Service canadien du renseignement de sécurité

Canadian Security Intelligence Service

À L'ÉTRANGER

Directives de sécurité sur les voyages

DES RENSEIGNEMENTS ET DES CONSEILS FIABLES POUR UN CANADA SÛR ET PROSPÈRE.
A SAFE, SECURE AND PROSPEROUS CANADA THROUGH TRUSTED INTELLIGENCE AND ADVICE.

Canada

TABLE DES MATIÈRES

LE CONTEXTE DE LA MENACE	**4**
LA SÉCURITÉ EST UN ÉTAT D'ESPRIT	**5**
DEMANDES DE VISA ET PRÉPARATION AU VOYAGE	**9**
À L'AÉROPORT	**12**
POINTS D'ENTRÉE ET DONNÉES BIOMÉTRIQUES	**13**
SUBTILISATION D'INFORMATIONS, DÉMARCHES INTÉRESSÉES ET AUTRES PIÈGES	**16**
INTERCEPTION DE COMMUNICATIONS	**25**
TÉLÉPHONES MOBILES ET TÉLÉPHONES INTELLIGENTS	**29**
ORDINATEURS PORTATIFS ET TABLETTES	**31**
CLÉS USB	**33**
À DESTINATION	**34**

LE CONTEXTE DE LA MENACE

Dans un monde qui mesure de plus en plus la sécurité et la puissance nationale en termes économiques et militaires, les Canadiens qui voyagent à l'étranger peuvent être la cible d'activités de collecte de renseignements. Bon nombre d'entreprises et de gouvernements étrangers accordent une grande importance à l'acquisition d'informations classifiées protégées par le gouvernement et de données exclusives sensibles liées aux activités de recherche et d'innovation d'entreprises, d'industries et d'établissements d'enseignement canadiens. La menace qui pèse sur vous à titre de voyageur canadien est bien réelle.

Le présent guide décrit la nature des menaces que représentent le renseignement étranger, le terrorisme et l'espionnage économique. Vous y trouverez des précautions élémentaires qui pourront vous aider à atténuer les risques ainsi que les mesures à prendre pour signaler tout incident suspect.

LA SÉCURITÉ EST UN ÉTAT D'ESPRIT

Vous êtes responsable de votre propre sécurité. Une bonne préparation et l'application de mesures de sécurité efficaces permettent d'éviter la plupart des problèmes de sécurité.

Votre conscience situationnelle est votre meilleur outil en matière de sécurité : vous devez être conscient de tout ce qui se passe autour de vous et comprendre les répercussions que cela pourrait avoir sur votre propre sécurité. La situation peut changer de jour en jour ou même d'heure en heure. Soyez toujours attentif à votre environnement et tenez-vous au courant des menaces auxquelles vous serez exposé à destination.

Nous nous imaginons souvent que les voyages à l'étranger sont faciles et sûrs. Pour beaucoup d'entre nous, les voyages à l'étranger sont devenus tellement courants que nous présumons, à tort, qu'ils comportent peu de risques. Vous devez prendre des précautions particulières quand vous allez à l'étranger à titre officiel, surtout dans des pays qui suscitent des inquiétudes sur le plan de la sécurité. Avant de partir en voyage pour le compte d'un organisme gouvernemental, vous devriez assister à une séance d'information sur le pays visité; de telles séances sont offertes par des agents de sécurité désignés.

De même, si vous voyagez pour le compte de votre entreprise, groupe industriel ou établissement d'enseignement, vous devriez consulter une source de confiance comme **voyage.gc.ca** pour connaître la situation sécuritaire dans le pays. Ne présumez jamais rien quand vous voyagez à

l'étranger. Faites toujours des recherches sur votre destination et préparez votre voyage. Vous êtes toujours responsable de votre propre sécurité.

Redoublez de vigilance à l'étranger. Vous êtes vulnérable quand vous êtes à l'étranger parce que vous n'exercez que peu d'influence sur ce qui vous entoure. Les gouvernements étrangers et leurs agents agissent en toute impunité sur leur propre territoire, sans parler des extrémistes et des criminels locaux.

Familiarisez-vous avec les lois. Il est très important que vous vous familiarisiez avec les lois, les coutumes et la culture du pays où vous allez. En tant que voyageur vous êtes assujetti aux lois et aux règlements du pays que vous visitez. Votre passeport canadien ne vous confère guère d'immunité. Remarquez que même un passeport diplomatique ne vous empêchera pas d'être pris pour cible pendant votre séjour dans le pays hôte. Avant de partir, consultez le site **voyage.gc.ca** pour obtenir des informations propres au pays visité et prenez en note les coordonnées de l'ambassade, du haut-commissariat ou du consulat du Canada le plus près.

Pour de nombreux acteurs hostiles, le Canada et les Canadiens sont des cibles. Le Canada et les Canadiens ont été et seront encore pris pour cible par des services de renseignement étrangers à la recherche de secrets universitaires, industriels ou d'État. Vous pouvez aussi être la cible d'extrémistes qui vous considèrent comme un ennemi à titre de représentant d'un établissement d'enseignement, d'une

entreprise ou d'un gouvernement occidental ou encore la cible de criminels qui cherchent simplement à faire de l'argent rapidement. Bref, vous n'êtes pas à l'abri simplement parce que vous êtes Canadien. Vous constituez une cible légitime aux yeux des personnes qui souhaitent nuire au Canada. Ainsi, efforcez-vous d'être une cible difficile en évitant de vous montrer prévisible et accessible. Soyez toujours conscient de ce qui se passe autour de vous.

Vous ÊTES une cible digne d'intérêt. En tant que Canadiens, nous présumons souvent que notre citoyenneté fait de nous des cibles peu intéressantes. De même, nous avons l'impression que nous sommes peu susceptibles d'être victimes d'un crime en faisant nos réservations d'hôtel dans un endroit « sûr ». Or, ce sont les auteurs de la menace, et non les voyageurs, qui décident. Essayez toujours d'éviter d'attirer l'attention en voyage. Ne portez pas de vêtements ou d'articles dont les logos indiquent clairement que vous êtes un représentant étranger. Votre habillement, votre comportement et votre langage corporel sont très importants lorsque vous êtes en voyage. Ne faites pas étalage de vos richesses ou de quoi que ce soit qui pourrait vous rendre plus à risque de devenir une cible.

