PLANIFICATION DE LA SÉCURITÉ TECHNOLOGIQUE

LISTE DE CONTRÔLE

La planification de la sécurité technologique doit toujours être jumelée avec une planification de sécurité plus traditionnelle. La violence en ligne et hors ligne sont interconnectées et il importe de s'intéresser aux risques n'étant pas liés à la technologie qui peuvent être pris en compte dans la planification de la sécurité technologique. Les partenaires violents utilisent souvent la technologie dans le cadre d'un schéma de violence plus étendu. Cette liste de contrôle pour la planification de la sécurité technologique se veut un complément à un plan de sécurité en bonne et due forme, de même qu'une ressource pour le personnel de soutien, plutôt qu'une liste de contrôle indépendante.

Lorsque vous planifiez la sécurité d'une femme ou d'un jeune exposé à la violence facilitée par la technologie, il faut savoir que l'agresseur peut avoir accès à leurs appareils ou leurs comptes, et qu'il peut s'en servir pour surveiller les communications et les déplacements. Le fait de modifier un appareil, un compte de médias sociaux, un courriel ou toute autre technologie peut alerter l'agresseur que votre cliente est en voie d'obtenir de l'aide et déclencher des violences supplémentaires. Il peut être nécessaire de redoubler de précautions dans ce genre de situation.

Dans certains cas, vous aurez besoin de l'aide de spécialistes en informatique ou des forces de l'ordre, par exemple pour détecter des logiciels espions ou qui facilitent le harcèlement.

Mots de passe

- ☐ Dressez une liste de tous les appareils (ordinateur portable, cellulaire, Fitbit, système de sécurité domestique, voiture intelligente, appareils connectés, Siri/Alexa, systèmes de sonorisation Bluetooth, etc.) et comptes (médias sociaux, courrier électronique, achats en ligne, services de restauration en ligne, applications de transport, comptes dans le cloud, trackers de fitness, jeux, etc.) Voir l'annexe A pour la liste des comptes potentiels.
- ☐ Notez ceux auxquels l'agresseur a accès, dont il connaît ou pourrait connaître les mots de passe.
- ☐ Réfléchissez aux informations qui figurent sur ces comptes (adresse personnelle, numéro de téléphone, adresse du domicile, informations sur les cartes de crédit, messages personnels, historique des recherches sur Internet, communication sur la planification de la sécurité, etc.).

- ☐ Remplacez tous les mots de passe par des phrases de passe uniques que l'agresseur ne pourra pas deviner. Évitez d'utiliser des éléments tels que les noms d'enfants ou d'animaux, les dates importantes, les anciennes adresses ou les anciens numéros de téléphone.
  Une phrase de passe est une phrase facile à retenir mais difficile à deviner. L'ajout de symboles de chiffres pour les lettres peut rendre la devinette encore plus difficile. Par exemple: M0TdeP@$$eD1FF1C1LE@dev1n8
- ☐ N'utilisez pas le même mot de passe pour plusieurs comptes.
- ☐ Utilisez une phrase de passe unique pour chaque compte ou un gestionnaire de mots de passe.
- ☐ Changez le mot de passe du réseau Wi-Fi de votre domicile.
- ☐ Pour les questions de sécurité sur les comptes, inventez de fausses réponses ou n'utilisez pas de questions que l'agresseur pourrait deviner (par exemple, au lieu d'utiliser le nom de jeune fille de votre mère, inventez une réponse lorsqu'on vous pose la question, mais souvenez-vous de votre fausse réponse).
- ☐ Désactivez tous les mots de passe enregistrés automatiquement sur tous les appareils et comptes.
- ☐ Déconnectez-vous de tous les comptes et appareils lorsque vous ne les utilisez pas.
- ☐ Utilisez l'authentification à deux facteurs sur toute application ou compte qui le permet. L'authentification à deux facteurs vous oblige à saisir un mot de passe qui est envoyé à votre téléphone ou à votre courrier électronique pour confirmer que c'est bien vous qui accédez au compte.
  Pour des informations générales sur l'authentification à deux facteurs, voir HackBlossom: https://hackblossom.org/domestic-violence/defense/two-step-verification.html
- ☐ Consultez ce site Web pour savoir quelles applications courantes utilisent l'authentification à deux facteurs : https://twofactorauth.org/#communication
- ☐ Imprimez ou notez plusieurs codes d'authentification à deux facteurs à usage unique en cas de perte de votre téléphone. Rangez-les dans un endroit où l'agresseur ne les trouvera pas.
- ☐ N'utilisez pas de comptes de médias sociaux pour vous connecter à d'autres comptes (c'est-à-dire les options «Se connecter avec Facebook» ou «Se connecter avec Google»).
- ☐ Supprimez les courriels ou les appareils de l'agresseur des comptes partagés et des «appareils de confiance» sur vos comptes.

