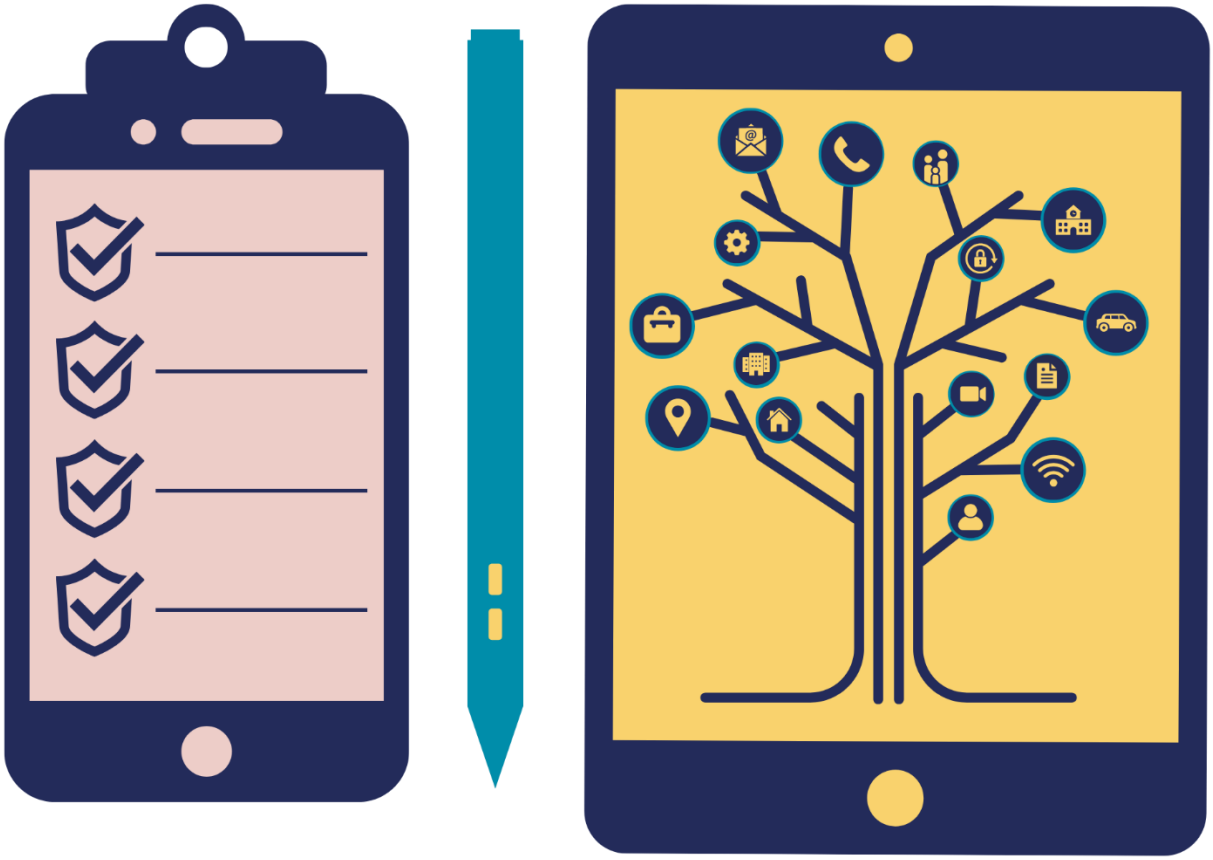
Liste de contrôle pour la planification de sécurité technologique



La planification de sécurité technologique doit toujours être effectuée en tandem avec la planification de sécurité plus conventionnelle. La violence en ligne et hors ligne sont interconnectées et la planification doit aussi tenir compte des risques qui ne sont pas directement associés à la technologie. La

présente liste de contrôle se veut le complément d'un plan de sécurité en bonne et due forme, et non une liste indépendante.

Lorsque vous établissez un plan de sécurité avec une personne qui a vécu la VFGFT, il ne faut pas oublier que l'auteur peut avoir accès à ses appareils ou à ses comptes et qu'il surveille peut-être ses communications et ses déplacements.

- Le fait de modifier un appareil, un compte de médias sociaux, un compte courriel ou toute autre technologie peut signaler à l'auteur que votre cliente recherche de l'aide et entrainer une escalade de la violence.
- Il est parfois nécessaire de prendre des précautions additionnelles dans ces situations.
- Dans certains cas, vous pouvez avoir recours à un spécialiste informatique ou aux forces de l'ordre, par exemple pour la détection de stalkerware ou d'autres logiciels espions.