Ne négligez pas la menace que représentent les voleurs. Les porte-documents, les ordinateurs portatifs, les téléphones intelligents et autres articles du genre attirent au moins autant les criminels de tout acabit que les services de renseignement étrangers. Le résultat est le même : une infraction à la sécurité qui pourrait vous faire du tort et

qui risque de nuire au gouvernement du Canada, à votre entreprise ou à votre établissement d'enseignement et, par extension, au Canada dans son ensemble. Méfiez-vous des personnes qui vous offrent leur aide « spontanément » et soyez attentif aux distractions ou aux diversions qui permettent à des inconnus d'orienter ou de canaliser vos déplacements.

DEMANDES DE VISA ET PRÉPARATION AU VOYAGE

Les services étrangers peuvent commencer à recueillir des informations avant même que vous ayez réservé vos vols et vos hôtels. Dans certains pays, la collecte d'informations vous concernant commence bien avant votre arrivée. Les données que vous fournissez sur votre formulaire de demande de visa peuvent aider à déterminer l'« intérêt » que vous présentez en tant que cible, à établir un profil initial détaillé de la personne que vous êtes. Si vous faites partie d'une délégation commerciale, universitaire ou gouvernementale de haut niveau, tenez pour acquis que vous serez considéré comme une cible éventuelle.

Vous devez absolument préparer votre voyage pour en assurer le succès. Effectuez 70 % du travail au Canada. Avant de partir, peu importe votre destination, informez-vous sur la situation politique et sécuritaire générale dans le pays. Une fois arrivé à destination, vous serez prêt à passer à l'action. Le reste du travail (30 %) se fait à destination : veillez à maintenir votre conscience situationnelle, à vérifier vos informations et à vous familiariser avec le pays.

Les demandes de visa sont plus exhaustives et comportent plus de questions que jamais. Quand vous remplissez une demande de visa, dites la vérité, mais ne fournissez pas plus d'informations qu'il le faut. Examinez toutes les exigences relatives au visa avant de faire des réservations de voyage étant donné la nature intrusive des questions. Par exemple, certains pays exigent les numéros des passeports des membres de la famille, même si ces derniers ne voyagent pas avec vous. En outre, certaines questions sur la nature de votre emploi peuvent viser à obtenir

des détails très précis. Soyez conscient des informations à votre sujet qui sont accessibles au public. Avant de présenter une demande de visa, faites une recherche sur Internet en utilisant votre nom et le titre de votre poste afin de savoir ce qu'on peut trouver sur vous.

Soyez prêt à répondre aux questions à la frontière. Avant de partir, assurez-vous que vous serez à l'aise pour répondre aux questions que pourraient vous poser les douaniers du pays visité sur le motif de votre voyage. C'est particulièrement important si vous voyagez en groupe, parce que les autorités locales pourraient profiter de la moindre divergence entre les explications fournies par divers membres du groupe pour prendre des mesures contre vous.

Que devriez-vous apporter lorsque vous quittez le Canada? Avant de partir, envisagez d'autres moyens de transférer les informations dont vous aurez besoin en voyage, surtout celles qui sont de nature délicate.

Consultez un agent de sécurité désigné avant de partir. En consultation avec l'agent de sécurité de votre entreprise ou ministère, vous pourriez décider d'utiliser un appareil de télécommunication « jetable » en voyage. Il ne s'agit pas d'un appareil qui peut être jeté à la poubelle, mais plutôt d'un dispositif qui ne renferme aucune information avant le départ. Au retour, il est complètement purgé, et le système d'exploitation, réinstallé. N'apportez pas à l'étranger un appareil rempli de courriels, de contacts et de documents.

Liste de contacts. N'apportez pas de carnet d'adresses ou de liste de noms et de coordonnées qui ne sont pas nécessaires pour le voyage.

Communications. Pour votre propre sécurité, tenez des personnes au courant de vos allées et venues. Laissez les coordonnées à utiliser en cas d'urgence à votre superviseur et prévoyez des appels à intervalles réguliers ou laissez des messages à la maison. **L'inscription des Canadiens à l'étranger** est un service gratuit qui permet au gouvernement du Canada d'aviser les voyageurs en cas d'urgence à l'étranger (catastrophe naturelle ou agitation civile, par exemple) ou à la maison.

Voyagez léger. Ne vous encombrez pas de trop de bagages. Vous attirerez l'attention, votre mobilité s'en trouvera réduite et vous aurez beaucoup de choses à protéger.

À L'AÉROPORT

Que faire à l'aéroport ? En plus de suivre les consignes normales de sécurité, soyez vigilant et assurez-vous de pouvoir observer toute activité suspecte de la part d'autres passagers ou de membres de l'équipage, par exemple.

Agents de contrôle du transporteur aérien et des services frontaliers. Présumez toujours que le pays visité recueille toutes les informations fournies aux agents du transporteur aérien ou des services frontaliers. **Ces informations peuvent aussi être communiquées à d'autres pays.** Gardez votre passeport dans votre sac ou dans votre poche jusqu'à ce que vous arriviez au poste de contrôle frontalier.

N'affichez pas votre identité. Dissimulez toujours les étiquettes de vos bagages. En fait, vous devriez même placer les étiquettes à l'intérieur de vos bagages enregistrés et utiliser un autre moyen (p. ex. un ruban autour de la poignée) pour les reconnaître.

Bagages. Ne laissez pas vos effets sans surveillance. Présumez que vos bagages enregistrés seront fouillés durant le transport. N'acceptez jamais de transporter quelque chose pour une autre personne à moins de savoir sans l'ombre d'un doute de quoi il s'agit. Ne laissez personne mettre la main sur vos valises ou vos sacs. Ne les quittez pas des yeux ou gardez-les en votre possession en tout temps à l'aéroport. Les zones de récupération des bagages sont souvent prisées par les criminels. Soyez particulièrement vigilant à cet endroit.

POINTS D'ENTRÉE ET DONNÉES BIOMÉTRIQUES

Mesures de ciblage officielles et clandestines. Si vous êtes considéré comme une cible possible à l'étape du processus de demande de visa, il se peut que les services de renseignement du pays visité aient recours à des moyens officiels ou clandestins pour en savoir plus sur vous.

