GUIDE D'ACTION SUR LES CONSIDÉRATIONS DE SÉCURITÉ PERSONNELLE POUR LESPERSONNES TRAVAILLANT SUR LES INFRASTRUCTURES CRITIQUES

INTRODUCTION

Dans le contexte actuel de menaces, il est essentiel pour toutes les personnes travaillant dans les infrastructures critiques de rester vigilantes et d'assumer la responsabilité de leur sécurité personnelle, tant au travail qu'en dehors. Les personnes travaillant dans les infrastructures critiques fournissent un large éventail de services qui assurent le fonctionnement, l'exploitation et l'entretien des systèmes et équipements clés nécessaires à la vie moderne des Américains. La prise en compte des risques ou des menaces liés à votre activité professionnelle et le respect de toutes les procédures de sécurité contribueront à votre protection, à celle de vos proches et à celle de l'infrastructure sur laquelle vous travaillez. La sécurité personnelle peut être segmentée en trois parties principales : la sécurité physique, la connaissance de la situation et la sécurité en ligne. Ce guide d'action non exhaustif a pour but de vous aider à évaluer votre niveau de sécurité et de vous proposer des options à envisager pour pallier les menaces.[1]

ÉVALUATION D'UN NIVEAU DE PROTECTION APPROPRIÉ POUR LES PERSONNES TRAVAILLANT DANS LES INFRASTRUCTURES CRITIQUES

Ce guide donne un aperçu général de la manière de rester en sécurité à la maison, au travail, en public et en ligne. Il vous revient de décider des mesures les plus appropriées à votre mode de vie, à vos vulnérabilités en matière de sécurité et aux situations que vous pourriez rencontrer, par exemple, certains facteurs peuvent accroître le risque de violence sur le lieu de travail :

- **Travailler seul** ou dans des zones isolées.
- **Fournir des services** ou des soins **en personne.**
- **Travailler avec des produits dangereux** ou des informations sensibles sur le plan de la sécurité nationale.
- **Responsabilité de la protection** d'infrastructures critiques locales ou nationales.

Lors de l'évaluation de vos besoins en sécurité, tenez compte des éléments suivants :

- **Votre profession et votre rôle professionnel.** Est-ce que votre emploi ou votre carrière fait de vous une cible attrayante ?
- **Menaces spécifiques.** Existe-t-il des preuves crédibles suggérant un risque pour vous ?
- **Votre histoire personnelle.** Avez-vous été pris pour cible ou menacé dans le passé ?
- **Vos identifiants visuels personnels.** Montrez-vous une appartenance à un groupe qui ferait de vous une cible attrayante ?

Aujourd'hui, les personnes travaillant dans les infrastructures critiques sont potentiellement confrontées à un large éventail de menaces, depuis les activités criminelles ordinaires jusqu'aux complots d'extrémistes violents. Si vous avez répondu par l'affirmative à une ou plusieurs des questions ci-dessus, il se peut que vous et potentiellement d'autres employés travaillant dans des infrastructures critiques soyez exposés à des risques et que vous deviez évaluer vos besoins en matière de sécurité. Au moment d'évaluer votre sécurité personnelle, il est important d'adopter une approche équilibrée et de ne pas oublier de tenir compte à la fois de votre vie privée et de votre vie professionnelle, **soyez vigilant dans vos pratiques et habitudes de sécurité personnelle et évaluez continuellement votre environnement.** Les mesures que vous prenez doivent être adaptées aux menaces perçues. Des mesures de sécurité excessives sont parfois source de stress et de désagréments inutiles ; en revanche, des dispositions insuffisantes peuvent vous mettre en danger.

La capacité à reconnaître les situations de vulnérabilité est essentielle pour les éviter ou s'y préparer si elles se produisent. Une vulnérabilité est une caractéristique physique ou un attribut opérationnel qui rend une entité, un bien, un système, un réseau ou une zone géographique susceptible d'être exploité ou exposé à un risque donné.[2] Les agresseurs peuvent faire preuve de créativité quand ils ciblent des personnes. L'objectif d'un agresseur peut être de causer de l'embarras, des désagréments ou de la détresse, mais il peut aussi avoir l'intention de causer des blessures physiques, de perturber le bien-être ou de menacer des vies humaines.

1 ProtectUK. 2022. Publicly accessible locations (PALs) guidance: Personal security. Consulté le 8 août 2023. protectuk.police.uk/personal-security.