Blocage, suppression et élimination d'amis

- ☐ Envisagez de bloquer l'agresseur sur les médias sociaux et de retirer son contact de votre adresse électronique et de votre téléphone cellulaire. Assurez-vous d'avoir recueilli toutes les preuves nécessaires auprès de ces comptes avant de procéder à cette opération. Certains programmes suppriment ou ne vous permettent pas d'accéder aux conversations avec l'individu retiré de la liste d'amis ou bloqué, ni aux informations relatives à son compte.
- ☐ Lorsque vous décidez de bloquer, de supprimer ou de désactiver une personne, demandez-vous si cela ne risque pas d'aggraver la situation. Il peut y avoir des avantages à prendre en compte quant à l'accès aux médias sociaux de l'agresseur (comme savoir où il se trouve).
- ☐ Réfléchissez aux amis et aux membres de votre famille qui pourraient avoir votre agresseur sur leurs comptes. Demandez-leur de ne pas publier d'informations ou de photos vous concernant et de s'assurer qu'elles seront hors de portée de l'agresseur.

Harcèlement, suivi et surveillance

- ☐ Utilisez un cache-caméra sur tous vos appareils lorsque vous ne les utilisez pas.
- ☐ Si l'agresseur suit votre appareil ou vos comptes, envisagez d'utiliser un autre appareil (par exemple, un ordinateur au travail ou dans une bibliothèque) pour rechercher des informations et commencer à planifier la manière de modifier vos appareils ou vos comptes.
- ☐ Réfléchissez aux informations personnelles publiées en ligne (adresse du domicile sur une invitation à un anniversaire, numéro de téléphone sur une publication Facebook ou annonce d'un nouveau lieu de travail sur LinkedIn) et supprimez ces informations ou rendez-les privées. N'oubliez pas que d'autres personnes pourraient partager ces informations avec votre agresseur, même si vous l'avez bloqué de vos comptes.
- ☐ Désactivez ou limitez les fonctions de localisation de vos appareils si possible.
- ☐ Désactivez les fonctions de localisation telles que «Trouver mon téléphone» ou «Trouver mes amis».
- ☐ Supprimez l'historique des lieux visités, en particulier avant et à l'arrivée en maison d'hébergement ou tout autre espace sécuritaire.
- ☐ N'optez pas pour divulguer votre localisation sur les médias sociaux.
- ☐ Modifiez les paramètres de confidentialité des applications et des médias sociaux pour qu'ils soient le plus privés possible.
- ☐ Ne publiez pas sur les médias sociaux de photos contenant des métadonnées ou des informations de fond.
- ☐ Une façon de supprimer les métadonnées de localisation d'une photo est de publier une capture d'écran plutôt que la photo originale qui contient les métadonnées.
- ☐ Retirez les courriels ou les appareils de l'agresseur des comptes partagés et retirez son appareil des «Appareils de confiance» sur tous vos comptes. Voir l'annexe A pour les comptes potentiels.
- ☐ Vérifiez la fonction «Activité du compte» pour voir si des adresses IP inhabituelles accèdent au compte.
- ☐ Si vous craignez que l'agresseur ait accès à vos comptes, envisagez d'utiliser une boîte postale pour les comptes et livraisons en ligne. Considérez le risque que l'agresseur accède aux informations de votre carte de crédit ou utilise le compte à mauvais escient.
- ☐ Débranchez votre téléphone ou d'autres appareils de ceux de l'agresseur (stéréo Bluetooth dans sa voiture ou à la maison, notifications de fitness sur sa smartwatch, etc.)
- ☐ Fouillez les effets personnels (sacs à main, voitures, vestes) à la recherche de dispositifs de repérage GPS ou d'autres dispositifs d'enregistrement.