Filature. Dans de nombreux pays, vous devrez présumer que vous faites l'objet d'une filature. Assistez à une séance d'information sur le pays visité et effectuez quelques recherches sur le sujet avant de partir. Exercez toujours une saine vigilance.

Une fouille secondaire pourrait servir de prétexte pour saisir ou copier vos documents. Au point d'entrée – habituellement un aéroport – les services frontaliers locaux peuvent décider de vous soumettre à une inspection secondaire. Pendant l'inspection, tous vos effets peuvent être examinés, saisis ou copiés, y compris les documents que vous transportez ou qui sont dans votre ordinateur portatif, votre tablette ou votre téléphone intelligent.

Une fouille secondaire peut indiquer un intérêt d'un service de renseignement adverse. Elle peut aussi vouloir dire tout simplement que vous répondez à l'un des nombreux critères de sélection des passagers qui seront soumis à une inspection secondaire. Dans un cas comme dans l'autre, soyez toujours prêt à y faire face (soyez prêt à expliquer, entre autres, le but de votre visite et les biens en votre possession). Informez votre supérieur ou le chef de la délégation que vous avez été sélectionné pour faire l'objet d'une inspection secondaire.

Soyez prêt à invoquer votre droit à une assistance consulaire. Si, au cours d'une fouille secondaire, les agents vous posent des questions qui n'ont pas lieu d'être ou qui pourraient mener à votre détention, téléphonez à l'ambassade, au haut-commissariat ou au consulat du Canada. Il est important de savoir que vous avez droit à une assistance consulaire. Lorsque vous parlez aux représentants consulaires, dites-en le moins possible, parce que vous pourriez être sur écoute. Dans les pays qui sont parties prenantes à la Convention de Vienne sur les relations consulaires, les autorités qui procèdent à votre arrestation sont tenues de vous aviser de votre droit de parler à un agent consulaire et de prendre des dispositions à cet égard. Elles ne sont pas obligées d'avertir un bureau du gouvernement du Canada de votre détention ou arrestation, à moins que vous ne le leur demandiez expressément.

Si vous possédez une double citoyenneté et que vous voyagez dans l'autre pays dont vous êtes citoyen, les autorités locales peuvent vous refuser l'accès aux services consulaires canadiens, empêchant ainsi les agents consulaires canadiens de vous fournir ces services.

Les **données biométriques** sont de plus en plus utilisées aux points d'entrée pour démasquer les criminels et les terroristes qui se forgent souvent différentes identités et utilisent divers titres de voyage. Par la même occasion, les autorités accumulent énormément d'informations qu'un service de renseignement adverse pourrait utiliser. Vous êtes particulièrement vulnérable si vous voyagez dans un pays donné à différents moments, parfois pour affaires et

parfois pour des raisons personnelles. En pareil cas, les autorités locales vous connaissent déjà et savent quel est votre travail, ce qui peut causer de très graves problèmes si vous occupez un poste sensible. Parmi les techniques de biométrie figurent la reconnaissance faciale, la lecture de l'iris et les empreintes digitales. Dans certains pays, les données biométriques sont saisies à votre insu au moyen de caméras de télévision en circuit fermé. En outre, un certain nombre de pays **échangent des données biométriques recueillies avec les pays avoisinants**. Il est possible que ces informations soient facilement disponibles dans un pays où vous n'êtes jamais allé.

SUBTILISATION D'INFORMATIONS, DÉMARCHES INTÉRESSÉES ET AUTRES PIÈGES

Pourquoi s'intéresserait-on à vous? Les gouvernements étrangers essaient de recueillir des renseignements pour servir leurs intérêts en matière de politique étrangère, de sécurité et d'économie. À titre de représentant d'un organisme gouvernemental, d'une entreprise ou d'un établissement d'enseignement canadien, votre accès à des renseignements classifiés du gouvernement, à des informations privilégiées du secteur privé ou à des recherches universitaires fait de vous une cible intéressante pour les services de renseignement étrangers.

Relations. Tenez pour acquis que le gouvernement du pays que vous visitez sera informé de chacune de vos rencontres avec des relations personnelles, même si elles ont lieu en dehors des périodes prévues pour les réunions officielles. Présumez également que, selon les liens qu'elles entretiennent avec le gouvernement, vos relations à l'étranger seront interrogées avant votre arrivée ou après votre départ.

Des criminels peuvent s'intéresser aux informations dont vous disposez, surtout si elles concernent l'application de la loi. Si vous travaillez dans le domaine de l'application de la loi, les informations que vous détenez ou auxquelles vous pouvez avoir accès pourraient être d'un grand intérêt pour les organisations criminelles qui souhaitent savoir si elles font l'objet d'une enquête et s'il y a des fuites au sein de leur organisation.

Les secrets peuvent sembler banals. Les services de renseignement étrangers qui prennent pour cible le Canada et les Canadiens ne

cherchent pas seulement à mettre la main sur les « joyaux de la couronne », comme le plan détaillé d'un nouvel avion de chasse ou une recherche commerciale sensible sur un nouveau produit ou service. Ils peuvent vouloir des informations ou des connaissances qui semblent banales aux yeux du Canadien ou de l'établissement qui les détient. Un organigramme sans grande valeur en apparence peut répondre à un besoin important pour un service de renseignement adverse.

Les services de renseignement étrangers peuvent tenter d'obtenir accès indirectement à un pays allié ou à une entreprise qui n'est pas canadienne. Ils peuvent également s'intéresser aux informations ainsi qu'à l'accès qu'ils pourraient obtenir grâce à l'appartenance du Canada à diverses organisations 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), l'Organisation de coopération économique Asie-Pacifique (APEC), l'Organisation de coopération et de développement économiques (OCDE), l'Organisation des Nations Unies (ONU) et l'Organisation mondiale du commerce (OMC) ainsi qu'à des centaines d'organisations commerciales et professionnelles.

Obtention d'un accès à des technologies américaines de pointe. En sa qualité d'allié de confiance des États Unis, le Canada occupe une position stratégique unique qui lui assure un accès privilégié à des technologies américaines de pointe que peu d'autres pays peuvent se procurer légitimement. Les fonctionnaires et les chercheurs canadiens en

voyage à l'étranger peuvent être considérés comme des cibles éventuelles parce qu'ils ont accès à des données de recherche ou à des institutions américaines.