2 Département de la sécurité intérieure des États-Unis. Comité de direction sur le risque. 2010. Édition 2010 du lexique sur le risque du DHS. Consulté le 8 août 2023. cisa.gov/resources-tools/resources/dhs- risk-lexicon.

SÉCURITÉ PHYSIQUE

PROTECTION DE VOTRE DOMICILE

De nombreuses mesures simples sont à prendre en compte pour vous protéger, vous et votre domicile. Commencez par l'installation ou l'amélioration de systèmes de sécurité autour de votre résidence ou de votre propriété. Sécurisez les portes et les fenêtres avec des serrures, des clés, des alarmes, des éclairages et évaluez la nécessité d'un système de vidéosurveillance (CCTV). Envisagez l'utilisation d'un système de verrouillage avancé pour les entrées et les fenêtres, ainsi que d'un système de vidéosurveillance contrôlé (capable de fournir plusieurs vues).

Entretenez les structures extérieures de votre propriété, comme les murs et les clôtures, et veillez à ce que les outils ou les échelles qui pourraient être utilisés pour accéder à votre domicile soient rangés en toute sécurité. Pensez à enlever tout ce qui pourrait être utilisé pour causer des dégâts, comme des briques détachées, de grosses pierres et des décorations de jardin. Veillez à ce que les arbustes, les mauvaises herbes, etc. soient taillés et entretenus de manière à ce que le feuillage :

- **ne puisse pas être utilisé** par des intrus pour se cacher ou accéder à la maison.
- **ne bloque pas** la vue de l'intérieur de la maison sur l'extérieur.

Sécurisez les portes et fenêtres extérieures à l'aide de dispositifs de verrouillage appropriés, notamment des mécanismes de verrouillage électroniques et codés. Il est conseillé de se procurer un jeu de clés ou des codes d'entrée supplémentaires qui pourront être utilisés en cas d'urgence. Envisagez de changer l'ensemble du système de verrouillage en cas de compromission des codes d'entrée ou de perte de clés.

Investissez dans un éclairage extérieur qui éclaire les portes extérieures, les aires de stationnement et les allées autour de la maison, et assurez-en l'entretien. Envisagez l'installation de caméras portant sur les portes et les fenêtres. Positionnez ces éclairages et caméras de manière stratégique afin d'éliminer tout angle mort où une personne pourrait échapper à la détection.

Si vous avez un véhicule et que vous ne pouvez pas le mettre à l'abri dans un garage ou dans un endroit fermé à clé, essayez de le laisser à la vue du public. Garez-le dans un endroit bien éclairé, dans le champ de vision d'une caméra de vidéosurveillance ou dans un parking pourvu de personnel. Fermez toujours les fenêtres, mettez vos objets de valeur hors de vue et verrouillez votre voiture, même si vous ne vous absentez que quelques minutes. Apprenez à utiliser le type de système d'alarme antivol installé dans votre véhicule. Certains systèmes comprennent des alertes sonores et visuelles, ainsi que des services de localisation du véhicule afin d'accélérer l'intervention de la police.

PLANIFIEZ À L'AVANCE

Envisagez de mettre au point un plan d'action d'urgence pour la famille et de vous exercer à faire ce qu'il faut faire en cas d'urgence. Si vous souhaitez obtenir de l'aide pour l'élaboration d'un plan, consultez le site :

fema.gov/blog/have-emergency-plan-your-family.

ATTAQUES À L'ARME À FEU

Par tireur actif, on entend un ou plusieurs individus qui s'emploient activement à tuer ou à tenter de tuer des personnes dans une zone peuplée.[3] Les événements impliquant des tireurs actifs sont souvent imprévisibles et évoluent rapidement. Dans le chaos, chacun peut jouer un rôle essentiel dans l'atténuation des conséquences d'un événement de tireur actif.

Les situations de tirs actifs se terminant souvent dans les 10 à 15 minutes, avant que les forces de l'ordre n'arrivent sur les lieux, il est indispensable de se préparer mentalement et physiquement à réagir à un tel événement.

En cas d'attaque par un tireur, envisagez de mettre en œuvre une stratégie de réaction pratique telle que le paradigme « Courir, Se cacher, Combattre », conformément aux politiques de sécurité de votre organisation. Des renseignements et des ressources supplémentaires sont disponibles sur la page d'accueil de la CISA : Active Shooter Preparedness.

