CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

Sécurité des appareils lors des déplacements et du télétravail à l'étranger

April 2023 | ITSAP.00.188

Voyager avec des appareils mobiles peut poser des risques envers les personnes et les organisations. Ces risques peuvent être plus graves dans le cadre du télétravail à l'étranger. La présente publication vise à offrir des conseils et de l'orientation aux employés qui sont en voyage ou qui travaillent depuis l'étranger avec des appareils organisationnels. Bien qu'une liste des risques spécifiques à chaque pays ne soit pas disponible, ce document regroupe les informations sur les risques et les mesures d'atténuation dont vous devez tenir compte avant, pendant et après avoir voyagé ou travaillé à l'étranger avec vos appareils.

Lorsque vous voyagez à l'extérieur du Canada, vous devriez bien évaluer les risques potentiels liés à l'utilisation de vos dispositifs mobiles. Chaque scénario de voyage nécessitera une évaluation pour déterminer les risques connexes. Si un appareil est émis pour voyager ou pour des accords de télétravail à l'étranger, assurez-vous que vos employés sont informés des politiques régissant l'utilisation d'appareils appartenant à l'organisation à l'extérieur du Canada. Votre organisation devrait tenir compte de ce qui suit dans le cadre des évaluations des risques liés aux déplacements ou aux ententes de télétravail à l'étranger.

Voyageuses et voyageurs connus du public

Les dispositifs mobiles des cadres supérieurs ou des personnes qui travaillent avec de l'information importante risquent plus d'être ciblés par les auteurs de menace. Les appareils de personnes connues contiennent des informations sensibles et en cas de compromission, ces informations pourraient servir à des fins malveillantes, par exemple pour de l'extorsion.

Envisagez d'attribuer des « appareils de voyage » pour remplacer les appareils organisationnels ou personnels des voyageuses et voyageurs connus du public ou des employés qui participent à des événements très médiatisés. Si toutefois, les appareils de l'organisation sont évalués comme présentant un risque acceptable, les contrôles de sécurité appropriés doivent être appliqués et la voyageuse ou le voyageur doit suivre une formation de sensibilisation.

Consultez ce document pour en savoir plus : Conseils sur les appareils mobiles à l'intention des voyageurs connus du public (ITSAP.00.088).

Événements très médiatisés

Un appareil mobile est nécessaire pour faire des affaires lorsque vous vous rendez à des événements très médiatisés, comme des conférences ou des sommets mondiaux, des événements d'État (p. ex. des funérailles d'État, une fonction de célébration de représentants de l'État) ou un événement mondial, comme les Jeux olympiques. En raison de l'attention accrue portée à l'événement auquel vous assistez, il est recommandé de mettre en place des mesures de sécurité supplémentaires pour vous protéger et protéger vos appareils.

Les employés qui se rendent à des événements très médiatisés devraient recevoir des appareils de voyage connectés à une enclave séparée et soumis à une surveillance renforcée.

Consultez le document suivant pour en savoir plus : Dispositifs mobiles et voyages d'affaires (ITSAP.00.087).

Séjours de courte durée

Lorsque vous voyagez avec un appareil pendant une courte période, la sécurité de votre appareil doit être primordiale. Si votre organisation vous a fourni un appareil de voyage, assurez-vous de connaître les limites de l'appareil et de votre utilisation à l'étranger. Si on vous autorise à utiliser un appareil fourni par votre organisme, assurez-vous de respecter les éléments de la liste de vérification qui se trouve à la fin du présent document.

Télétravail à l'étranger

Le télétravail à long terme à l'extérieur du Canada peut représenter un danger pour votre organisation. Considérez ce qui suit avant d'approuver une entente de télétravail à l'étranger :

Si vous avez des télétravailleurs qui ont besoin d'accéder à des informations sensibles, votre organisation doit s'assurer que vos politiques indiquent que de « zones de sécurité » sont nécessaires dans les installations contrôlées par votre organisation à l'étranger. Les employés doivent avoir accès aux informations sensibles uniquement dans ces zones approuvées. Si cela n'est pas possible, vous devez utiliser des lieux raisonnablement privés tels qu'une chambre d'hôtel ou votre domicile à l'étranger, au lieu d'espaces publics ou de halls d'hôtel pour des affaires moins sensibles.