Le Canada : une source d'innovations technologiques et de propriété intellectuelle. Le Canada est membre d'un ensemble de partenariats militaires et stratégiques et regorge de ressources naturelles et de talents humains qui lui permettent de continuer de réaliser des percées technologiques. Ces technologies sont convoitées par des pays qui souhaitent accroître leurs propres possibilités technologiques et commerciales sans avoir à engager les frais liés à la recherche et au développement. La perte de telles informations réduit l'avantage concurrentiel du Canada et équivaut à un transfert de richesses du Canada vers un autre pays.

Comment la collecte d'informations est-elle effectuée?

Voici certaines des méthodes les plus fréquemment employées par les services de renseignement étrangers pour recueillir des informations.

Subtilisation d'informations. Il s'agit d'une technique au moyen de laquelle des agents de renseignement étrangers engagent avec vous une conversation qui semble anodine ou fortuite, mais qui a pour but de vous soutirer subtilement des informations sur vous, votre travail et vos collègues. Méfiez-vous si quelqu'un :

- **flatte votre ego;**
- **insiste sur vos intérêts communs et vous propose une autre rencontre pour en discuter;**
- **tient des propos erronés pour vous amener à le corriger en lui fournissant de l'information que vous détenez;**
- **vous fournit spontanément des informations selon le principe de « donnez et vous recevrez » ou vous communique certaines données de nature délicate dans l'espoir que vous lui rendrez la pareille;**
- **vous fait croire qu'il connaît très bien votre domaine de compétence. S'il s'agit d'un agent de renseignement, ses connaissances sont probablement limitées et superficielles, mais suffisantes pour donner le change et tenir une conversation.**

Démarches intéressées. Les approches bien orchestrées des services de renseignement adverses commencent par une période de « démarches intéressées ». Une relation est établie entre un représentant d'un service de renseignement (qui cache sa véritable identité) et l'éventuelle recrue qui ne se doute de rien. Vous devez être vigilant et surveiller la progression de vos fréquentations, particulièrement avec des gens que vous venez de rencontrer et des étrangers. Soyez toujours prudent quand la conversation s'oriente vers votre travail, même si elle semble banale.

Divulgation involontaire. Ne parlez jamais de votre travail et ne mentionnez jamais des informations de nature délicate en présence de chauffeurs de taxi, de serveurs ou de barmans, parce qu'il pourrait

s'agir d'agents de renseignement ou d'informateurs. La moindre bribe d'informations peut être utile à un concurrent.

L'« effet mosaïque ». Certains services de renseignement obtiennent un élément d'information de votre part et l'ajoutent à d'autres informations qui ont été acquises auprès de vos collègues ou qui vous ont été soutirées sans que vous vous en rendiez compte par d'autres sources avec qui ils travaillent. Vous aurez peut-être l'impression de ne pas avoir fourni la moindre information importante, mais le résultat peut être très précieux une fois plusieurs informations rassemblées (c'est ce qu'on appelle « l'effet mosaïque »).

Compromission et chantage. La compromission sexuelle consiste à utiliser une personne attirante – qui connaît votre identité et vos préférences sexuelles – pour vous séduire et vous placer dans une situation qui peut se révéler compromettante ou servir d'instrument de chantage. Il arrive souvent que des rencontres intimes soient enregistrées secrètement. Cet enregistrement est ensuite utilisé pour faire chanter ou embarrasser publiquement la victime. Des gouvernements étrangers utilisent cette méthode.Vous devez donc être conscient des risques lorsque vous acceptez de la compagnie en voyage. Certaines personnes croient également avoir été droguées. À leur réveil, elles ont constaté que leur chambre d'hôtel avait été fouillée et que leur téléphone intelligent et des documents d'affaires secrets avaient disparu. Il est important de connaître les lois régissant les activités sexuelles dans le ou les pays où vous allez, surtout en ce qui a trait à l'âge de consentement et à l'orientation sexuelle.

Méthodes secrètes (intrusions et autres). Des personnes hostiles pourraient décider de réaliser une opération d'intrusion vous visant. L'intrusion consiste à s'introduire par effraction dans une chambre d'hôtel pour voler ou copier des documents de nature délicate (copie papier ou électronique). Vous ne remarquerez peut-être pas l'infraction, mais certains voyageurs ont déjà surpris des individus en train de fouiller leurs effets ou de réaliser des travaux d'entretien inutiles. D'autres ont signalé que leur ordinateur portatif présentait des signes d'utilisation non autorisée ou était endommagé, que des paquets avaient été ouverts et refermés ou laissés ouverts ou encore que les mécanismes de verrouillage des porte-documents ou des valises avaient disparu ou avaient été forcés.

- **Les intrusions peuvent être réalisées par le gouvernement hôte, un service de renseignement d'un autre pays ou des gens à la solde d'une entreprise étrangère.**
- **Les intrusions sont souvent réalisées en collaboration avec le personnel hôtelier.**
- **Plusieurs pays et entreprises étrangères peuvent réussir à craquer les logiciels et les dispositifs informatiques commerciaux de protection contre les intrusions.**
- **Si vous signalez la preuve d'une intrusion à la direction de l'hôtel ou aux autorités locales, il est possible qu'elles vous trompent délibérément en affirmant traiter le dossier comme un acte criminel.**

Même s'il n'y a aucun signe évident d'intrusion, il se peut qu'un tel acte se soit produit en douce.

Écoute clandestine. Présumez toujours que vos conversations peuvent être écoutées dans les lieux publics et les transports en commun. L'écoute clandestine peut aller de la présence stratégique d'un passant discret à la dissimulation d'appareils audiovisuels perfectionnés.