LE FEU COMME ARME

L'incendie volontaire est défini comme le fait de brûler ou de tenter de brûler, volontairement ou malicieusement, avec ou sans intention de commettre une fraude, une maison d'habitation, un bâtiment public, un véhicule à moteur, un aéronef ou d'autres biens personnels.[4] Les motivations d'un pyromane peuvent comprendre, entre autres, la vengeance, le vandalisme, la fraude ou la dissimulation d'un crime. L'incendie peut être allumé à l'aide d'accélérateurs, de flammes ou d'un type d'engin incendiaire improvisé (EEI).

La menace d'utiliser le feu comme arme peut être difficile à détecter avant que l'attaque ne soit lancée. Vous devez comprendre les mesures à prendre si vous sentez une odeur de fumée ou si vous voyez un objet en feu.

3 Federal Bureau of Investigation, n.d. Ressources sur la sécurité en cas de fusillade. Consulté le 1er décembre 2023, fbi.gov/how-we-can-help-you/active-shooter-safety-resources.

4 Agence de cybersécurité et de sécurité des infrastructures (Cybersecurity and Infrastructure Security Agency). 2021. Fire as a Weapon Action Guide. Consulté le 8 août 2023. cisa.gov/resources-tools/resources/fire-weapon-action-guide.

En cas d'attaque par le feu, appelez le 9-1-1 et suivez les instructions du personnel de secours. Quittez immédiatement la zone de l'incendie et alertez les autres personnes, si possible. Évitez les endroits où vous pouvez sentir de la fumée ou voir du feu. Évacuez les lieux fermés ; fermez toutes les portes derrière vous pour endiguer l'incendie. Si vous ne pouvez pas évacuer, éloignez-vous le plus possible du danger et utilisez les extincteurs au besoin. Gardez une vue d'ensemble de la situation et surveillez les activités suspectes ou les nouvelles menaces qui pourraient survenir.

Consultez le guide d'action Fire as a Weapon Action Guide de la CISA pour d'autres conseils sur la manière de gérer les cas où le feu est utilisé comme une arme.

ENGINS EXPLOSIFS IMPROVISÉS (EEI)

Un engin explosif improvisé est un dispositif placé ou fabriqué de manière improvisée, qui comprend des produits chimiques destructeurs, létaux, nocifs, pyrotechniques ou incendiaires et qui est conçu pour détruire, neutraliser, harceler ou détourner l'attention.[5] En fonction des objectifs et des matériaux dont dispose le fabricant de bombes, les engins explosifs improvisés vont de petits dispositifs rudimentaires, tels que des dispositifs de surpression ou des bombes tuyaux le plus souvent remplis de poudres explosives, à de grands engins transportés par des véhicules et contenant de grandes quantités d'explosifs.

Les menaces peuvent prendre différentes formes. En cas d'inquiétude concernant une situation ou un objet suspect, appelez immédiatement les autorités locales de maintien de l'ordre. Des fils ou des composants électroniques inexplicables, d'autres éléments visibles ressemblant à une bombe, des sons, des vapeurs, des brouillards ou des odeurs inhabituels sont autant d'indices de la présence d'une bombe. Les incidents liés à des engins explosifs improvisés impliquant un dispositif suspect nécessitent l'intervention d'une équipe de démineurs et la capacité de diagnostiquer et de mettre hors d'état de nuire les engins viables.

Pour plus d'informations sur la reconnaissance des objets suspects, consultez la carte et l'affiche Unattended vs. Suspicious Item et regardez la vidéo « What to Do: Suspicious or Unattended Item ».

PROTESTATIONS ET MANIFESTATIONS

Quelle que soit la mission ou l'intention, restez calme si une protestation ou une manifestation publique a lieu près de votre domicile, de votre lieu de travail ou même sur votre propriété. Les manifestations peuvent paraître intimidantes, mais il est peu probable qu'elles aboutissent à une menace physique. Même si la situation se tend, restez calme. Restez à l'intérieur, fermez et verrouillez vos portes et fenêtres et tirez les rideaux/stores. Si vous vous sentez en danger ou si la situation s'aggrave, appelez les forces de l'ordre locales.

Au besoin, inscrivez la description des personnes et des véhicules présents. Remettez à la police les images de vidéosurveillance, les vidéos ou les photos prises avec votre téléphone portable, car elles peuvent s'avérer utiles dans le cadre d'une enquête.

La fiche d'information de la CISA sur la protection des infrastructures lors des manifestations publiques (Protecting Infrastructure During Public Demonstrations Fact Sheet) propose des recommandations en matière de sécurité aux entreprises susceptibles d'être la cible d'actes illégaux lors de manifestations publiques.