- ☐ Examinez tous les cadeaux ou les objets inhabituels de la maison, y compris les articles pour enfants, à la recherche de caméras cachées ou de dispositifs d'enregistrement.
- ☐ Réfléchissez aux informations qui se trouvent sur les appareils et les comptes de vos enfants (téléphones, systèmes de jeux vidéo, comptes de médias sociaux) et à celles qui pourraient être partagées avec l'agresseur.
- ☐ Demandez-vous si l'agresseur peut avoir accès aux informations du système de sécurité de la maison, comme l'accès aux caméras ou des informations sur les personnes qui vous rendent visite.
- ☐ Envisagez d'utiliser un dispositif ou un programme (par exemple, des scanners de réseau, des scanners de port, des détecteurs de signaux de FR) capable de détecter certaines caméras cachées et de scanner votre Wi-Fi ou celui de votre lieu de résidence.
- ☐ Regardez les applications sur le téléphone et supprimez celles qui ne vous sont pas familières.
- ☐ Si vous craignez que votre agresseur ait installé un logiciel espion sur vos appareils, vous pouvez demander à un spécialiste des TI ou aux forces de l'ordre de vérifier que l'appareil n'en contient pas. N'oubliez pas que si un logiciel espion est installé sur l'appareil, l'agresseur peut voir tout ce qui est fait sur l'appareil, ce qui peut intensifier la violence.
- ☐ La Clinic To End Tech Abuse propose également des ressources pour aider à identifier les logiciels espions sur un appareil : https://www.ceta.tech.cornell.edu/resources

  Signes qu'un appareil peut contenir un logiciel espion:
  - Le dispositif fonctionne lentement
  - La batterie se décharge
  - Les données sont épuisées
  - L'appareil chauffe
  - Dispositif s'allumant lorsqu'il n'est pas utilisé
  - Clics ou sons bizarres lors des appels
  - Prend beaucoup de temps pour s'éteindre.
- ☐ Maintenez les systèmes d'exploitation de vos appareils à jour. Ces mises à jour corrigent souvent les éventuelles lacunes en matière de sécurité du logiciel que les pirates utilisent à mauvais escient et les logiciels espions. Vérifiez vos paramètres de confidentialité après une mise à jour pour vous assurer qu'ils n'ont pas été modifiés.
- ☐ Envisagez de remplacer entièrement les appareils. Si vous décidez de le faire, vous ne devez pas vous servir d'appareils précédents pour l'installation car cela peut transférer un logiciel espion sur le nouvel appareil.
- ☐ Recherchez le matériel inhabituel fixé aux ordinateurs de bureau. Les enregistreurs de frappe sont souvent fixés entre le clavier et le bureau.

- ☐ Il convient de noter que les pirates et les ingénieurs informatiques expérimentés peuvent accéder à la localisation d'un appareil, même si celle-ci est désactivée dans les paramètres. Si votre agresseur a une formation en TI, cela peut poser des problèmes de sécurité numérique supplémentaires.

Comptes alternatifs

- ☐ Si l'agresseur a accès à vos comptes et qu'il n'existe aucun moyen sûr de l'en empêcher pour le moment (par exemple, s'il vous oblige à partager vos mots de passe en vous menaçant de vous faire du mal), créez un compte de messagerie ou de médias sociaux alternatif auquel l'agresseur n'a pas accès pour les communications de nature délicate.
- ☐ Ne vous connectez pas à ce compte sur vos appareils personnels ou partagés. Utilisez un ordinateur au travail, dans une bibliothèque ou chez une amie.

