



Guide sur la sécurité en voyage à l'intention du personnel et des chercheurs universitaires

Décembre 2019

Ce document a été conçu pour être adapté par les établissements et compléter leurs politiques et outils existants.

Table des matières

Contexte.....	3
1. Cinq raisons qui font des chercheurs canadiens une cible de choix.....	4
2. Votre profil.....	5
3. Sources d'accès à vos recherches.....	6
3-A. Relations interpersonnelles.....	6
3-B. Intrusion physique.....	7
3-C. Cyberintrusion.....	8
Annexe A – Liste de conseils sur la sécurité en voyage pour les chercheurs universitaires.....	9
Avant de partir.....	9
Pendant votre voyage.....	9
À votre retour.....	10

Contexte

Les chercheurs sont souvent appelés à voyager à l'étranger dans le cadre de leurs travaux, et ces déplacements sont bénéfiques non seulement pour eux, mais aussi pour l'avancement général des connaissances au moyen de la recherche universitaire et de la collaboration. Les chercheurs et les universités du Canada constituent une ressource stratégique pour le pays et définissent notre place dans le monde d'un point de vue économique, politique et social.

En cette période de changements sur le plan géopolitique, les chercheurs canadiens qui voyagent à l'étranger peuvent être ciblés pour avoir accès à certaines sources d'information. En effet, les entreprises et les gouvernements étrangers convoitent les renseignements protégés en lien avec la recherche et l'innovation. Le présent guide ne contient pas de conseils généraux sur la sécurité en voyage; il met plutôt l'accent sur les risques directement liés à au recoupement entre les dynamiques géopolitiques et le domaine de la recherche. **Vous y trouverez de l'information sur les menaces motivées par des considérations économiques et géopolitiques qui pèsent sur vous, à titre de chercheur, ou sur vos travaux de recherche, des conseils à suivre pour réduire les risques et des mesures à prendre en cas d'incident.**

Il ne fait aucun doute, les déplacements internationaux pour les travaux de recherche ont leur raison d'être. L'information contenue dans le présent guide sert à vous sensibiliser aux risques associés aux voyages à l'étranger et aux mesures nécessaires à prendre pour veiller à votre propre protection ainsi qu'à celle de vos travaux de recherche. Par commodité, vous trouverez une liste de conseils sur la sécurité à l'annexe A.

1. Cinq raisons qui font des chercheurs canadiens une cible de choix

La quête de connaissances et d'excellence universitaire des chercheurs canadiens les amène à travailler partout au pays et même à l'étranger. Bien que les voyages fassent partie intégrante de votre travail de collaboration, cinq facteurs augmentent votre risque d'être victime de vol ou d'espionnage à l'étranger.

- 1. Nature des travaux de recherche :** Tous les travaux de recherche peuvent intéresser les personnes malveillantes, surtout s'ils portent sur l'un des sujets suivants :
 - a. Les pratiques de sécurité canadiennes ou étrangères, comme les manœuvres militaires ou l'application de la loi.
 - b. Les activités commerciales canadiennes ou étrangères, ou encore le développement de la propriété intellectuelle.
 - c. Les domaines des sciences, de la technologie, du génie et des mathématiques (STGM) et le secteur des nouvelles technologies.
 - d. La santé ou d'autres données personnelles (p. ex. le génome humain, des entrevues avec des personnages clés, etc.).
 - e. Les questions politiques délicates (nationales ou étrangères).
- 2. Accès aux partenaires indirects :** On pourrait s'intéresser à toute information pouvant être obtenue de votre part concernant vos partenaires de recherche, votre établissement, vos partenaires du secteur privé et le gouvernement canadien¹.
- 3. Accès aux États-Unis :** Puisque le Canada et les États-Unis entretiennent une relation étroite et que bien des chercheurs profitent de la mobilité entre établissements canadiens et américains, les chercheurs canadiens occupent une position stratégique unique. Ils peuvent avoir un accès privilégié à des technologies américaines de pointe que très peu de gens peuvent se procurer en toute légitimité. Ainsi, lorsqu'ils se déplacent à l'étranger, les chercheurs canadiens sont parfois vus comme des cibles faciles pour avoir accès aux établissements américains ou à leurs données de recherche.
- 4. Destinations :** Les chercheurs canadiens ont la chance de pouvoir voyager à peu près partout dans le monde. Bien que la plupart des pays soient sécuritaires, certains dangers sont présents et le niveau de risque évolue selon la dynamique mondiale.
- 5. Compagnons de voyage :** Les chercheurs ont souvent l'occasion de faire partie d'une délégation avec d'autres chercheurs, de hauts dirigeants universitaires, des chefs d'entreprise et des représentants du gouvernement. En vous déplaçant avec quelques personnalités bien en vue, vous risquez davantage d'attirer l'attention des gouvernements étrangers et de divers intervenants.