Dans les endroits non sécurisés, le travail doit être limité à un niveau de sensibilité faible et doit être effectué sur un appareil approuvé par l'organisation. Considérez les mesures suivantes pour améliorer la sécurité de vos ententes de télétravail à l'étranger :

- Assurez-vous que les employés se connectent à l'environnement TI de votre organisation avec un appareil approuvé par qui applique le chiffrement des disques et l'authentification multifacteur (AMF).
- Connectez tous les appareils approuvés à un RPV sécurisé.
- Utilisez un accès sécurisé à la messagerie Web qui offre des mesures supplémentaires par rapport au RPV (isole et protège votre infrastructure).
- Évitez de vous connecter au réseau Wi-Fi et utilisez l'appareil mobile fourni par votre organisation comme point d'accès pour accéder à Internet. Les réseaux Wi-Fi locaux ne sont parfois pas sécurisés ou ont des lacunes par rapport à leurs contrôles de sécurité, ce qui rend vulnérables aux cybermenaces votre appareil et les systèmes et réseaux connectés.
- Protégez votre point d'accès avec une phrase de passe ou un mot de passe complexe et activez le plus haut niveau de chiffrement pris en charge par votre fournisseur.
- Définissez des procédures claires pour régir ce que les employées et employés ont l'autorisation de faire avec les ressources informatiques de l'organisation.

Centre de la sécurité des télécommunications
Communications Security Establishment

Canada

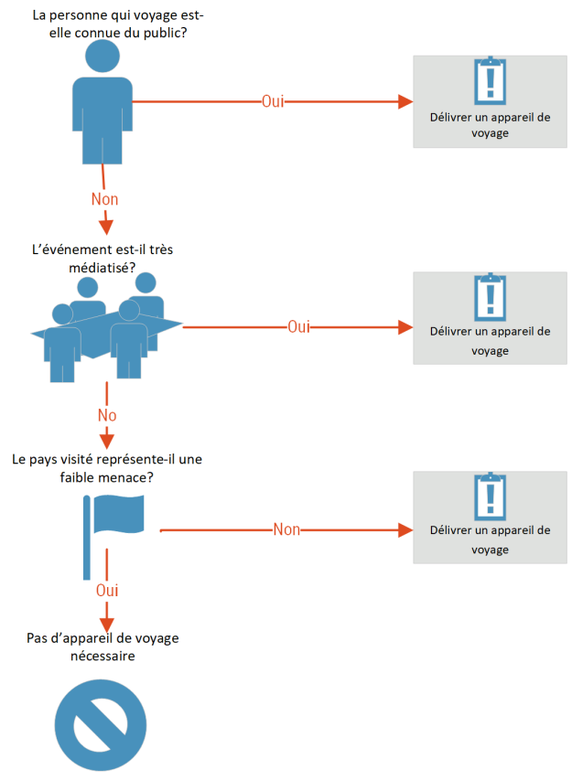
CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

Considérations sur la probabilité des risques liés aux dispositifs de voyage

Votre organisation devrait prendre en considération les risques associés aux voyages internationaux et déterminer son niveau de tolérance à l'égard de tels risques. Veillez à ce que les mesures appropriées soient mises en œuvre pour atténuer les risques.

A-t-on besoin d'appareils de voyage?

La décision de délivrer ou non un dispositif de voyage pour un scénario de voyage ou un accord de télétravail spécifique dépend de nombreux facteurs de risques et de considérations de sécurité, principalement basés sur la voyageuse ou le voyageur, l'événement et la destination. Tenez compte de l'illustration ci-dessous pour vous aider à déterminer si votre employée ou employé peut voyager avec son appareil organisationnel ou si un appareil spécifique à son scénario de voyage doit être fourni.