Stockage en nuage, comptes partagés, accès non autorisé

- ☐ Retirez l'agresseur de tout compte, appareil ou plan partagé.
- ☐ Supprimez les connexions Bluetooth des appareils de l'agresseur (c'est-à-dire ceux qui sont connectés à sa chaîne stéréo, à sa voiture intelligente, etc.)
- ☐ Réfléchissez au contenu automatiquement téléchargé ou connecté (c'est-à-dire les calendriers, le stockage iCloud pour les photos et les textes, Fitbit, les montres intelligentes) et si l'agresseur pourrait avoir accès à ces comptes ou informations.
- ☐ Supprimez tous les appareils, sauf les vôtres, de la liste des «Appareils de confiance» sur tous les comptes.
- ☐ Vérifiez la «Dernière activité du compte» sur tous les comptes pour voir si une adresse IP ou un appareil inhabituel a accédé au compte.

Historique de recherche

- ☐ Si l'agresseur a accès à un appareil ou un compte, il peut vérifier votre historique de recherche.
- ☐ Si vous cherchez de l'aide ou des ressources, utilisez un ordinateur situé hors du domicile.
- ☐ Supprimez sélectivement l'historique des recherches sur Internet.
- ☐ Utilisez les options «privé» ou «incognito» pour que l'historique des recherches ne soit pas enregistré.
- ☐ Désactivez les cookies dans les paramètres du navigateur.

Images intimes (pornographie de vengeance)

- ☐ Faites une liste des images et des vidéos qui peuvent exister.
- ☐ Envisagez d'utiliser le programme de Facebook qui empêche d'autres personnes de télécharger des images sexuelles qui ont été enregistrées et «hashée» auprès de l'entreprise. Cependant, vous devrez envoyer ces photos à Facebook afin que les images soient reconnues et supprimées de Facebook et Instagram.
- ☐ Si vous pouvez le faire sans risquer de violence, demandez à l'ex-partenaire de supprimer les images après la fin de la relation et dites-lui qu'il n'a pas votre consentement pour les partager. Documentez cette communication.
- ☐ Examinez si l'agresseur a pu capturer des images sans consentement (par exemple, caméra cachée, capture d'écran via Zoom ou Skype).
- ☐ Faites une recherche inversée d'images sur Google.
- ☐ Cherchez votre nom sur des sites pornographiques courants. Les gens sont souvent victimes de doxing et de dénonciation lorsque leurs images sont partagées.
- ☐ Créez une alerte Google pour votre nom. Cela peut alerter une personne lorsque son nom est mentionné en ligne s'il est affiché avec ses images.
- ☐ Envisagez d'alerter la famille, les proches et les collègues de travail susceptibles de recevoir les images afin de réduire les risques.
- ☐ Si l'image a été partagée sans consentement, consultez le guide de l'initiative pour les droits civiques sur Internet pour faire retirer du contenu https://www.cybercivilrights.org/online-removal/
- ☐ Faites rapport aux médias sociaux ou aux entreprises pornographiques, la plupart ont des politiques qui interdisent les images de nudité partagées sans consentement.
- ☐ Si vous partagez des images intimes, envisagez des stratégies de réduction des risques:
- ☐ Évitez de montrer votre visage ou des marques d'identification (tatouages, taches de naissance)
- ☐ Évitez les images dans des lieux identifiables (la pièce est-elle reconnaissable?)
- ☐ Utilisez des programmes comme Signal qui permettent de faire disparaître les messages
- ☐ Si des images ont été publiées, envisagez de faire appel à un service qui peut vous de réputation aider à faire retirer le contenu.