- **Soyez discret en tout temps.**
- **Méfiez-vous de l'écoute clandestine durant les activités sociales où les participants ont l'impression qu'ils peuvent parler librement d'eux et de leur travail.**
- **Vous êtes particulièrement vulnérable dans les transports en commun et les services de transport offerts par l'hôte, les restaurants, les bars, les toilettes des salles de réunion, les chambres d'hôtel et au téléphone.**
- **Les appareils dissimulés ne coûtent pas cher, présentent peu de risques et peuvent être utilisés de concert avec des appareils visibles, comme des caméras de sécurité ou de surveillance routière ou piétonnière.**

Collecte d'informations de sources ouvertes. Les recherches dans les sources ouvertes ne se résument pas à taper votre nom et votre adresse sur Internet. Elles consistent aussi à fouiller dans toutes les sources publiques possibles, comme les revues spécialisées et universitaires, les sites Web, les réseaux sociaux ou les registres publics, pour trouver des informations sur vous, votre famille et votre travail. Vous

seriez surpris de constater la quantité d'informations que peut trouver une personne qui sait où et comment chercher. Même si vous pensez être discret et ne pas avoir laissé la moindre empreinte numérique, certaines informations sur vous, votre famille et vos amis sont facilement accessibles. Les informations recueillies servent à établir votre profil et à repérer les endroits où vous pourriez le plus facilement être abordé, ouvertement ou clandestinement. Une personne prête à y mettre les efforts peut dresser de vous ou de votre entreprise un portrait personnel, financier et professionnel. *N'oubliez pas que l'information à votre sujet sur Internet y restera presque certainement affichée pour toujours*.

Même si les réseaux sociaux ont leurs bons côtés, tout le monde sait maintenant qui vous êtes et peut-être même de quoi vous avez l'air. Vous n'avez peut-être pas vous-même de comptes sur les réseaux sociaux comme Facebook, Twitter ou LinkedIn, mais un membre de votre famille, un ami ou un collègue qui en a un peut avoir affiché par inadvertance de l'information à votre sujet. Rappelez à vos parents et amis d'être discrets quand ils affichent de l'information sur vous. Même si vous appliquez des paramètres de sécurité et de confidentialité renforcés dans vos comptes sur les médias sociaux, vous devez considérer toutes les informations publiées en ligne comme accessibles au public.

Même les ordures renferment des informations. Il est possible de trouver une foule d'informations sur vous en fouillant dans vos ordures. Faites attention à ce que vous jetez, surtout s'il s'agit de documents de

nature délicate. Ne jetez pas de notes professionnelles ou personnelles dans les poubelles de votre chambre d'hôtel ou dans les salles de réunion.

Soyez prudents lorsque vous acceptez des cadeaux. Méfiez-vous des cadeaux, surtout les cadeaux électroniques qui peuvent être branchés à votre ordinateur (clés USB, appareils photo, cadres numériques, etc.). De tels articles peuvent être contaminés par un maliciel ou un virus qui assurerait un accès à distance à votre ordinateur et à votre réseau. Ne branchez jamais un appareil dont vous ignorez l'origine sans l'avoir convenablement passé au détecteur de virus. Veuillez consulter votre équipe de technologie de l'information (TI) ou les procédures de votre entreprise en matière de sécurité avant d'utiliser tout cadeau numérique.

Le secteur privé s'adonne aussi à ce type d'activités. Certaines entreprises privées rassemblent de l'information de sources ouvertes sur des gens et des entreprises contre rémunération. Elles peuvent aussi utiliser des méthodes plus intrusives pour y parvenir.

INTERCEPTION DE COMMUNICATIONS

Interception de vos communications. Les communications sans fil peuvent être surveillées dans n'importe quel pays. Votre institution peut avoir des conseils sur l'utilisation des services sans fil en voyage, par exemple, sur l'utilisation de réseaux privés virtuels. Il est aussi important de consulter le site **voyage.gc.ca** pour être au courant du niveau de sécurité recommandé dans la région géographique où vous allez. Les autorités locales peuvent accéder aux réseaux de télécommunications, ce qui signifie qu'elles peuvent avoir accès aux informations qui se trouvent sur vos appareils, comme les journaux des appels, les listes de contacts ou les messages, et qu'elles peuvent même écouter et enregistrer vos appels téléphoniques. Envisagez de partir avec un téléphone ne contenant que les informations dont vous avez besoin pour votre voyage.

Vulnérabilité des appareils sans fil. La plupart des appareils que vous transportez peuvent être branchés à Internet ou sont accessibles au moyen d'un réseau sans fil, ce qui les rend vulnérables aux cyberattaques et au piratage. Les pirates peuvent avoir accès à votre disque dur et à tout ce qui s'y trouve à votre insu. Ils peuvent activer votre microphone ou votre appareil photo. Ils peuvent notamment enregistrer chaque touche et chaque numéro que vous saisissez. Ces failles peuvent être exploitées longtemps après votre retour à la maison. Soyez vigilant et signalez les activités suspectes.

Appliquez de bonnes mesures de sécurité électronique : Ne laissez personne brancher un appareil externe à votre matériel.

Les autorités n'ont aucune raison de placer votre matériel à un endroit où vous ne pouvez pas le voir, que ce soit à l'aéroport, à un point de contrôle de sécurité ou à l'hôtel. Si cela se produit, même pour très peu de temps, présumez que votre matériel a été compromis.

Tous les types de communications électroniques sont vulnérables. En théorie, tous les types de communications (les communications vocales, les messages texte, la messagerie instantanée, la navigation sur le Web, l'utilisation des réseaux sociaux, etc.) peuvent être interceptés. Il convient toutefois de noter que les conversations sur une ligne terrestre – même si elles ne sont pas protégées – sont habituellement plus difficiles à intercepter que les conversations sur un téléphone mobile. Le téléphone public peut être une solution de rechange intéressante, mais vous ne devez pas tenir pour acquis que vos conversations seront protégées.

Interception des communications vocales par l'entremise du fournisseur de services de télécommunication. Les autorités peuvent surveiller vos conversations téléphoniques. Elles peuvent tirer des informations directement des propos échangés, mais aussi des numéros composés (relevés d'appels). L'étude des habitudes d'appel permet d'établir le profil non seulement de la personne, mais aussi de son organisation.

Interception des données par l'entremise du fournisseur de services Internet. Le fournisseur de services Internet dispose de moyens techniques d'interception des données. Qu'il s'agisse d'un téléphone intelligent, d'une tablette ou d'un ordinateur de bureau ou portatif, il est possible d'intercepter les communications et même de prendre le « contrôle » de l'appareil.

Votre véhicule est un dispositif d'écoute. Lorsqu'ils sont en voyage d'affaires, les gens ont souvent l'impression qu'ils peuvent parler du travail dans un véhicule loué. Or, l'installation d'appareils dans le véhicule ou la manipulation des technologies qui y ont été intégrées par le fabricant peuvent permettre de les écouter et de les localiser.