Conseils pour réduire les risques

- Évaluez le niveau de risque associé à votre voyage en ce qui concerne votre domaine de recherche, vos partenaires indirects et votre accès à des travaux de recherche américains, surtout dans les domaines sensibles.*
- S'il y a lieu, discutez de vos préoccupations avec les ressources appropriées dans votre université (superviseur, service de TI, bureau des voyages).*
- Consultez le [site Web des conseils aux voyageurs du gouvernement du Canada](#) et prenez les mesures appropriées selon votre destination.*
- Préparez un itinéraire de voyage et remettez-le aux personnes-ressources appropriées de votre établissement.*
- Inscrivez vos voyages à l'étranger à [Voyage.gc.ca](#).*
- Procurez-vous une assurance voyage auprès de l'agence de voyages de votre université ou d'une autre source.*

¹ Les liens que vous entretenez comme chercheur avec certains organismes comme l'Organisation du traité de l'Atlantique Nord (OTAN), le G7 et le G20, le Commonwealth, la Francophonie, l'Organisation des États américains (OEA), la Coopération économique pour l'Asie-Pacifique (APEC), l'Organisation de coopération et de développement économiques (OCDE), les Nations Unies (ONU) et l'Organisation mondiale du commerce (OMC) pourraient susciter de l'intérêt.

2. Votre profil

Les chercheurs universitaires se forgent une réputation par la qualité de leurs recherches et les nouvelles idées qui en découlent. Les voyages à l'étranger contribuent à accroître la visibilité de votre travail et à établir des contacts précieux. En sachant quel genre de renseignements sont accessibles à votre sujet et en apprenant à gérer votre profil adéquatement avant votre voyage, vous pouvez réduire les risques qu'un gouvernement étranger ou d'autres intervenants s'intéressent à vos recherches ou à vous-même pour les mauvaises raisons.

Il y a quatre principales façons de réunir de l'information à votre sujet avant même que vous arriviez.

- 1. Vos travaux de recherche et votre profil sur les médias sociaux** contiennent souvent des renseignements détaillés sur votre domaine de recherche, vos collaborateurs, vos opinions, vos contacts et votre famille. Tenez pour acquis que les intervenants intéressés peuvent consulter votre profil avant votre arrivée.
- 2. Les demandes de visa et de voyage** peuvent être combinées aux renseignements contenus dans votre profil sur les réseaux sociaux et votre profil de recherche pour évaluer le niveau d'intérêt d'un gouvernement étranger ou d'autres intervenants envers vos travaux de recherche et vous-même.
- 3. Les données bibliométriques** qui vous concernent seront probablement recueillies et échangées entre les diverses autorités.
- 4. Les agents des services frontaliers** recueillent, enregistrent et transmettent de l'information sur le motif de votre voyage. De plus, si vous avez déjà été signalée comme une personne d'intérêt, vous devrez peut-être répondre à des questions supplémentaires ou faire l'objet d'une inspection secondaire.