Alertes Google

- ☐ Créez une alerte Google afin d'être averti lorsque votre nom apparaît en ligne. Cela ne permettra pas de trouver toutes les occurrences où votre nom est affiché, mais peut parfois vous alerter.
- ☐ Créez une alerte Google pour toutes les versions de votre nom (par exemple, «Victoria Chan, Vickie Chan, Vicky Chan»)

Signaler les contenus préjudiciables aux entreprises de médias sociaux

- ☐ Rassemblez des preuves (captures d'écran) du contenu préjudiciable avant de le signaler, car il peut être supprimé par l'entreprise de médias sociaux s'il enfreint ses politiques.
- ☐ Consultez les «Media Safety Guides» de HeartMob pour obtenir des conseils sur les politiques et les mécanismes de signalement des entreprises de médias sociaux : https://iheartmob.org/resources/safety_guides

Mises à jour des logiciels, pare-feu et anti-virus

- ☐ Mettez régulièrement à jour vos logiciels. Cela inclut vos interfaces de téléphones portables. Ces mises à jour corrigent souvent les éventuelles lacunes de sécurité du logiciel que les pirates peuvent utiliser à mauvais escient.
- ☐ Activez les pares-feux et les logiciels anti-virus sur tous les appareils.

Collecte des preuves

- ☐ Créez un journal de toutes les expériences de violence facilitée par la technologie, en y incluant des informations telles que l'heure, la date, l'identité de l'agresseur, les preuves recueillies et d'autres informations utiles. Voir l'exemple de journal de violence facilité par la technologie de la BCSTH ici: https://bcsth.ca/techsafetytoolkit/sample-technology-facilitated-violence-log/
- ☐ Faites des captures d'écran ou des enregistrements qui démontrent la violence.
- ☐ Vérifiez si l'application alerte l'autre personne si quelqu'un fait une capture d'écran. Si c'est le cas, il n'est peut-être pas sécuritaire de faire une capture d'écran et il vaut peut-être mieux prendre une photo ou une vidéo avec un deuxième appareil.
- ☐ Veillez à inclure dans les preuves le profil et les autres informations permettant d'identifier l'agresseur.
- ☐ Assurez-vous que la date de figure aux cotés des actes violents.
- ☐ Si la violence se produit par courriel, conservez le courriel original car il contient des métadonnées telles que l'adresse IP de l'expéditeur.

- ☐ Si les actes violents ont été publiés par quelqu'un d'autre, capturez-les avant que l'agresseur puisse les supprimer.
- ☐ Conservez des copies des preuves dans un endroit sûr. Sauvegardez les informations dans deux endroits ou plus.
- ☐ Si l'agresseur a accès à l'appareil ou au stockage en nuage où sont entreposées les preuves, il peut les supprimer.
- ☐ Conservez à la fois des copies imprimées et des copies électroniques des preuves.

Entrez en contact avec une intervenante antiviolence ou une avocate pour obtenir du soutien

Si vous souhaitez obtenir plus d'informations sur la manière d'intégrer la technologie dans un plan de sécurité, consultez les ressources de sécurité technologique de la BC Society of transition Houses ou tout spécialiste juridique dans votre communauté.

- VictimLink BC
- KUU-US Crisis Line Society
- Aide juridique de la Colombie-Britannique
- Rise Women's Legal Centre
- hebergementfemmes.ca
- BCSTH planification de la sécurité technologique et A Guide for Canadian Women Experiencing Technology-Facilitated Violence: Strategies for Enhancing Safety

Spark Teen Digital Dating Violence Project

Nous remercions Suzie Dunn, doctorante à l'Université d'Ottawa, pour la création de cette fiche d'information.

Ce document a été publié en mars 2021.

ANNEXE A:

Appareils et comptes à considérer

Comptes de médias sociaux

- ☐ Facebook
- ☐ Twitter
- ☐ Instagram
- ☐ Snapchat
- ☐ TikTok
- ☐ Pinterest
- ☐ WeChat
- ☐ YouTube
- ☐ Tumblr
- ☐ Reddit
- ☐ LinkedIn

Communication

- ☐ Téléphone intelligent
- ☐ Ordinateur
- ☐ Gmail
- ☐ Courriel personnel et professionnel
- ☐ Messenger
- ☐ WhatsApp
- ☐ Signal
- ☐ Slack
- ☐ QQ
- ☐ Viber
- ☐ Telegram
- ☐ Messages instantanés, DM ou privés sur les plateformes en ligne

