci, mais également pour d'autres personnes non autorisées. Le vol de renseignements peut permettre à quelqu'un d'ouvrir des comptes bancaires, d'obtenir des cartes de crédit ou des passeports, d'échanger ou de vendre des renseignements sur un produit ou sur la gouvernance ou encore de commettre d'autres activités criminelles.

Quels renseignements pourraient être stockés dans un appareil mobile?

- Données sur les personnes qui figurent dans votre répertoire.
- Historique des appels (sortants et entrants).
- Messages textes ou sessions de clavardage.
- Historique de localisation en fonction de l'historique GPS ou de la tour de la station de base.
- Historique des sites Web visités et pages Web dans la mémoire cache.
- Photos, vidéos, enregistrements audios et courriels.
- Mots de passe, documents, dossiers de la Compagnie et autres fichiers sensibles stockés dans l'appareil.

La présente ligne directrice a été conçue pour vous aider à utiliser les appareils mobiles de manière sécurisée. Cela dit, elle ne donne pas de renseignements approfondis sur la façon d'activer divers dispositifs.

RECOMMANDATIONS EN MATIÈRE DE CONFIGURATION SÉCURISÉE

Les dispositifs de sécurité qui suivent sont offerts par la plupart des appareils mobiles et devraient être activés pour garantir une protection appropriée.

Gestion des mots de passe

- **Robustesse du mot de passe.** La plupart des appareils mobiles permettront l'utilisation d'un numéro d'identification personnel (NIP) simple de quatre chiffres ou de mots de passe plus longs. Idéalement, il faudrait se servir d'un mot de passe robuste (qui inclut des lettres majuscules et minuscules, des chiffres et des symboles) plutôt que d'un NIP plus faible de quatre chiffres. Le mot de passe devrait expirer ou être modifié de façon régulière. Dans le même ordre d'idées, certains appareils mobiles permettent de tracer un motif pour les déverrouiller. Encore une fois, plus le motif est long et complexe, mieux ce sera.

- **Verrouillage automatique.** L'appareil mobile devrait être configuré de manière à se verrouiller automatiquement après quelques minutes d'inactivité. Pour le déverrouiller, votre mot de passe devrait être exigé.

- **Mot de passe effacé.** L'appareil mobile devrait être configuré de manière que, si le mot de passe est entré incorrectement trop de fois, il supprime toutes les données de l'utilisateur pour protéger ce dernier contre les recherches par force brutes.

- **Mot de passe utilisé pour le partage de connexion / les points d'accès sans fil.** Si votre appareil mobile vous permet d'y brancher d'autres appareils mobiles Wi-Fi afin de partager le service Internet (ce qu'on nomme « partage de connexion » ou « points d'accès sans fil »), assurez-vous que la connexion est assortie d'un mot de passe robuste (qui inclut des lettres majuscules et minuscules, des chiffres et des symboles). D'autres personnes pourraient se servir de votre connexion ou voler vos données s'il est facile de déterminer le mot de passe. Gardez aussi à l'esprit les attentes ou les restrictions relatives à l'utilisation des données.

Cryptage

- **Cryptage matériel**. La plupart des appareils mobiles acceptent le cryptage matériel intégré. Toutes les données de l'utilisateur sont automatiquement protégées. Le cryptage protège les données dans l'éventualité où une personne tenterait d'accéder directement aux zones de mémoire.

- **Cryptage d'une carte de support amovible.** Si votre appareil mobile peut accueillir des cartes de support amovible, vous devriez alors activer le cryptage de celles-ci également pour protéger les données sensibles que vous y avez stockées, le cas échéant.

- **Cryptage des sauvegardes.** Pour garantir la protection des fichiers de sauvegarde que vous créez, activez le cryptage de ceux-ci. Encore une fois, vous devez établir un mot de passe robuste pour ce qui est de vos fichiers de sauvegarde. Protection contre les malicieux.

- **Services de sécurité mobile**. Autant pour votre appareil mobile que pour votre PC ou votre portatif, la sécurité globale est une nécessité d'importance. Installez une solution antivirus et un coupe-feu sur votre appareil mobile personnel si celui-ci peut les accueillir.

RECOMMANDATIONS EN MATIÈRE D'UTILISATION SÉCURISÉE

En plus de suivre les recommandations précédentes en matière de configuration, vous devriez adopter les comportements sécuritaires de l'utilisateur, dans le respect des *Normes concernant l'usage acceptable des outils technologiques*.