Conseils pour réduire les risques

- ❑ *Passez en revue votre profil de recherche et votre profil sur les médias sociaux avant votre voyage pour savoir quels renseignements sont disponibles à votre sujet. Au besoin, prenez les mesures nécessaires pour réduire votre présence sur les médias sociaux.*
- ❑ *Lorsque vous remplissez vos demandes de visa et de voyage, ne donnez que l'information strictement nécessaire. Évitez de fournir des renseignements personnels ou professionnels supplémentaires.*
- ❑ *Limitez au strict nécessaire l'information fournie aux agents des services frontaliers.*
- ❑ *Si vous devez vous soumettre à une inspection secondaire :*
 - sachez que vous avez le droit d'entrer en contact avec les services consulaires si les questions deviennent inappropriées;
 - si vous avez une double nationalité, informez-vous à l'avance sur la meilleure manière d'exercer vos droits.

3. Sources d'accès à vos recherches

Il est essentiel de communiquer vos résultats de recherche pour participer au succès de l'entreprise universitaire, et les conférences internationales constituent la plateforme idéale pour le faire. Toutefois, tous les chercheurs ont intérêt à s'assurer que leurs idées ne sont pas utilisées à leur insu ou sans qu'ils (ou leurs partenaires) n'y aient consenti.

Lorsque vous voyagez, les gouvernements, les entreprises et les intervenants étrangers peuvent utiliser vos renseignements personnels à votre insu de trois façons différentes :

1. Relations interpersonnelles
2. Intrusion physique
3. Cyberintrusion

Les prochaines sections du guide abordent chacun de ces sujets et présentent une liste de conseils à suivre pour atténuer les risques.

3-A. Relations interpersonnelles

Pour un chercheur, l'un des objectifs des voyages à l'étranger est de faire du réseautage lors des conférences et de mettre en commun ses champs de recherche, ses résultats et ses orientations futures. Il est toutefois important de savoir reconnaître les situations où ces activités normales risquent de servir d'occasions pour voler ou espionner les travaux de recherche.

- 1. Subtilisation de renseignements :** Un chercheur, un étudiant ou une personne du milieu des affaires (légitime ou non) agissant sous la contrainte entame une conversation qui semble anodine, mais qui a pour but de subtiliser des renseignements sur le chercheur, son travail et ses collègues.
- 2. Leurre :** Le chercheur, étudiant ou relation d'affaires entretient une relation avec le chercheur dans le but de lui soutirer de l'information.
- 3. Chauffeurs de taxi, serveurs et barmans :** Dans certains contextes, des gouvernements ou des groupes à la recherche d'information sur des étrangers peuvent confier différents rôles d'agents d'information à des gens ordinaires.
- 4. Piège sexuel pour chantage :** Une situation où un individu séduit sa victime pour la placer dans une position embarrassante et la soumettre à un chantage. Souvent, la victime est enregistrée à son insu pendant une relation sexuelle. L'enregistrement sert ensuite à faire chanter la victime ou à l'humilier publiquement.

Conseils pour réduire les risques

- Soyez vigilant et portez attention à l'évolution de vos relations, surtout les nouvelles relations et celles avec des ressortissants étrangers. Soyez attentif aux discussions concernant votre travail, même si la conversation semble anodine.**
- Évitez de parler des aspects délicats de vos travaux de recherche dans les lieux publics ou avec des personnes que vous connaissez depuis peu de temps.**
- N'acceptez pas la compagnie de gens que vous ne connaissez pas pendant votre voyage et soyez bien conscient des risques associés aux activités sexuelles (p. ex. âge de consentement et orientation sexuelle) dans les pays que vous visitez.**
- Si vous êtes victime d'une subtilisation de renseignements, d'un leurre ou d'un piège, ou si vous soupçonnez avoir été ciblé, avisez immédiatement le consulat canadien le plus près et déposez une plainte auprès de la personne-ressource appropriée de votre établissement, immédiatement ou à votre retour. Pour demander de l'aide d'urgence à l'étranger, communiquez avec le gouvernement du Canada par téléphone (1 613 996-8885) ou par courriel (sos@international.gc.ca).**

3-B. Intrusion physique

Le risque de vol en voyage n'est pas nouveau. Savoir que le risque est encore plus grand pour les chercheurs lorsqu'un gouvernement ou un intervenant s'intéresse à leurs travaux de recherche peut aider les chercheurs à assurer leur propre sécurité et celle de leurs travaux.