Vidéo conférence

- ☐ Zoom
- ☐ MS Teams
- ☐ Skype
- ☐ FaceTime
- ☐ Appels vidéo sur des plateformes en ligne

Stockage en nuage

- ☐ iCloud
- ☐ Dropbox
- ☐ Google Drive
- ☐ Amazon Drive

Appli garde et animaux domestiques

- ☐ Calendriers partagés
- ☐ Appli de suivi des enfants
- ☐ Écoute-bébé
- ☐ Partage de photos
- ☐ Applis de planification
- ☐ Caméra pour animaux
- ☐ Traceur d'animaux (par exemple, dispositif GPS dans le collier)

Factures et services publics

- ☐ Plans de téléphone
- ☐ Électricité
- ☐ Gaz
- ☐ Internet/Câble

Services de livraison de nourriture

- ☐ SkipTheDishes
- ☐ Uber Eats
- ☐ DoorDash
- ☐ Foodora
- ☐ Autres comptes de restaurants

Finances

- ☐ Comptes bancaires (y compris les cartes de crédit)
- ☐ Comptes d'investissement (actions, investissements, retraite, éducation, etc.)
- ☐ PayPal
- ☐ Portefeuille Apple
- ☐ Portefeuille Bitcoin
- ☐ OXF

Comptes publics

- ☐ Agence du revenu du Canada
- ☐ Applications de prise de rendez-vous
- ☐ Compte de prêt étudiant
- ☐ Mon compte
- ☐ Compte de services de la province

Applis de transport

- ☐ Uber
- ☐ Lyft
- ☐ Applis pour les taxis
- ☐ Waze
- ☐ Google maps
- ☐ Applis de transport public

Applis de magasinage

- ☐ Amazon
- ☐ Carte de points d'épicerie
- ☐ PC Optimum
- ☐ Carte de points pour le café
- ☐ Applis immobilières
- ☐ Applis de compte/récompense dans les magasins où vous faites vos achats ou en ligne

Divertissement

- ☐ Spotify
- ☐ Netflix
- ☐ Crave
- ☐ Disney+
- ☐ Amazon Prime Video
- ☐ Apple Music et TV
- ☐ iTunes
- ☐ Applis de podcast
- ☐ Audible
- ☐ PornHub

Jeux vidéo

- ☐ Discord
- ☐ Twitch
- ☐ Switch
- ☐ Steam
- ☐ Xbox Live
- ☐ Réseau PlayStation
- ☐ Origin
- ☐ Jeux pour téléphones intelligents

Santé et fitness

- ☐ Fitbit
- ☐ Apple Watch
- ☐ Suivi de la distance (par exemple, Strava, MapMyRun)
- ☐ Dispositifs GPS (par exemple, Garmin, applis de randonnée)
- ☐ Applis relatives aux règles ou à la fertilité
- ☐ Compteurs de régimes ou de calories
- ☐ Applis de suivi médical
- ☐ Applis thérapeutiques

Voyage

- ☐ Cartes de points de voyage (p. ex. Aeroplan, Air Miles)
- ☐ Airbnb
- ☐ Expedia
- ☐ TripAdvisor
- ☐ AubergeInternationale
- ☐ Compagnies aériennes
- ☐ Trains

Appareils de maison intelligente

- ☐ Amazon Echo
- ☐ Google Nest
- ☐ Alexa
- ☐ Siri
- ☐ Sonos One
- ☐ The Ring
- ☐ Systèmes de sécurité domestique
- ☐ Thermostat intelligent
- ☐ Éclairage intelligent
- ☐ Serrure intelligente

Appareils portables intelligents

- ☐ Voiture intelligente
- ☐ GPS, voiture
- ☐ Bluetooth, voiture
- ☐ Appli de suivi pour vélo
- ☐ Tile
- ☐ Trouver mon téléphone

Comptes d'éducation et d'apprentissage

- ☐ Courriel de l'école
- ☐ Plate-forme d'affectation en ligne de l'école
- ☐ Carte de bibliothèque
- ☐ Applis linguistiques