Mots de passe

- ☐ Dressez une liste de tous les appareils (ordinateur, téléphone, Fitbit, AirTags, système de sécurité résidentiel, voiture intelligente, appareils connectés à Internet, Siri/Alexa, systèmes audio connectés par Bluetooth, etc.) et tous les comptes (médias sociaux, courriels, achats en ligne, services de restauration, applis de transport, comptes infonuagiques, fitness, jeux, etc.).
    - Voir l'annexe A pour une liste de comptes.

Notez ceux auxquels l'auteur a accès et dont il connait ou pourrait connaitre les mots de passe.

- ☐ Demandez-vous quelles informations figurent sur ces comptes.
    - Par example: Adresse, numéro de téléphone, courriel, informations relatives aux cartes de crédit, messages personnels, historique des recherches sur Internet, communications relatives à la planification de sécurité, etc.

- ☐ Créez de nouveaux mots de passe que l'auteur de violence ne pourra pas deviner.
    - Évitez d'utiliser les noms des enfants ou des animaux de compagnie, des dates importantes, d'anciennes adresses ou d'anciens numéros de téléphone.
    - Un code d'accès est une phrase facile à retenir, mais difficile à deviner.
    - L'ajout de symboles de chiffres pour les lettres peut rendre la tâche encore plus difficile (par exemple, C0mT3D3M0nT3Cr1St0).

- ☐ N'utilisez pas le même mot de passe pour plusieurs comptes.

- ☐ Créez un code d'accès unique pour chaque compte ou utilisez un gestionnaire de mots de passe.

- ☐ Changez le mot de passe de votre réseau Wi-Fi.

- ☐ Pour les questions de sécurité, inventez de fausses réponses ou n'utilisez pas de questions dont l'auteur pourrait deviner la réponse.
    - Par exemple: Si la question concerne le nom de jeune fille de votre mère, inventez une réponse.
    - Tâchez de vous souvenir de votre fausse réponse.
- ☐ Désactivez la sauvegarde automatique des mots de passe de tous les appareils et comptes.
- ☐ Déconnectez-vous de tous les comptes et appareils lorsque vous ne les utilisez pas.
- ☐ Utilisez la vérification en deux étapes si possible.
    - Ce processus vous oblige à saisir un code envoyé à votre téléphone ou à votre courriel pour confirmer que c'est bien vous qui accédez au compte.
    - Utilisez ce site web pour une liste des applis qui offrent la vérification en deux étapes.
- ☐ N'utilisez pas de comptes de médias sociaux pour vous connecter à d'autres comptes.
    - Par exemple: «Se connecter avec Facebook», «Se connecter avec Google», etc.
- ☐ Supprimez les adresses courriel ou les appareils de l'auteur de violence des comptes partagés et des Appareils de confiance sur vos comptes.

Blocage, suppression d'amis

- ☐ Envisagez de bloquer ou de supprimer de votre liste d'amis l'adresse courriel, le numéro de téléphone ou l'identifiant sur les médias sociaux de l'auteur de violence.
    - Assurez-vous d'abord d'avoir recueilli toutes les preuves nécessaires.
    - Certains programmes suppriment ou empêchent l'accès aux conversations et aux informations de l'autre personne une fois que son compte a été supprimé de la liste d'amis, ou bloqué.
- ☐ Lorsque vous décidez de bloquer ou de supprimer des amis, demandez-vous si cela pourrait aggraver la situation.
    - L'accès aux médias sociaux de l'auteur peut présenter des avantages (comme le fait de savoir où il se trouve) qui méritent d'être pris en compte.
- ☐ Réfléchissez aux proches et membres de votre famille qui pourraient avoir votre partenaire violent comme «ami» sur leurs comptes.
    - Demandez-leur de ne pas publier d'informations ou de photos vous concernant et de ne rien divulguer à votre sujet à l'auteur des faits.

Harcèlement, traque et surveillance

- ☐ Utilisez un cache-caméra sur tous vos appareils lorsque vous n'utilisez pas la caméra.

- ☐ Si l'auteur surveille votre appareil ou vos comptes, envisagez d'utiliser un autre appareil (l'ordinateur d'un proche, un appareil au travail ou un ordinateur à la bibliothèque) pour rechercher des informations et commencez à planifier la sécurité de vos appareils.

- ☐ Demandez-vous quelles informations personnelles sont publiées en ligne (adresse du domicile sur une invitation à un anniversaire, numéro de téléphone dans une publication Facebook, nouveau lieu de travail sur LinkedIn, etc.) et déterminez si vous souhaitez supprimer ces informations ou les rendre privées.

    - N'oubliez pas que d'autres personnes pourraient partager ces informations avec l'auteur de violence, même si vous les avez bloquées.