CONNAISSANCE DE LA SITUATION

La connaissance de la situation consiste à être conscient de ce qui se passe autour de soi, à tout prendre en compte et à adapter son comportement afin de réduire le risque de blessure pour soi, sa famille ou ses collègues de travail.

VISITEURS

Identifiez toujours vos visiteurs avant de les faire entrer chez vous. Envisagez d'installer un judas ou une caméra de porte pour vous aider à identifier qui se trouve de l'autre côté. Demandez aux visiteurs inconnus de s'identifier avant d'ouvrir la porte. Une fois à l'intérieur de votre domicile, gardez-les à proximité, de préférence devant vous ou à un endroit où ils peuvent être surveillés visuellement. Pensez à garder un téléphone portable sur vous en permanence.

DOCUMENTS SENSIBLES

Éliminez ou détruisez toujours correctement les documents confidentiels susceptibles de contenir des informations sensibles ou données à caractère personnel (DCP). Les données à caractère personnel comprennent toute information de nature personnelle susceptible d'être utilisée pour vous identifier.

SÉCURITÉ DES PIÉTONS

Donnez la priorité à votre sécurité personnelle quand vous vous déplacez, marchez ou faites du jogging dans les espaces publics. La prise de précautions appropriées peut vous aider à réduire vos vulnérabilités et le risque d'être victime de violence ou d'agression. Envisagez des mesures simples telles que planifier un itinéraire sûr à l'avance, varier votre itinéraire pour vous rendre à des endroits habituels et éviter les points de danger potentiels, comme les allées peu fréquentées ou mal éclairées, les parkings couverts peu fréquentés et les aires de stationnement éloignées.

5 Département de la sécurité intérieure des États-Unis. Federal Bureau of Investigation. n.d. *Security and Resiliency Guide: Counter-Improvised Explosive Device (C-IED) Concepts, Common Goals, and Available Assistance.* Consulté le 8 août 2023. P. 4. cisa.gov/resources-tools/resources/security-and-resiliency-guide-srg-and-annexes.

Du moment que vous êtes en public, faites preuve de discrétion et prenez des précautions pour cacher vos références professionnelles ou vos informations personnelles. Faites preuve de prudence quand vous portez des badges ou entrez des mots de passe dans des espaces publics. Pour plus de renseignements et de conseils, rendez-vous sur le site Internet de l'Administration nationale de la sécurité routière (National Highway Traffic Safety Administration) consacré à la sécurité des piétons.

GARDER LA CONNAISSANCE DE LA SITUATION

En cas d'inquiétude ou de sentiment d'insécurité dans un lieu public, rapprochez-vous d'un groupe de personnes. Si ce n'est pas possible, adaptez vos mouvements pour améliorer votre connaissance de la situation et **prenez les précautions suivantes :**

- **Gardez votre téléphone portable** à portée de main pour pouvoir passer un appel d'urgence.
- **Soyez vigilant** et restez conscient de votre position exacte et de votre environnement.
- **Évitez d'exhiber** des bijoux ou des objets de valeur.
- **Prenez en compte l'éclairage de la zone, l'emplacement et la proximité** d'autres entreprises locales.
- **Quand vous vous déplacez à pied, faites face à la circulation en sens inverse** afin d'éviter les véhicules qui arrivent par derrière.
- **Gardez les mains libres** et restez attentif à votre environnement.
- **Évitez de parler au téléphone**, de porter des écouteurs ou d'envoyer de longs messages.
- **Restez vigilant** quand vous marchez et évitez de vous attarder.
- **Quand vous utilisez un guichet automatique bancaire ,** évitez de montrer votre argent à la vue de tous..

SERVICES DE COVOITURAGE

En cas d'utilisation d'une application de covoiturage, pensez à informer un ami ou un collègue des détails de votre position et de votre destination. Vérifiez les détails concernant le conducteur et le véhicule avant d'accepter la course et de monter dans le véhicule.

RECONNAÎTRE ET SIGNALER TOUTE ACTIVITÉ SUSPECTE

Reconnaissez et signalez les activités suspectes, comme les personnes qui traînent sans raison précise autour de votre domicile, de votre lieu de travail ou de votre véhicule, ou les personnes qui essaient de vous prendre en photo de manière clandestine. Si vous remarquez que quelqu'un laisse tomber un objet ou un paquet près de votre domicile, de votre lieu de travail ou de votre véhicule, signalez-le immédiatement à la police. Pour en savoir plus sur le signalement d'activités suspectes, consultez la campagne « If You See Something, Say Something® » (Si vous voyez quelque chose, dites quelque chose).