- 1. Hôtels :** Des agents directs et indirects du gouvernement peuvent se trouver parmi le personnel de l'hôtel et entrer par effraction dans votre chambre pour voler ou copier des documents ou encore vous piéger et vous soumettre à un chantage. Ils pourraient aussi donner accès à votre chambre à d'autres personnes. Alors que certains voyageurs ne remarquent pas qu'un individu est entré discrètement dans leur chambre pendant leur absence, d'autres ont déjà surpris des étrangers en train de fouiller dans leurs effets personnels ou de faire des tâches d'entretien sans raison apparente. Dans d'autres cas, quelques personnes qui soupçonnent avoir été droguées ont constaté à leur réveil que leur chambre d'hôtel avait été fouillée, que leur téléphone intelligent avait été volé et que des documents de nature délicate étaient manquants.
- 2. Salles de conférence :** Les salles de conférence peuvent être sous écoute et surveillées. Comme dans le cas des hôtels, des agents directs et indirects du gouvernement peuvent se trouver parmi le personnel.
- 3. Véhicules :** On pense souvent qu'un véhicule est un endroit sécuritaire pour une conversation professionnelle. Il peut toutefois avoir été mis sous écoute ou équipé de dispositifs de localisation qui permettraient à des intervenants externes de suivre vos déplacements.
- 4. Écoute clandestine :** Dans certains contextes, les conversations peuvent être interceptées dans les lieux publics ou dans les transports en commun. L'écoute clandestine peut se faire au moyen d'un témoin discret ou d'appareils audiovisuels de haute technologie dissimulés.

Conseils pour réduire les risques

- Consultez votre service de TI avant votre départ. Dans la mesure du possible, utilisez des téléphones « jetables » ou des appareils sécuritaires pour les déplacements. (Consultez la section 3-C sur la cybersécurité.)**
- Ne voyagez pas avec des appareils et des documents inutiles (listes de contacts, fichiers électroniques, etc.).**
- Soyez discret sur l'endroit où vous séjournez et sur votre numéro de chambre.**
- Ne laissez pas les clés de votre chambre à la réception de l'hôtel.**
- Laissez la radio ouverte dans votre chambre quand vous êtes absent.**
- Évitez d'utiliser les ordinateurs de l'hôtel ou des salles de conférence et les téléphones publics, car ils pourraient être surveillés.**
- Ne laissez pas vos appareils électroniques sur les lieux de la conférence.**
- Évitez de parler des aspects de nature délicate de vos travaux de recherche actuels ou futurs.**
- Si vous êtes victime d'un vol ou que vous soupçonnez qu'on a tenté de vous voler, avisez immédiatement le consulat canadien le plus près et déposez une plainte auprès de la personne-ressource appropriée de votre établissement, immédiatement ou à votre retour. Pour demander de l'aide d'urgence à l'étranger, communiquez avec le gouvernement du Canada par téléphone (1 613 996-8885) ou par courriel (sos@international.gc.ca).**

3-C. Cyberintrusion

Les appareils numériques vous permettent d'échanger de l'information et de maintenir le lien avec vos relations professionnelles. Toutefois, ces appareils vous exposent au vol de données et d'identité, que ce soit pendant vos déplacements ou à votre retour. Comme les pratiques exemplaires en cybersécurité évoluent rapidement, consultez votre service de TI avant de partir pour connaître les politiques et les pratiques en vigueur dans votre établissement. Voici quelques risques et pratiques exemplaires à considérer.