Voyage à haut risque

Il faut tenir compte non seulement de l'identité de la voyageuse ou du voyageur, mais aussi de la destination du voyage. Les infrastructures de télécommunications d'autres nations ne sont pas nécessairement aussi sécuritaires que celles du Canada. Lors de l'évaluation du niveau de risque et des menaces, votre organisation doit tenir compte des niveaux de risque de voyage utilisés par Affaires mondiales Canada (AMC) et délivrer des appareils en fonctions des risques. Voici les catégories dans lesquelles AMC classe différents pays :

- Prenez des mesures de sécurité normales
- Faites preuve d'une grande prudence
- Évitez tout voyage non essentiel

Évitez tout voyage

Certains pays sont classés comme présentant un risque élevé, pourtant il peut y avoir des régions de ces mêmes pays qui sont considérées comme présentant un risque plus faible. Lors de l'examen des niveaux de risque d'AMC pour l'évaluation de votre scénario de voyage, assurez-vous d'examiner l'ensemble du profil du pays pour cerner les risques pertinents par région. Les niveaux de risque variables selon les régions pourraient avoir une incidence sur le risque global évalué pour le scénario de voyage.

De plus, votre organisation doit tenir compte des points suivants lorsqu'une personne doit voyager vers une destination au niveau de risque élevé selon AMC :

- Dites à vos employées et employés d'éviter d'utiliser leurs appareils personnels ou professionnels réguliers. Si vous devez apporter un dispositif personnel, désactivez les fonctions de Bluetooth, de Wi-Fi et de partage de la localisation.
- Imposez l'utilisation d'un réseau privé virtuel (RPV) pour vous connecter à n'importe quel réseau ou système d'entreprise.
- Assurez-vous que votre service de TI dispose d'un inventaire d'appareils de voyage et, si nécessaire, de comptes de voyage restreints pour limiter l'accès au système et aux données pendant que vos employées et employés se déplacent dans un environnement à haut risque ou à forte menace.
- Chiffrez les informations sur les appareils que votre employée ou employé emportera lors de ses déplacements avant son départ, car les communications transmises par les réseaux de fournisseurs publics risquent d'être interceptées.
- N'oubliez pas qu'à l'hôtel, les connexions Internet, les photocopieurs et les télécopieurs font l'objet d'une surveillance. Ils ne devraient donc être utilisés que pour envoyer de l'information non sensible.
- Dites à vos employées et employés de signaler à votre service de sécurité des TI tout problème de rendement du dispositif ou toute préoccupation de sécurité.

Lors de l'évaluation de vos scénarios de voyage, consultez toujours la page des conseils aux voyageurs d'Affaires mondiales Canada (AMC) pour obtenir les informations les plus récentes sur les niveaux de risque spécifiques à chaque pays, les tendances en matière de crime et les précautions de sécurité recommandées.

Centre de la sécurité des télécommunications
Communications Security Establishment