DISPOSITIFS DE PROTECTION INDIVIDUELLE

Envisagez de vous munir d'un pulvérisateur de gaz poivre, d'une alarme sonore ou d'un autre dispositif de protection personnelle pour désorienter un agresseur, avertir les passants et vous créer une possibilité de fuite. Dans la mesure du possible, et dans le respect des lois et réglementations fédérales et locales, portez et utilisez des dispositifs de protection personnelle.

En prêtant attention aux signes d'alerte suivants et en les signalant rapidement, il est possible de réduire les risques d'incident :

- **Menace verbale ou écrite** contre vous, votre domicile, vos biens ou votre lieu de travail.
- **Endommagement ou altération** de systèmes ou d'équipements.
- **Objets suspects ou laissés sans surveillance**, notamment des sacs, des boîtes, des récipients cachés, susceptibles de contenir des substances dangereuses.
- **Questionnement suspect** sur des plans de bâtiments, l'emplacement des entrées/sorties, les ascenseurs, les extincteurs, les arrivées d'eau, ainsi que les systèmes de chauffage, de ventilation et de climatisation (CVC).
- **Quantités ou emplacements inhabituels de matériaux inflammables ou combustibles,** notamment d'accélérateurs, de peintures, de dégraissants, de nettoyants à base d'alcool, d'aérosols et de bouteilles de gaz propane.
- **Messages sur les réseaux sociaux** faisant la promotion d'images ou d'idées d'attentats.

Reportez-vous aux Indicateurs et exemples de signalement d'activités suspectes pour plus d'informations.

CONFRONTATIONS

Le fait de se retrouver dans une situation de confrontation peut être stressant. L'attention doit être concentrée sur les comportements observables susceptibles de constituer des indices de potentiel de violence. Dans ces situations, il est important de rester calme et d'évaluer la situation afin de déterminer si un engagement est possible en toute sécurité. Tenez compte des limites de vos propres capacités et demandez de l'aide au personnel de sécurité ou aux forces de l'ordre dès que vous pouvez le faire en toute sécurité.

Si vous disposez d'une formation et de compétences suffisantes, envisagez de désamorcer en toute sécurité les situations tendues au moyen d'actions ciblées qui incluent une écoute et une communication efficaces. Rappelez-vous que la « désescalade » n'est pas simplement quelque chose qui se fait, c'est l'objectif.

Consultez la série sur la désescalade de CISA pour des conseils sur la façon de rester vigilant et de faire face à des situations potentiellement hostiles.

VÉHICULES MOTORISÉS ET DÉPLACEMENTS

Avant de quitter votre domicile ou votre lieu de travail, regardez autour et notez les véhicules suspects qui pourraient être à l'affût ou rôder. Inspectez la zone autour du véhicule pour vérifier qu'il ne se trouve rien qui ne devrait pas être sur ou près de votre véhicule. Si une situation se produit, ces informations peuvent être utiles à la police.

Dans la mesure du possible, évitez de répéter les mêmes habitudes dans vos déplacements afin que les acteurs malveillants potentiels ne puissent pas prédire vos allées et venues. Changez vos itinéraires et variez autant que possible les heures de départ. Assurez-vous que toutes les portes et les coffres du véhicule restent verrouillés pendant votre déplacement. N'ouvrez les fenêtres que pour aérer. Conduisez prudemment et maintenez une distance de sécurité avec le véhicule devant vous. Assurez-vous également toujours que votre véhicule a suffisamment de carburant (ou, s'il est électrique, qu'il est suffisamment chargé) pour le trajet.

Si vous pensez être suivi, essayez de rester calme et maintenez votre véhicule en mouvement. Fermez toutes les fenêtres et assurez-vous que les portes sont verrouillées. Contactez immédiatement les forces de l'ordre. Si vous le pouvez, dirigez-vous vers le poste de police le plus proche, n'allez pas chez vous. Essayez de noter le numéro de la plaque d'immatriculation, la marque et le modèle de tout véhicule suspect.

Si vous êtes impliqué dans une collision avec un véhicule ou si vous êtes victime d'une panne mécanique, tenez compte de votre environnement et contactez immédiatement le personnel d'urgence et le service de remorquage de véhicules. Suivez les instructions des forces de l'ordre.