1. Interception des communications :

Les communications sans fil peuvent être surveillées dans tous les pays. Les autorités locales peuvent avoir accès aux réseaux de télécommunications, ce qui signifie qu'elles peuvent obtenir divers renseignements contenus dans vos appareils (registres d'appels, listes de contacts, documents, messages). Elles pourraient même être en mesure d'écouter et d'enregistrer vos appels. Le fournisseur de services Internet dispose de différents moyens techniques pour intercepter les données. Il peut même prendre le contrôle de toutes vos communications sur votre téléphone intelligent, votre tablette, votre ordinateur de bureau ou votre ordinateur portable. Vous demeurez vulnérables à ces intrusions bien après votre retour au pays.

2. Fraude d'identité et hameçonnage :

Vos renseignements personnels pourraient être utilisés par un fraudeur qui se servirait de votre identité pour envoyer des courriels avec des logiciels malveillants, comme des logiciels rançonneurs, à des employés de votre réseau professionnel. Cette fraude pourrait être coûteuse pour vos collègues ou votre établissement.

3. Clés USB : Les personnes malveillantes se servent souvent de ports et de clés USB pour avoir accès aux ordinateurs ou en compromettre la sécurité. Tout appareil qui peut être branché dans le port USB de votre ordinateur est une menace potentielle.

Conseils pour réduire les risques

- ❑ *Consultez votre service de TI pour vous assurer que tous vos appareils électroniques sont à jour en ce qui concerne les antivirus, le chiffrement, les pare-feu et les correctifs. Utilisez des téléphones « jetables » ou des appareils conçus pour les déplacements. Suivez les directives sur l'utilisation des réseaux privés virtuels et des dispositifs de protection pour accéder à Internet pendant vos déplacements.*
- ❑ *Avant de voyager, réfléchissez aux données dont vous aurez besoin. N'apportez que le minimum.*
- ❑ *Chiffrez et transférez vos données sur un périphérique de stockage externe que vous garderez avec vous en tout temps pendant votre voyage. Conservez les mots de passe pour vos données dans un endroit distinct.*
- ❑ *Si vous perdez de vue vos appareils à quelque moment que ce soit pendant votre voyage, tenez pour acquis que votre matériel a été exposé à des risques.*
- ❑ *Ne branchez aucun appareil externe (clé USB, caméra, cadre pour photo numérique, etc.) à vos appareils.*
 - Si vous devez absolument le faire pour un exposé lors d'une conférence, vous devez supposer que votre appareil a été exposé à des risques.
- ❑ *Si possible, évitez d'accéder à des données stockées dans un nuage pendant vos déplacements.*
 - Si vous en avez absolument besoin, assurez-vous d'y accéder seulement à partir de vos appareils personnels et sécurisés.
- ❑ *Si votre appareil est perdu ou volé, avisez immédiatement votre service de TI.*
- ❑ *À votre retour, prenez les mesures appropriées pour nettoyer votre disque dur et les autres appareils, surtout si vous avez des raisons de croire qu'ils ont été exposés à des risques. Avant de les utiliser, faites analyser vos appareils externes (y compris les cadeaux et le matériel promotionnel reçus lors des conférences) pour détecter la présence de virus.*

Annexe A – Liste de conseils sur la sécurité en voyage pour les chercheurs universitaires

