



## Document de position du SNDPI

### Voyages internationaux

Rédigé pour le compte du SNDPI avec des suggestions de ses membres par

Mohammad Qureshi/ONTARIO

Le 15 janvier 2018

---

#### INTRODUCTION

Alors que le cyber paysage continue à se développer et que les capacités de cyber intrusion s'accroissent, ce document donne la position du SNDPI sur les meilleures pratiques en matière de voyages internationaux. Les risques reliés aux voyages internationaux doivent être évalués par les administrations en se basant sur ce qui suit :

- Destination ;
- Objectifs du voyage incluant le rôle du voyageur, ses responsabilités et les renseignements détenus ;
- Engagements anticipés, événements et activités au cours du voyage.

#### POSITION DU SNDPI

Les employés du gouvernement qui doivent partir pour un voyage international doivent faire face à plusieurs risques physiques et relatifs à l'information. Toute compromission à un appareil mobile peut avoir un impact négatif sur l'organisation, ses informations et sa réputation. Toute compromission a le potentiel de s'étendre à d'autres parties du réseau, ce qui pourrait affecter la performance du réseau, provoquer un état d'incapacité, des pertes de production et de propriété intellectuelle et d'importants coûts et efforts de récupération. Il est bénéfique pour une organisation de faire une évaluation basée sur les risques pour les voyages internationaux afin que la posture de sécurité ne soit pas affectée.

Les éléments clés à considérer incluent les éléments suivants :

- Les voyageurs font face à une variété de menaces, y compris celles qu'on associe aux technologies sans fil.
- Les individus qui occupent des postes supérieurs au gouvernement et ceux qui ont des informations de valeur peuvent être à plus haut risque.
- Des moyens existent qui permettent à des acteurs menaçants de :
  - Identifier et cibler des appareils mobiles ;
  - Transmettre un code malicieux à l'appareil ;
  - Utiliser les connexions au réseau de l'appareil pour ses propres desseins (c.-à-d. sans fil, système Bluetooth) ;
  - Utiliser l'appareil comme un moyen d'infecter les réseaux du gouvernement ;
  - Utiliser l'appareil pour suivre votre position (c.-à-d. GPS) ;
  - Activer à distance le microphone de l'appareil ;
  - Intercepter les communications électroniques.



Pour soutenir le voyageur, il est important que les pratiques de sécurité soient en ligne avec la perception du niveau de risque. Les niveaux de risques qui suivent fournissent un guide pour les appareils après l'évaluation des risques faite pour un individu après considération de la destination, de l'importance de son poste et de l'information en sa possession :

	Voyage à cyber risque élevé Exigence minimum	Voyage à cyber risque bas Exigence minimum
Formation et sensibilisation	Avoir des séances d'information avec les voyageurs pour les sensibiliser aux risques. Les personnes qui tiennent ces rencontres peuvent différer selon les disponibilités des services internes et la capacité d'utiliser des services à l'externe.  Partagez les pratiques d'excellence sur la façon de travailler à distance et de se connecter lorsqu'à l'étranger.	
Guide de l'appareil	Fournir un appareil temporaire ou qui provient d'un inventaire consacré au voyage (pour certaines administrations, il s'agit d'un simple téléphone plutôt qu'un téléphone intelligent).	Utiliser l'appareil régulier.
Exigences de sécurité	Nettoyer et reformater les appareils de l'inventaire consacré au voyage selon les procédures des TI.  Lorsque c'est possible : <ul style="list-style-type: none"> <li>Augmenter les capacités d'enregistrement et de surveillance de l'appareil de voyage et du compte du voyageur ;</li> <li>Utiliser un réseau distinct pour les appareils de voyage, lorsque possible.</li> </ul>	Limiter les privilèges administratifs.  Implanter les pratiques d'excellence de voyage.

## RECOMMANDATION

Les membres du SNDPI s'entendent pour dire qu'il est critique de fournir des outils afin d'assurer la sécurité pour les voyages internationaux en instaurant une évaluation des risques dans chaque administration. Les membres croient également que les étapes qui suivent doivent être prises avant, pendant et après chaque période de voyage pour améliorer la sécurité de l'information cumulée sur chaque appareil et mieux protéger le réseau :



- Évaluer le risque : considérer la nature du voyage et le rôle du voyageur, ses responsabilités et l'information détenue. Les organisations devraient collaborer avec les services de police ou des renseignements, là où c'est possible, pour évaluer la menace.
- Évaluer les besoins en informations : avoir des séances d'information avec le voyageur pour déterminer s'il a besoin de transmettre des informations sensibles ou classifiées. Informer le voyageur sur les coutumes habituelles et les restrictions de l'immigration s'il veut communiquer par le biais de services cryptés ou RPV.
- Éduquer le voyageur : l'éducation est une étape essentielle pour assurer que le voyageur soit conscient des menaces et gère les risques en conséquence. Le voyageur doit connaître les procédés d'hameçonnage et les tactiques de piratage psychologiques qui peuvent être déployées pour prendre le contrôle de ses appareils et de la vulnérabilité associée à la connexion au réseau sans fil et sans frais de l'hôtel ou d'ailleurs.
- Réduire les possibilités d'attaques : lorsque possible, le voyageur devrait être encouragé à laisser derrière lui ce qui ne lui est pas nécessaire. Cela s'applique aux appareils, mais aussi aux informations sensibles.
- Rapportez-les : dans les cas où le voyageur identifie quelque chose de suspect, il devrait avoir à le rapporter le plus rapidement possible. Cela inclut les moments où il est tenu de se connecter et lorsqu'il perd de vue son appareil en arrivant dans un pays.