APPELS TÉLÉPHONIQUES ET MENACES ANONYMES[6]

Les appels téléphoniques et les menaces anonymes sont généralement destinés à susciter la peur, l'inquiétude et la détresse. Pensez à toujours faire ce qui suit :

- **Restez calme** et NE raccrochez PAS le téléphone.
- **Faites en sorte que l'appelant reste en ligne** le plus longtemps possible. Soyez poli et montrez de l'intérêt pour qu'il continue de parler. Il peut révéler des informations importantes susceptibles d'être utiles en cas d'enquête policière.
- Si possible, **faites signe ou faites passer une note** à d'autres personnes autour de vous pour qu'elles écoutent et aident à prévenir les autorités.
- **Notez** autant d'informations que possible, numéro de téléphone de l'appelant, formulation exacte de la menace, type de voix ou de comportement, etc.
- **Enregistrez l'appel,** dans la mesure où cela est possible et autorisé par la loi.

La loi fédérale interdit les appels téléphoniques menaçants ou abusifs. Si vous recevez des appels de ce type, contactez les forces de l'ordre locales. Vous pouvez également signaler la menace au FBI. Consultez le guide du FBI sur l'intimidation par la menace (Threat Intimidation Guide) pour des conseils.

La plupart des menaces à la bombe étant faites par téléphone, consultez la liste de contrôle des menaces à la bombe du DHS (DHS Bomb Threat Checklist) et le guide des menaces à la bombe de la CISA (CISA Bomb Threat Guide), qui fournissent des instructions sur la manière de répondre à une telle menace, ainsi qu'une liste complète d'informations qui aideront les forces de l'ordre à mener à bien une enquête sur une menace à la bombe.

SÉCURITÉ EN LIGNE

N'installez que des applications provenant d'« app stores » réputés afin d'éviter les téléchargements potentiellement dangereux. Ne téléchargez pas d'applications provenant de sources inconnues ou qui ne peuvent être vérifiées. Faites attention aux autorisations dont disposent les applications pour accéder à d'autres informations contenues dans votre téléphone.

Créez et conservez un mot de passe fort et unique pour chacun de vos appareils ou comptes et utilisez un gestionnaire de mots de passe pour les organiser. Activez l'authentification multifactorielle (MFA) pour chaque compte ou application qui la propose. L'activation de cette fonction permet de protéger les informations personnelles comme le courrier électronique, les données des réseaux sociaux, les données financières et d'autres informations importantes.

MISES À JOUR DES LOGICIELS

Maintenez les logiciels à jour afin que les pirates ne puissent pas exploiter des informations sensibles ou des vulnérabilités. De nombreux systèmes d'exploitation proposent des mises à jour automatiques. Si cette option est possible, activez les mises à jour automatiques dans les paramètres de sécurité des applications de l'appareil.

Dans votre navigateur Internet, recherchez les localisateurs de ressources uniformes (URL) qui commencent par « https », indiquant que les sites utilisent le chiffrement, plutôt que par « http ». Hyper Text Transfer Protocol Secure (HTTPS) est un protocole de communication Internet utilisé pour chiffrer et transmettre en toute sécurité des informations entre le navigateur Internet d'un utilisateur et le site Internet auquel il est connecté. Il est conçu pour mieux protéger l'intégrité et la confidentialité des informations des utilisateurs quand ils se rendent sur des sites Internet.[7]

Consultez le site Sécuriser notre monde de la CISA (Secure Our World) pour en savoir plus sur la sécurité en ligne.

6 Federal Bureau of Investigation. n.d. Threat Intimidation Guide. Consulté le 8 août 2023. fbi.gov/file-repository/threat-intimidation-guide-english-022322.pdf/view.

7 Département de la sécurité intérieure des États-Unis. 2018. Hyper Text Transfer Protocol Secure (HTTPS). Consulté le 12 février 2024. cisa.gov/resources-tools/resources/hyper-text-transfer- protocol-secure-https.

UTILISATION D'APPAREILS ÉLECTRONIQUES

Les appareils portables et les réseaux peuvent contenir diverses données personnelles, comme des informations bancaires en ligne, des e-mails, des textos, des contacts, des contenus de réseaux sociaux et des photos. Pour assurer la sécurité de vos appareils, utilisez toutes les fonctions de sécurité et veillez à toujours mettre à jour les logiciels de vos appareils. Créez des codes d'accès robustes pour votre téléphone et vos cartes SIM et désactivez les services inutiles de géolocalisation.[8]

Changez toujours votre code secret par défaut pour l'accès à la messagerie vocale. Envisagez de limiter les services de localisation sur votre téléphone et de revoir les paramètres de confidentialité afin d'empêcher que des tiers ne suivent vos déplacements et n'identifient votre adresse personnelle ou votre lieu de travail par le biais d'applications tierces. Vérifiez les dispositifs de protection de la vie privée et de la sécurité d'Apple et d'Android afin d'améliorer la sécurité de votre ou de vos appareils.