Installation d'applications (de logiciels)

- **Rendez-vous uniquement dans les boutiques d'applications officielles.** Faites vos achats dans les boutiques d'applications réputées (p. ex., iTunes, Google Play, BlackBerry App World). Le

fabricant de votre appareil mobile effectue un contrôle de la qualité minimal quant aux applications offertes dans les boutiques officielles. Même si ce n'est pas l'idéal, cela réduit le risque que des applications malveillantes soient installées sur votre appareil mobile.

- **Scrutez les applications avant de les installer.** Lisez les commentaires et les évaluations d'autres utilisateurs pour savoir si une application est sécuritaire. Informez-vous sur la quantité de données auxquelles accède l'application, en plus de vérifier si elle transmettra votre information à des tiers et si une politique de confidentialité est en vigueur. Contrôlez les permissions exigées par l'application. Est-il réellement nécessaire que l'application fasse le suivi de tout ce que vous faites? Si l'application éveille des soupçons chez vous ou si elle vous inquiète, ne la téléchargez pas.

- **Effectuez les mises à jour des applications et du système d'exploitation.** Périodiquement, des mises à jour seront offertes pour les applications et le système d'exploitation installés sur votre appareil mobile. Destinées à apporter les correctifs nécessaires pour faire échec à des vulnérabilités et à des bogues, ces mises à jour devraient être effectuées en temps opportun. À défaut de le faire, votre appareil mobile pourrait être exposé aux malicieux et aux pirates informatiques. Permettez toujours l'installation des mises à jour.

- **Ne bidouillez pas votre appareil mobile.** Ne faites pas le « débridage » ou le « *root* » (terme anglais) de votre appareil mobile. Ces termes se rapportent à l'acte, pour un utilisateur, de bidouiller son appareil mobile afin que celui-ci puisse surmonter les murs qu'il n'est pas censé franchir. Ces murs offrent une protection dont vous ne pourrez pas autrement profiter. Si vous débridez votre appareil mobile, vous l'exposez alors aux malicieux et aux pirates informatiques.

Gestion des données

- **Stockez uniquement ce qu'il vous faut.** Prenez conscience de ce que vous stockez dans votre appareil mobile. En avez-vous réellement besoin? Moins vous stockez, mieux ce sera. De plus, notez les données que renferme votre appareil mobile à mesure qu'elles y sont stockées : s'il est perdu ou volé, vous aurez ainsi un relevé de son contenu.

- **Effectuez des sauvegardes régulières.** La plupart des appareils mobiles permettent de sauvegarder vos données et vos applications. Comme c'est le cas pour votre ordinateur, il est sage de faire de même avec votre appareil mobile sur une base régulière dans l'éventualité où, pour une raison ou pour une autre, vous perdriez l'accès à vos données.

- **Adoptez des pratiques sécuritaires en matière de surf sur Internet ou de courriels.** Le pourriel et l'hameçonnage sont une réalité autant pour les appareils mobiles que pour les PC ou les portatifs. Ne cliquez pas sur les liens ou les pièces jointes qui figurent dans des courriels ou des messages textes non sollicités. Évitez de divulguer, au moyen de votre appareil mobile, tout renseignement confidentiel dans des textos ou des courriels ou encore lorsque vous utilisez des navigateurs Web. N'oubliez pas de suivre les pratiques exemplaires relatives à Internet. Supprimez tout message non sollicité ou suspect dès que vous le recevez. Réfléchissez avant de cliquer!

Réseautage

- **Faites preuve de prudence dans les points d'accès sans fil publics.** Des yeux indiscrets pourraient être à l'œuvre dans les points d'accès sans fil publics. Évitez d'effectuer des transactions bancaires, de faire des achats en ligne ou d'accéder aux ressources de la Compagnie à partir de telles connexions. Il vaut mieux attendre d'avoir accès à un réseau auquel vous faites confiance avant d'effectuer des transactions sensibles. Par ailleurs, soyez sur vos gardes si vous utilisez votre appareil mobile à l'extérieur de votre pays d'origine. Les interceptions non autorisées et l'analyse de trafic pourraient être plus répandues dans un réseau étranger.