Fraude à l'identité et hameçonnage. Il existe une autre raison pour laquelle vous devez protéger vos informations en voyage : un pirate pourrait les utiliser afin de se faire passer pour vous et d'envoyer des courriels truffés de maliciels à des employés de votre entreprise ou à d'autres personnes dans l'espoir d'amener ces gens à ouvrir les courriels et les pièces jointes, ce qui contaminerait automatiquement leurs ordinateurs ou leurs réseaux. Si vous assistez à des conférences ou suivez une formation à l'étranger, sachez que les pirates peuvent se servir des listes de présence pour vous prendre expressément pour cible au moyen de courriels bien conçus. Réfléchissez avant de cliquer!

Entreposage. Ne remettez pas vos téléphones cellulaires ou intelligents à la réception ou aux postes de sécurité. Laissez-les plutôt à l'ambassade, au haut commissariat ou au consulat si vous voyagez à titre de représentant du gouvernement, ou déposez-les à tout autre endroit sûr si vous voyagez pour affaires.

Au retour. Si vous avez apporté du matériel ou des logiciels de votre organisation en voyage, faites-les examiner par le technicien ou le service de TI avant de les utiliser à votre lieu de travail, de façon à détecter tout signe d'intrusion ou de compromission.

TÉLÉPHONES MOBILES ET TÉLÉPHONES INTELLIGENTS

Interception des communications vocales

L'interception illicite des communications sans fil suscite toujours des préoccupations. Il est très difficile de protéger les appels téléphoniques effectués sur des appareils sans fil à moins d'utiliser de coûteux produits de tiers pour en assurer le chiffrement. Là encore, les autorités du pays hôte ont accès aux réseaux cellulaires.

Interception des transmissions de données

Il est particulièrement inquiétant de savoir que les infrastructures de certains gouvernements étrangers sont en mesure d'isoler, de déchiffrer et de stocker certaines communications de données que l'on croit souvent protégées au moyen de logiciels de chiffrement brevetés. Présumez que vos transmissions de données sont interceptées.

Microphones ouverts dans des endroits sécurisés – téléphones mobiles

Le simple fait d'apporter un téléphone cellulaire dans une zone de sécurité entraîne un risque de transmission (non intentionnelle) à partir du microphone ouvert. Tous les téléphones cellulaires doivent être gardés à l'extérieur des zones protégées.

Localisation

La surveillance clandestine des allées et venues de l'utilisateur est particulièrement préoccupante. Les téléphones intelligents fournissent

à un adversaire sérieux le moyen de suivre les mouvements de l'appareil ciblé et de son utilisateur, c'est-à-dire qu'ils lui permettent d'intercepter ou d'obtenir les données GPS transmises ou stockées dans le téléphone. Votre téléphone a une signature unique qui, une fois qu'elle a été repérée par un pirate informatique, peut être suivie n'importe où dans le monde.

Bluetooth et Wi-Fi

D'autres réseaux sans fil accessibles au moyen de la plupart des téléphones intelligents, comme le Bluetooth et le Wi-Fi, comportent des failles additionnelles en matière d'interception et de perte des données qu'un pirate informatique peut exploiter. Par définition, le Wi-Fi public n'est pas privé!

Téléphones intelligents ou ordinateurs portatifs perdus ou volés

Lorsqu'on perd ou qu'on se fait voler un appareil, ce ne sont pas les frais de remplacement qui inquiètent le plus, mais l'accès non autorisé aux données qu'il contient. Ce risque peut être atténué au moyen de mots de passe, d'un logiciel de chiffrement, d'un verrouillage temporisé et d'un nettoyage à distance.

Ne laissez jamais un téléphone intelligent ou un ordinateur portatif sans surveillance. Il pourrait être compromis en quelques secondes.

ORDINATEURS PORTATIFS ET TABLETTES

Informations personnelles. Ne conservez pas d'informations personnelles dans votre ordinateur portatif. Un produit comme « Identity Finder » peut trouver sur votre disque dur des dossiers susceptibles de contenir des informations personnelles. Envisagez de laisser vos appareils personnels à la maison parce qu'ils sont aussi vulnérables que les appareils de votre organisation, mais plus difficiles à remplacer.

Dossiers sensibles. Supprimez-les du disque dur et sauvegardez-les sur une clé USB, au besoin. Pour vous assurer que les dossiers sont effectivement supprimés du disque dur de l'ordinateur portatif, utilisez un logiciel de nettoyage qui a fait ses preuves. Gardez la clé USB sur vous. Chiffrez les dossiers sur le support amovible et conservez le mot de passe à un autre endroit.

Stockage infonuagique. Sachez que certaines applications et certains navigateurs Web enregistrent les mots de passe. Étant donné la connectivité inhérente à l'infonuagique, toutes les informations stockées deviendraient accessibles et non protégées si ces mots de passe étaient compromis. Les autres comptes ou bases de données auxquels il est possible d'avoir accès au moyen de ces mots de passe seraient aussi vulnérables. Dans la mesure du possible, limitez vos interactions avec les disques infonuagiques lorsque vous êtes en voyage en transférant les recherches et les documents nécessaires dans un appareil sûr et sain. Si vous devez accéder au stockage infonuagique, assurez-vous de ne le faire que sur des appareils personnels et sûrs.

Pile. Assurez-vous que la pile de votre ordinateur portatif est chargée avant de vous rendre à l'aéroport et attendez-vous à devoir prouver que votre ordinateur fonctionne correctement. Assurez-vous que votre écran de mise en marche est anodin.

Sécurité à l'aéroport. Ne déposez votre ordinateur sur le tapis roulant du dispositif à rayon X que lorsque votre tour est venu de traverser le portique de détection des métaux. Vous pourrez ainsi le reprendre rapidement quand il sortira à l'autre bout et empêcher que quelqu'un s'en empare. Ne placez jamais votre ordinateur dans un bagage enregistré. **Ne le perdez jamais de vue. Il s'agit d'un article très prisé.**

CLÉS USB

Comme ces appareils sont souvent très petits, il est facile de les perdre, de se les faire voler ou de les cacher.

Popularité. La popularité des clés USB en fait un moyen pour les cybercriminels de répandre des maliciels. Comme elles sont même prises pour cible à l'étape de la production, pendant leur fabrication, une clé toute neuve pourrait être déjà contaminée. Soyez prudent si vous projetez de vous en servir.