RÉSEAUX SOCIAUX

L'Internet peut être une source précieuse d'information, d'éducation et de divertissement. Il convient cependant de rester vigilant et de prendre des précautions afin de limiter la quantité d'informations personnelles que vous publiez en ligne, en particulier sur les réseaux sociaux.

Les sites de réseaux sociaux populaires permettent de créer un profil personnel et d'interagir avec d'autres personnes en ligne. Sur les sites de réseaux professionnels, les personnes peuvent ajouter plus de détails à leur profil et inclure leurs expériences professionnelles et d'autres informations sur leur parcours. Bien que ces outils permettent de communiquer avec d'autres personnes et de faire connaître son parcours professionnel, la publication d'informations personnelles en ligne présente des risques potentiels.

Faites preuve de prudence avant de publier des informations personnelles. Les acteurs malveillants peuvent utiliser les données de localisation des photos, les anniversaires, les noms et prénoms, les adresses personnelles et les adresses électroniques dans le cadre d'un piratage ou d'une usurpation d'identité. Par ailleurs, les informations concernant l'emploi, les membres de la famille, les loisirs ou les détails des véhicules sont précieuses pour les criminels et les parties hostiles. Votre famille et vos amis peuvent également partager involontairement des renseignements vous concernant s'ils ne prennent pas les mesures appropriées pour protéger les informations de leurs propres profils. N'oubliez pas que l'Internet ne comporte pas de bouton « supprimer ». Partagez avec prudence, car même si vous supprimez un message ou une photo de votre profil, il y a de fortes chances que quelqu'un l'ait quand même vu.

Certains sites de réseaux sociaux sont propriétaires des données que vous publiez et les vendent à des tiers. Vérifiez régulièrement vos paramètres de confidentialité et de localisation sur ces sites, sinon vous risquez qu'une partie ou la totalité de votre profil personnel soit visible par un large public, sans que vous le sachiez.[9, 10]

8 Federal Communications Commission. 2019. Protect Your Smart Device. Consulté le 20 septembre 2023. fcc.gov/consumers/guides/protect-your-mobile-device.

9 Gouvernement du Royaume-Uni. National Cyber Security Centre. 2019. Social Media: how to use it safely. Consulté le 20 septembre 2023. ncsc.gov.uk/guidance/social- media-how-to-use-it-safely.

10 Agence de cybersécurité et de sécurité des infrastructures (Cybersecurity and Infrastructure Security Agency), National Cyber Alliance. 2019. Social Media Cybersecurity. Consulté le 20 septembre 2023. cisa.gov/sites/default/files/ publications/NCSAM_SocialMediaCybersecurity_2020.pdf.

VÉRIFIER LES PARAMÈTRES DE CONFIDENTIALITÉ ET DE LOCALISATION DES RÉSEAUX SOCIAUX

X, anciennement Twitter

- twitter.com/settings/privacy_and_safety
- twitter.com/settings/location_information

Instagram

- help.instagram.com/811572406418223
- **IOS :** help.instagram.com/171821142968851
- **Android :** Sur votre appareil Android, allez dans Réglages > Applis > Instagram > Permissions > Localisation

Facebook

- facebook.com/help/325807937506242/
- facebook.com/help/337244676357509

Snapchat

- help.snapchat.com/hc/en-gb/sections/5690164367636-Privacy-Settings
- help.snapchat.com/hc/en-us/articles/7012322854932-How-do-I-turn-on-Ghost-Mode

TikTok

- tiktok.com/safety/en/privacy-and-security-on-tiktok/
- support.tiktok.com/en/account-and-privacy/account-privacy-settings/location-services-on-tiktok

DOXING (DIVULGATION DE DONNÉES PERSONNELLES)

Le « doxing » est une pratique qui consiste à recueillir des données à caractère personnel (PII) d'une personne ou des informations sensibles d'une organisation à partir de sources ouvertes ou de documents compromis et à les diffuser publiquement ou à les utiliser à des fins malveillantes.[11, 12] Les criminels peuvent utiliser ces informations à des fins de chantage ou pour susciter la peur chez des cibles potentielles.

Lorsque vous publiez en ligne, il est important d'être conscient de ce que vous publiez et de la manière dont vous le faites. Vous pourriez mettre votre sécurité personnelle en danger si vous publiez trop d'informations sans appliquer les paramètres de confidentialité appropriés. Ces informations peuvent être utilisées pour dresser un tableau de vos relations, de vos opinions, de vos centres d'intérêt et d'autres sujets qui pourront être exploités à l'avenir.