Avant de partir

- ❑ Évaluez le niveau de risque associé à votre voyage en ce qui concerne votre domaine de recherche, vos partenaires indirects et votre accès à des travaux de recherche américains, surtout dans les domaines sensibles.
- ❑ Consultez le site Web des conseils aux voyageurs du gouvernement du Canada et prenez les mesures appropriées selon votre destination.
- ❑ S'il y a lieu, discutez de vos préoccupations avec les personnes-ressources appropriées de votre université (superviseur, service de TI, bureau des voyages).
- ❑ Préparez un itinéraire de voyage et remettez-le à une personne-ressource appropriée de votre établissement.
- ❑ Consultez votre service de TI avant votre départ.
 - Dans la mesure du possible, utilisez des téléphones « jetables » ou des appareils sécuritaires pour les déplacements.
 - Assurez-vous que tous vos appareils électroniques sont à jour en ce qui concerne les antivirus, le chiffrement, les pare-feu et les correctifs.
 - Demandez des conseils sur l'utilisation des réseaux privés virtuels et des dispositifs de protection pour accéder à Internet pendant vos déplacements.
- ❑ Ne voyagez pas avec des appareils et des documents superflus (listes de contacts, fichiers électroniques, etc.).
- ❑ Avant de voyager, réfléchissez aux données dont vous aurez besoin. N'apportez que le minimum.
- ❑ Chiffrez et transférez vos données sur un périphérique de stockage externe que vous garderez avec vous en tout temps pendant votre voyage. Conservez les mots de passe pour vos données dans un endroit distinct.
- ❑ Inscrivez vos voyages à l'étranger à Voyage.gc.ca.
- ❑ Procurez-vous une assurance voyage auprès du service des voyages de votre université ou d'un assureur.

Pendant votre voyage

Si vous êtes victime d'un événement indésirable ou si vous pensez être ciblé, avisez immédiatement le consulat canadien le plus près et déposez une plainte auprès de la personne-ressource appropriée de votre établissement, immédiatement ou à votre retour. Pour demander de l'aide d'urgence à l'étranger, communiquez avec le gouvernement du Canada par téléphone (1 613 996-8885) ou par courriel (sos@international.gc.ca).

Relations interpersonnelles

- ❑ Évitez de parler des aspects délicats de vos travaux de recherche (ou de vos futurs travaux de recherche) dans les lieux publics ou avec des personnes que vous connaissez depuis peu de temps.
- ❑ Soyez conscient des risques de subtilisation de renseignements, des leurres et des pièges. Portez attention à l'évolution de vos relations, surtout les nouvelles relations et celles avec des ressortissants étrangers. N'acceptez pas la compagnie de gens que vous ne connaissez pas pendant votre voyage.

Intrusion physique

- ❑ Soyez discret sur l'endroit où vous séjournez et sur votre numéro de chambre.
- ❑ Ne laissez pas les clés de votre chambre à la réception de l'hôtel.
- ❑ Laissez la radio ouverte dans votre chambre quand vous êtes absent.
- ❑ Évitez d'utiliser les ordinateurs de l'hôtel ou des salles de conférence et les téléphones publics, car ils pourraient être surveillés.
- ❑ Ne laissez pas vos appareils électroniques sur les lieux de la conférence ou à l'hôtel.

Cyberintrusion

- ❑ ***Ne laissez jamais vos appareils hors de votre vue pendant votre voyage. Si vous les perdez de vue, vous devez supposer qu'ils ont été exposés à des risques.***
- ❑ ***Ne branchez aucun appareil inconnu (clé USB, caméra, cadre pour photo numérique, etc.) à votre matériel.***
 - Si vous devez absolument le faire pour un exposé lors d'une conférence, vous devez supposer que votre appareil a été exposé à des risques.
- ❑ ***Si possible, évitez d'accéder à des données stockées dans un nuage pendant vos déplacements.***
 - Si vous en avez absolument besoin, assurez-vous d'y accéder seulement à partir de vos appareils personnels et sécurisés.
- ❑ ***Si votre appareil est perdu ou volé, avisez immédiatement votre service de TI.***

À votre retour

- ❑ ***À votre retour, prenez les mesures appropriées pour nettoyer votre disque dur et les autres appareils, surtout si vous avez des raisons de croire qu'ils ont été exposés à des risques. Faites analyser vos appareils externes (y compris les cadeaux et le matériel promotionnel reçus lors des conférences) pour détecter la présence de virus.***
- ❑ ***Si des activités suspectes ou criminelles sont survenues pendant vos déplacements, parlez-en à vos collègues, à une personne-ressource ou à un expert en voyage. Demandez des conseils pour savoir si vous devez communiquer avec les autorités.***