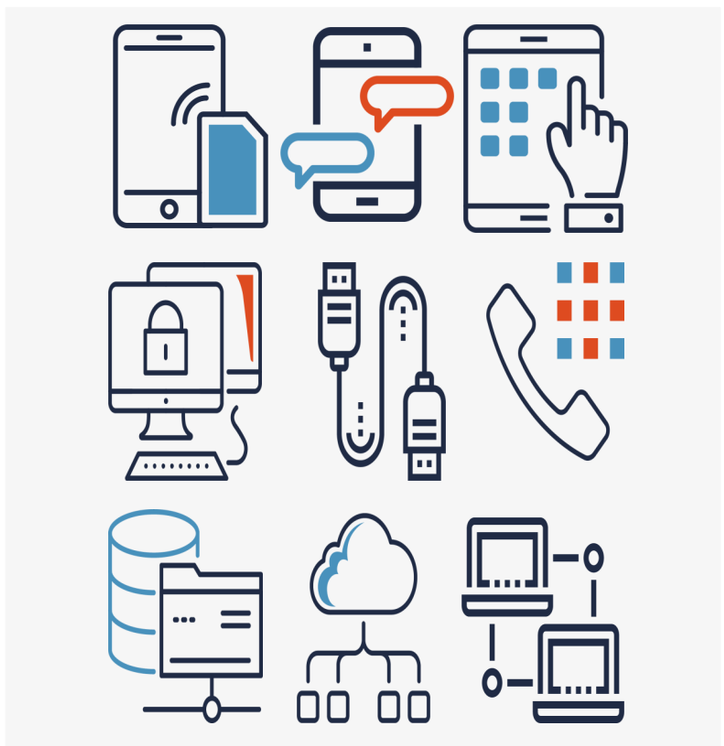
Canada

Est-ce que les autrices et auteurs de menace ciblent les voyageuses et voyageurs?

Les autrices et auteurs de menace s'intéressent aux données que contiennent vos appareils et à l'accès qu'ils pourraient avoir aux réseaux et systèmes de votre organisation. Ils peuvent recourir à des dispositifs commerciaux d'espionnage électronique (p. ex. des intercepteurs d'identité internationale d'abonnement mobile [IMSI]) aux fins suivantes :

- repérer et cibler des dispositifs mobiles
- accéder au dispositif et suivre vos déplacements
- utiliser les connexions réseau d'un dispositif, p. ex. Wi-Fi et Bluetooth
- installer du code malveillant sur un dispositif
- activer le microphone ou la caméra du dispositif
- intercepter vos communications

Liste de vérification pour assurer la protection de vos appareils lorsque vous voyagez ou travaillez à l'étranger



- ☐ Mettez régulièrement à jour les logiciels, micrologiciels et systèmes d'exploitation des appareils appartenant à votre organisation.
- ☐ Assurez-vous que les appareils et autres supports sont chiffrés avec le niveau le plus élevé autorisé pour l'appareil.
- ☐ Activez l'authentification multifacteur (AMF) sur vos dispositifs et vos comptes.
- ☐ Installez des logiciels antivirus, antimaliciel et antihameçonnage sur les appareils.
- ☐ Utilisez des plugiciels bloqueurs de publicités et de maliciels dans votre navigateur.
- ☐ Mettez en œuvre le contrôle d'accès pour tous les appareils avec protection par mot de passe ou phrase de passe.
- ☐ Adoptez des pratiques de sécurité des appareils, p. ex. le filtrage de système de noms de domaine (DNS).
- ☐ Sauvegardez les données de vos appareils avant votre départ.
- ☐ Réduisez au minimum la quantité d'informations stockées sur les appareils de l'organisation pour ne conserver que les fichiers requis pour le scénario de voyage.
- ☐ Supprimez les justificatifs d'identité et les mots de passe stockés pour les comptes et les services auxquels vous n'aurez pas besoin d'accéder lors de votre voyage ou travail à l'étranger.
- ☐ Modifiez les mots de passe de tous vos comptes, surtout les comptes partagés ou ayant des droits d'accès communs.
- ☐ Désactivez les fonctions comme le GPS, le Bluetooth et le Wi-Fi quand vous n'en avez pas besoin.
- ☐ Désactivez les capacités de connexion automatiques afin que vos dispositifs ne se connectent pas automatiquement à des appareils inconnus ou à des réseaux non sécurisés ou qu'il n'y ait pas de jumelage avec ces appareils et réseaux.
- ☐ Évitez de télécharger des applications non essentielles et limitez l'utilisation d'applications avec vos appareils.
- ☐ Surveillez vos dispositifs pour détecter tout comportement inhabituel, fenêtres intruses, ou réduction de l'efficacité de la pile.
- ☐ Ne perdez pas de vue vos appareils, y compris les câbles, les chargeurs et les périphériques, car ils peuvent contenir des microcontrôleurs intégrés pouvant diffuser des logiciels malveillants.

Centre de la sécurité des télécommunications
Communications Security Establishment

Canada

 No de cat.D97-1/00-188-2023F-PDF ISBN 978-0-660-48517-1