- ☐ Désactiver ou limiter les fonctions de localisation sur vos appareils lorsqu'ils ne sont pas utilisés.

- ☐ Désactivez les fonctions de localisation comme Trouver mon téléphone ou Trouver mes amis.

- ☐ Supprimez l'historique des lieux visités, en particulier avant et après votre arrivée dans une maison d'hébergement ou dans un autre endroit sécuritaire.

- ☐ Ne vous «enregistrez» pas sur les médias sociaux lorsque vous participez à un événement.

- ☐ Modifiez les paramètres de confidentialité des applis et des médias sociaux pour qu'ils soient privés dans la mesure du possible.

- ☐ Ne publiez pas sur les médias sociaux de photos contenant des métadonnées ou des informations de fond qui pourraient révéler où vous êtes allée.

    - Une façon de supprimer les métadonnées de localisation d'une photo consiste à publier une capture d'écran plutôt que la photo originale qui contient les métadonnées.

- ☐ Supprimez les adresses courriel ou les appareils de l'auteur de vos comptes partagés et supprimez son téléphone des Appareils de confiance sur tous vos comptes.

    - Voir l'annexe A pour une liste des comptes.

- ☐ Vérifiez l'activité du compte pour voir si des adresses IP inconnues y accèdent.

- ☐ Si vous craignez que l'auteur ait accès à vos comptes, envisagez d'utiliser une boîte postale pour les comptes et livraisons en ligne.

    - Considérez le risque que l'auteur accède aux informations des cartes de crédit ou utilise le compte à votre détriment s'il y a accès.

- ☐ Déconnectez votre téléphone ou d'autres appareils de ceux de l'auteur.
    - Par exemple: La stéréo Bluetooth dans sa voiture ou chez lui, les notifications de fitness sur sa montre intelligente, etc.
- ☐ Fouillez vos effets personnels (sacs à main, voitures, vestes, etc.) à la recherche de dispositifs GPS ou d'autres appareils 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, consoles de jeux, médias sociaux, etc.) et à celles qui pourraient fournir des informations à l'auteur.
- ☐ Demandez-vous si l'auteur peut accéder aux informations sur le système de sécurité du domicile, comme l'accès aux caméras ou des informations sur les personnes qui sortent ou entrent dans la maison.
- ☐ Envisagez d'utiliser un dispositif ou un programme (scanners de réseau, scanners de port, détecteurs de signaux RF, etc.) capable de détecter certaines caméras cachées pour scanner votre Wi-Fi ou votre maison.
- ☐ Faites l'inventaire des applis sur votre téléphone et supprimez celles qui ne vous sont pas familières

- ☐ Si vous craignez que l'auteur ait installé un logiciel espion sur vos appareils, vous pouvez demander à un spécialiste informatique ou aux forces de l'ordre de vérifier l'appareil.
    - N'oubliez pas que si un logiciel espion est installé, l'auteur peut être en mesure de voir toutes les activités sur l'appareil, ce qui peut aggraver la violence.
    - The Clinic To End Tech Abuse propose également des ressources pour aider à identifier les logiciels espions sur un appareil.
    - Signes qu'un appareil peut contenir un logiciel espion:
        - L'appareil fonctionne lentement
        - La batterie se décharge rapidement
        - Les données s'épuisent rapidement
        - L'appareil chauffe
        - L'appareil s'allume lorsqu'il n'est pas utilisé
        - Clics ou sons bizarres lors des appels
        - Prends beaucoup de temps pour s'éteindre
- ☐ Maintenez les systèmes d'exploitation de vos appareils à jour.
    - Ces mises à jour corrigent souvent les éventuelles failles du système d'exploitation dont les pirates et les logiciels espions peuvent tirer parti.
    - Vérifiez à nouveau vos paramètres de confidentialité après une mise à jour pour vous assurer qu'ils n'ont pas été modifiés.

- ☐ Envisagez de remplacer les appareils.
    - Dans ce cas, vous ne devez pas effectuer de sauvegarde des données d'appareils précédents.
    - Cela pourrait transférer un logiciel espion sur le nouvel appareil.
- ☐ Recherchez les dispositifs inhabituels fixés aux ordinateurs de bureau.
    - Par exemple: Les enregistreurs de frappe sont souvent fixés entre le clavier et l'ordinateur.
- ☐ Il convient de noter que les pirates et les ingénieurs informatiques expérimentés peuvent accéder à la localisation d'un appareil, même si cette fonction est désactivée dans les paramètres.
    - Si l'auteur de violence a une formation informatique, votre sécurité technologique peut demander des efforts supplémentaires en fonction de ses compétences.
    - Si tel est le cas, vous pouvez vous adresser à un spécialiste informatique ou aux forces de l'ordre.