Des courtiers en données peuvent également recueillir ces informations personnelles et les vendre à d'autres sociétés. Pour éviter que vos données ne parviennent à des courtiers :

- **Évitez** de partager des informations confidentielles.
- **N'acceptez pas** sur les réseaux sociaux des personnes que vous ne connaissez pas dans la vie réelle.
- **Assurez-vous** que les applications que vous utilisez sont chiffrées de bout en bout.
- **Limitez** les autorisations des applications.
- **Créez** des alertes Google pour votre nom.
- **Envisagez de prendre le temps** de vous désinscrire des principaux courtiers en données et sites de recherche de personnes ou de vous abonner à un service qui s'en chargera pour vous.

Des informations géolocalisées peuvent être publiées sur les réseaux sociaux, notamment à partir de téléphones portables et d'appareils mobiles équipés d'un GPS. Ces informations ne sont pas sécurisées et peuvent être consultées par n'importe qui, notamment par des personnes qui peuvent vous vouloir du mal. Gardez la trace de ce que vous publiez et publiez de manière responsable afin de vous assurer que personne n'est mis en danger par les informations que vous rendez publiques.

Si vous pensez que vous faites l'objet d'un « doxing » :

- **Signalez l'incident** aux forces de l'ordre locales et à toute plateforme en ligne où vos informations personnelles ont pu être divulguées.
- **Documentez** ce qui s'est passé et prenez des captures d'écran pour les communiquer aux enquêteurs.
- **Déterminez** quelles informations ont été exploitées, la gravité de la menace et le point de compromission.
- **Collaborez avec les administrateurs** de sites Internet pour retirer des informations des sites ou des applications.
- **Configurez les paramètres de confidentialité** sur les options les plus strictes.
- **Soyez à l'affût des signes** d'usurpation d'identité, surveillez vos comptes financiers, mettez en place des alertes à la fraude et changez les informations de connexion et de mot de passe de tous vos comptes en ligne.

Les lois contre la divulgation de données personnelles varient d'une juridiction à l'autre, il est donc important de les consulter dans votre région pour envisager des options d'atténuation et de prévention. En cas d'inquiétude pour la sécurité physique, contacter les forces de l'ordre locales pour savoir ce qu'il convient de faire.

RECONNAÎTRE ET SIGNALER LE PHISHING (HAMEÇONNAGE)

Les criminels utilisent souvent des tactiques d'hameçonnage pour vous inciter à ouvrir des liens, des e-mails ou des pièces jointes dangereux susceptibles de vous demander des informations personnelles ou d'infecter vos appareils. Ces messages sont souvent conçus pour donner l'impression qu'ils proviennent d'une personne ou d'un organisme de confiance.

Les messages de phishing peuvent prendre la forme d'un e-mail, d'un texte, d'un message direct sur les réseaux sociaux ou d'un appel téléphonique. Méfiez-vous des propos urgents ou émotionnels, des demandes d'envoi d'informations personnelles, des URL raccourcis non fiables et des adresses électroniques et liens incorrects.

Si vous pensez être la cible d'une tentative d'hameçonnage, ne cliquez pas sur les liens ni sur les pièces jointes. En revanche, signalez le message, puis supprimez-le.

11 Département de la sécurité intérieure des États-Unis. 2024. Office of Partnership and Engagement. Resources for Individuals on the Threat of Doxing. Consulté le 09 février 2024. dhs.gov/ publication/resources-individuals-threat-doxing.

12 Conseil européen pour la recherche nucléaire. 2017. Computer Security: Enter the next level: Doxware. Consulté le 12 décembre 2023. home.cern/news/news/computing/computer-security-enter-next-level-doxware.

RESSOURCES

SÉCURITÉ PHYSIQUE

- CISA Security and Resiliency Guide
- CISA Active Shooter Preparedness
- FBI Threat Intimidation Guide
- CISA Bomb Threats
- CISA De-escalation Series

CONNAISSANCE DE LA SITUATION

- Centre de prévention, de sensibilisation et de ressources contre le harcèlement (Stalking Prevention, Awareness, & Resource Center) (SPARC)

SÉCURITÉ EN LIGNE

- CISA Secure Our World
- CISA Privacy and Mobile Device Apps
- CISA Insights: Mitigating the Impacts of Doxing on Critical Infrastructure
- CISA Social Media Cybersecurity