Exécution d'un code de logiciel. Un ordinateur peut exécuter un code de logiciel à partir d'une clé USB dès qu'elle est branchée. Le logiciel qui a été installé peut faire en sorte que la clé USB s'exécute automatiquement quand elle est insérée dans un système d'exploitation, faisant croire à ce dernier qu'il s'agit d'un disque compact, puis envoyant un maliciel dans l'ordinateur. Lorsqu'ils apparaissent, divers problèmes liés, par exemple, à la perte de données, à la consommation de bande passante, au comportement du réseau, à l'octroi de licences de logiciels ou encore à la productivité peuvent être des indices qu'un appareil a été manipulé.

Autres risques. Il est facile d'amener des gens à divulguer des informations personnelles et confidentielles dans le cadre d'une fraude généralisée, d'une collecte d'informations ou d'un stratagème d'accès à un système. Il suffit par exemple de déposer plusieurs clés USB quelque part près de la cible (p. ex. dans un hôtel) et d'attendre qu'une victime sans méfiance en insère une dans son système pour que l'auteur du stratagème puisse accéder au système et le manipuler.

À DESTINATION

Hôtels

Personnel hôtelier. Ne fournissez que les informations nécessaires pour effectuer vos transactions. Si on vous demande le nom de votre employeur ou de votre organisme, utilisez les informations les plus générales possible. Ne donnez pas d'informations non sollicitées. Ayez des copies de votre passeport à portée de main au lieu de remettre votre passeport lui-même. Essayez toujours d'exercer un contrôle serré sur votre passeport.

Téléphones et ordinateurs de l'hôtel. Soyez prudent quand vous utilisez les téléphones et les ordinateurs de l'hôtel parce que les autorités ont accès à ces réseaux.

Répondez « Allo ». Si votre téléphone sonne, répondez simplement « Allo ». Là encore, ne fournissez pas d'informations non sollicitées, car l'appel peut être utilisé pour confirmer que vous êtes effectivement dans une chambre donnée.

Coffres-forts d'hôtels et mise sous clé des documents classifiés. N'utilisez pas le coffre-fort de l'hôtel pour ranger vos documents classifiés ou de nature délicate. Ne laissez pas de documents ou de matériel classifiés ou sensibles sans surveillance dans votre chambre d'hôtel. Il est préférable de déposer les documents gouvernementaux classifiés dans un endroit sûr à l'ambassade, au haut commissariat ou au consulat.

Utilisez le chiffrement et les réseaux privés virtuels (RPV) si vous devez travailler sur des réseaux non protégés. En voyage officiel, ne travaillez jamais sur un réseau ouvert (à l'hôtel, dans un café, etc.) parce que son contenu peut facilement être intercepté (voir ci-dessous). Avant de partir, discutez avec un agent de sécurité désigné ou un agent de la TI de votre ministère, entreprise ou établissement des divers RPV ou méthodes de chiffrement auxquels vous avez accès.

Ne travaillez jamais à partir d'un réseau ouvert ou du réseau de l'hôtel. Évitez d'utiliser une connexion Wi-Fi gratuite ou inconnue parce que vous pourriez accéder à un réseau contrôlé par un service de renseignement ou, plus probablement, par un criminel. Le Wi-Fi est disponible dans de nombreux endroits comme les aéroports, les cafés et les gares ferroviaires. Ces systèmes sont très vulnérables aux activités des pirates informatiques, des concurrents ou des services de renseignement étrangers. Il est donc préférable d'éviter de les utiliser pour tenir des discussions ou échanger des informations sensibles ou exclusives. Assurez-vous que des fonctionnalités ou un logiciel de chiffrement sont installés sur votre réseau local sans fil pour éviter la compromission. Veillez à faire remplacer les systèmes de chiffrement préinstallés.

Soyez discret sur l'endroit où vous logez. Si quelqu'un connaît le numéro de votre chambre, il est plus facile pour lui de vous prendre pour cible, qu'il s'agisse d'un agent de renseignement ou d'un criminel. Cela est particulièrement important pour les femmes. Veuillez consulter le site **voyage.gc.ca** pour en savoir plus sur la façon d'assurer votre sécurité

personnelle. Pour des raisons de sécurité, rencontrez toujours les invités dans le hall d'entrée de l'hôtel, jamais dans votre chambre.

Faites comme s'il y avait toujours quelqu'un dans votre chambre. Laissez la télévision ou la radio en marche ou les lumières allumées pour donner l'impression qu'il y a quelqu'un dans la chambre. Les criminels sont opportunistes et ne courront probablement pas le risque d'entrer dans votre chambre s'ils croient qu'il y a quelqu'un. Fermez les rideaux pour éviter les regards indiscrets. Laissez la carte « Ne pas déranger » sur la porte. **N'ouvrez jamais la porte à quelqu'un sans avoir vérifié au préalable son identité auprès de la réception. Vérifiez toujours auprès de la réception l'identité d'une personne qui se présente à l'improviste ou sans avoir été invitée.**

Sorties de secours. Repérez toujours les sorties de secours en cas d'urgence. Dans certains cas, il est essentiel de sortir rapidement. Vous n'aurez peut-être pas le temps d'attendre. Assurez-vous que votre chambre n'est **pas** accessible au niveau de la rue (plus bas que le 3e étage), mais qu'elle **est** accessible aux premiers intervenants (plus bas que le 7e étage, que les échelles de pompier peuvent atteindre). Munissez-vous en tout temps d'une trousse d'urgence contenant une lampe de poche, votre passeport, de l'argent, vos cartes de crédit, vos médicaments, vos lunettes, de l'eau, des barres repas, etc.

Ne confiez jamais vos clés à quelqu'un. Il s'agit d'une simple mesure de sécurité.

Généralités

Dans la mesure du possible, voyagez avec des appareils « jetables ». Envisagez d'apporter des appareils sains ou « jetables » en voyage. Même s'ils ne sont pas piratés ou manipulés, ils peuvent être volés. Les ordinateurs portatifs, les téléphones intelligents et les clés USB sont tous des appareils mobiles essentiels pour communiquer avec vos collègues, mais ils comportent des risques.

- **Ils ne doivent être utilisés par personne d'autre que vous.**
- **Ils ne doivent pas être branchés à des appareils sans fil non protégés.**
- **Ils ne doivent contenir aucun logiciel non autorisé.**

Un accès direct à ces appareils permet d'en extraire des données ou de compromettre des systèmes à l'appui d'activités de collecte d'informations.