- **Voyez au cryptage des connexions sans fil.** Si vous utilisez une connexion Wi-Fi ou Bluetooth, assurez-vous qu'il s'agit d'une connexion sécurisée. Par exemple, la connexion devrait être

- **Désactivez les capacités sans fil (lorsqu'elles ne sont pas utilisées).** Éteignez les connexions Wi-Fi et Bluetooth lorsqu'elles ne sont pas utilisées. Les connexions sans fil ouvertes et sans surveillance représentent une cible facile pour les criminels. Quand elles sont activées, configurez-les de manière à ce qu'elles demandent l'ouverture d'une connexion plutôt que de se brancher automatiquement à toute connexion disponible.

Protection physique

Apposez une étiquette sur votre appareil mobile. Apposez une étiquette ou une pièce d'identification sur votre appareil mobile au cas où il serait perdu ou volé. Il pourra ainsi vous être retourné si une personne ou la police devaient le retrouver. De plus, sur un document que vous conserverez

- **Ne laissez jamais votre appareil mobile sans surveillance.** Un moment d'inattention suffit pour se faire voler un appareil mobile.

- **Débarrassez-vous de votre appareil de manière sécurisée.** Votre appareil mobile stocke beaucoup plus de renseignements sensibles que vous pourriez le penser. Vous devez faire le nécessaire pour assurer qu'ils sont supprimés de l'appareil mobile avant que vous vous en débarrassiez. Faites une sauvegarde de toute information que vous voulez conserver, puis effacez le contenu de l'appareil mobile en réinitialisant celui-ci. Le simple fait de supprimer des renseignements n'est pas une mesure sécurisée. De plus, n'oubliez pas la carte SIM et toute carte de support amovible : enlevez-les ou effacez le contenu de celles-ci également.

Utilisation générale

- **Fermez votre session.** Comme vous le faites avec votre PC ou votre portatif, fermez toute session ouverte dans un site Web ou un programme quand vous n'avez plus à vous en servir. De plus,

rappelez-vous de ne pas « enregistrer » vos renseignements de manière à ce que la session s'ouvre automatiquement la fois suivante : si votre appareil mobile est perdu ou volé, une autre personne pourrait accéder à vos comptes ou dossiers.

- **Faites preuve de prudence avec les codes QR.** Les codes QR (*Quick Response*, en anglais) sont les curieuses petites images carrées qui ressemblent à des écrans de télévision flous, insérées dans des annonces et des affiches. Ces codes sont destinés à être numérisés par l'appareil photo d'un appareil mobile afin de diriger d'office le navigateur Web vers un site pour obtenir plus de renseignements. Toutefois, vous ne pouvez pas savoir à l'avance où mènera un code QR. Quelqu'un pourrait avoir créé un code QR pour vous emmener à un site Web malveillant. En cas de doute, ne numérisez pas!

- **Prenez des précautions lors de réparations.** S'il est nécessaire de faire vérifier l'appareil mobile, vous devez garantir la protection des données qu'il contient. Avant de faire réparer l'appareil mobile, vous devriez supprimer toute donnée pertinente et retirer toute unité amovible de l'appareil. Si cela n'est pas possible, assurez-vous alors d'activer tous les mécanismes de protection par mot de passe. Ne divulguez jamais vos mots de passe à qui que ce soit. Si l'on vous remet un appareil de remplacement, assurez-vous que toutes les données ont été effacées de l'appareil mobile original. Par ailleurs, quand vous retournez tout appareil mobile que l'on vous a prêté, supprimez les données qu'il pourrait contenir.

- **Signalez immédiatement tout appareil mobile perdu ou volé.** Si vous croyez que vous avez perdu votre appareil mobile ou qu'il a été volé, communiquez avec votre fournisseur de services pour le signaler. Entrez en contact également avec le Bureau des services technologiques et le chef de la vérification de la conformité pour obtenir de plus amples directives.

CONCLUSION

Les appareils mobiles sont pratiques et faciles à transporter. Ils peuvent toutefois stocker de considérables quantités de données de la Compagnie qui, si elles, ne sont pas protégées adéquatement, pourraient être perdues ou exposées. Il est important que vous sachiez quelles protections sont à votre disposition, lesquelles constituent des paramètres de l'appareil mobile et lesquelles représentent des comportements exemplaires visant à maintenir le caractère sécurisé de l'appareil mobile.