Consultez votre service de TI. Assurez-vous que les derniers logiciel antivirus, logiciel de chiffrement, pare-feu et correctifs de programmes ont été installés sur vos appareils. N'oubliez pas que votre ordinateur ou votre téléphone intelligent peut être utilisé comme porte d'entrée pour avoir accès au réseau et, de là, à vos « joyaux de la couronne ».

La menace d'enlèvement est réelle. Dans certains pays, la menace d'enlèvement par des terroristes est importante, parce que bon nombre de groupes comptent sur ce type d'activité criminelle pour financer leurs opérations. Pour réduire le risque d'être pris pour cible, soyez attentif aux indices d'une reconnaissance de nature hostile, variez

vos habitudes et empruntez différents itinéraires pour passer de votre lieu de travail à votre hôtel et vice-versa. Les terroristes utilisent les mêmes méthodes que les agents de renseignement pour obtenir des informations. Ils subtilisent des informations et mènent diverses activités de collecte. Votre meilleur moyen de défense est d'être attentif à ce qui se passe autour de vous. La routine et le relâchement de la vigilance sont les deux causes les plus fréquentes des problèmes de sécurité.

Ne parlez pas du travail dans des lieux non protégés. Tenez pour acquis que votre chambre d'hôtel est sur écoute et que la liste des appels téléphoniques faits de votre hôtel sera recueillie par le pays hôte. Ne parlez pas du travail dans les taxis, les transports en commun et les lieux publics. Il est également possible que le taxi soit muni d'une caméra et d'autres équipements audiovisuels. Ces technologies, qui peuvent être installées dans tous les taxis pour assurer la sécurité du chauffeur, peuvent avoir un double usage.

Taxis. Essayez de prévoir vos moyens de transport. Demandez à quelqu'un de fiable de venir vous chercher. Si ce n'est pas possible, utilisez la navette gratuite de l'hôtel si ce service est offert ou faites une recherche à l'avance pour trouver une entreprise de taxis de bonne réputation. Négociez toujours le montant de la course avant le départ, ne partagez jamais un taxi avec un étranger et ne prenez jamais un taxi anonyme ou qui n'a pas de permis officiel bien visible. Assoyez-vous toujours à l'arrière, en diagonale du chauffeur. Cette place vous permet de voir les

mains du chauffeur et de sortir plus facilement du taxi en cas d'urgence (sur le trottoir plutôt que du côté de la circulation, par souci de sécurité).

Vos données personnelles sont stockées sur plusieurs appareils. Le terme appareils électroniques renvoie principalement à votre téléphone et à votre ordinateur portatif, mais même votre porte-clé et votre montre intelligente peuvent être pris pour cible parce qu'ils contiennent des données personnelles comme des photos, des horaires et des informations sur votre santé. Ces appareils peuvent être de véritables mines d'or pour les services de renseignement, les entreprises concurrentes, les établissements d'enseignement et les criminels. Évitez de vous laisser distraire par vos appareils. Soyez toujours conscient de ce qui se passe autour de vous quand vous les utilisez.

Évitez les quartiers où le taux de criminalité est élevé. Normalement, vous ne devriez pas visiter ces quartiers. Par contre, si vous devez absolument vous y rendre, prévoyez des mesures appropriées pour garantir votre sécurité, par exemple des vérifications en personne ou par téléphone à intervalles réguliers. Soyez conscient que la population locale se rendra immédiatement compte que vous êtes un étranger. En cas de vol, ayez un portefeuille ou un sac « jetable », contenant de fausses cartes de crédit et de l'argent américain ou en devises du pays, pour satisfaire un voleur et éviter des ennuis.

Les criminels cherchent eux aussi à tirer parti des informations disponibles. Les criminels sont des opportunistes. Ils attendent que

vous commettiez une erreur pour en profiter. Vous leur facilitez la tâche si vous fournissez spontanément des informations sur vous, sur vos allées et venues ou sur vos biens à des personnes que vous ne connaissez pas. Par exemple, quand vous êtes dans un taxi, n'expliquez pas comment utiliser le coffre-fort de l'hôtel pour y ranger votre ordinateur portatif ou d'autres biens de valeur, puis à votre arrivée à destination, ne payez pas avec une carte de crédit et ne mentionnez pas votre nom. Ce type d'information peut être très utile pour les criminels, parce qu'eux aussi payent pour obtenir des informations.

N'attirez pas l'attention. Soyez discret au sujet de votre identité, de votre travail et des objets de valeur que vous transportez.

Dans la mesure du possible, évitez de voyager seul. Il est habituellement plus sûr de voyager en groupe. Les criminels, comme les autres types de prédateurs, sont moins enclins à cibler un groupe qu'une personne seule. Le groupe doit toutefois s'efforcer d'être discret pour éviter d'attirer indûment l'attention.

Médicaments et établissements de soins de santé. Voyagez toujours avec suffisamment de médicaments prescrits dans leurs contenants originaux pour la durée du séjour. Prévoyez une réserve au cas où votre retour serait retardé. Assurez-vous que les médicaments que vous transportez sont conformes aux lois du pays visité. Renseignez-vous également sur les établissements de soins de santé, les soins d'urgence

locaux, les modes de paiement, les normes de soins et les services dispensés dans le pays visité.

Argent. Arrivez toujours avec suffisamment d'argent en devises locales (ou suffisamment d'argent que vous pourrez utiliser à destination) pour les 24 premières heures.

Réaction à une menace. Restez calme, évaluez vos possibilités et retirez-vous ou éloignez-vous si possible. Attirez l'attention en criant ou en faisant du bruit. Essayez de mettre de la distance entre votre agresseur et vous au moyen de meubles ou d'un véhicule. En voyage, il est utile de se munir d'un sifflet, parce qu'il permet d'attirer l'attention presque n'importe où.

N'oubliez pas – Ayez toujours un plan de base et un plan en cas d'urgence.

Voyagez de façon intelligente
Souscrivez une assurance-voyage
Inscrivez-vous auprès de Voyage.gc.ca
En cas d'urgence à l'étranger,
composez le numéro 1-613-996-8886, à frais virés.
sos@international.gc.ca