Comptes alternatifs

- ☐ Si l'auteur a accès à vos comptes et que vous n'avez pas d'autres options (par exemple, s'il vous oblige à partager vos mots de passe en vous menaçant de vous faire du mal autrement), créez un nouveau compte courriel ou de médias sociaux à son insu et auquel il n'a pas accès pour vos communications sensibles.

- ☐ Ne vous connectez pas à ce compte sur vos appareils personnels ou partagés.
    - Utilisez un ordinateur au travail, à la bibliothèque ou celui d'un proche pour y accéder.

Stockage en nuage, comptes partagés, accès non autorisé

- ☐ Retirez l'auteur de tous les comptes, appareils ou plans partagés, si vous pouvez le faire sans danger.
- ☐ Supprimez les connexions Bluetooth des appareils de l'auteur
    - Par exemple: Ceux qui sont connectés à la chaîne stéréo de son domicile, à sa voiture, etc.
- ☐ Réfléchissez au contenu automatiquement téléchargé ou connecté (calendriers, stockage iCloud pour les photos et les textes, Fitbit, montres intelligentes, etc.) et demandez-vous si l'auteur pourrait avoir accès à ces comptes ou informations.
- ☐ Assurez-vous que seuls vos appareils figurent dans la liste des Appareils de confiance sur tous vos comptes.
- ☐ Vérifiez la dernière activité sur tous vos comptes pour voir si une adresse IP ou un appareil inhabituel a accédé au compte.

Historique de recherche

- ☐ Si l'auteur a accès à l'appareil ou au compte, il peut vérifier votre historique de recherche.
- ☐ Si vous cherchez de l'aide ou des ressources, utilisez un ordinateur sécuritaire.
    - Par exemple: Ordinateur public, d'un proche, au travail, etc.
- ☐ Supprimez sélectivement l'historique des recherches sur Internet.
- ☐ Utilisez les modes «privé» ou «incognito» pour que l'historique des recherches ne soit pas enregistré.
- ☐ Désactivez les cookies dans les paramètres du navigateur.

Images intimes

- ☐ Dressez de mémoire une liste des images et des vidéos qui peuvent exister.
- ☐ Envisagez d'utiliser StopNCII.org pour empêcher d'autres personnes de télécharger des images sexuelles qui ont été enregistrées et «hachées» auprès de l'entreprise.
- ☐ Si vous pouvez le faire en toute sécurité, demandez à vos ex-partenaires de supprimer toute image intime et spécifiez que vous ne leur

accordez pas la permission de les publier. Documentez cette communication.

- ☐ Demandez-vous si l'auteur a pu capturer des images sans consentement.
    - Par exemple: Caméra cachée, capture d'écran via applications.
- ☐ Faites une recherche inversée d'images sur Google.
- ☐ Cherchez votre nom sur des sites pornographiques courants.
    - Par exemple: Les gens sont souvent victimes de doxing et d'atteinte à leur réputation lorsque leurs images sont partagées.
- ☐ Créez une alerte Google pour votre nom. Vous serez avertie lorsque votre nom est mentionné en ligne et affiché avec vos images.
- ☐ Envisagez d'alerter la famille, les proches et les collègues de travail susceptibles de recevoir les images afin de réduire les préjudices.
- ☐ Si l'image a été partagée sans consentement, voir le Cyber Civil Rights Initiative Guide pour obtenir le retrait de contenu de l'Internet.
- ☐ Faites un signalement aux entreprises de médias sociaux ou pornographiques, car 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 les images qui montrent votre visage ou des marques d'identification (tatouages, taches de naissance, etc.).
    - Évitez les images dans des lieux identifiables (par exemple, une pièce reconnaissable).
    - Utilisez des programmes comme Signal qui permettent de faire disparaître les messages.

- ☐ Si des images ont été diffusées, envisagez d'utiliser un service réputé pour vous aider à faire retirer le contenu.

Alertes Google

- ☐ Créez une alerte Google pour votre nom afin d'être avertie lorsqu'il apparaît en ligne. Cela peut vous alerter dans certains cas.

- ☐ 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 (par exemple, des 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.

Mises à jour des logiciels, pare-feu et antivirus

- ☐ Mettez régulièrement à jour vos logiciels.
    - Cela inclut vos appareils mobiles.
    - Ces mises à jour corrigent souvent les failles de sécurité que les pirates pourraient exploiter.
- ☐ Activez les pare-feu et les antivirus sur tous les appareils.

Collecte des preuves

- ☐ Créez un journal de toutes les expériences de VFGFT et incluez des informations telles que l'heure, la date, l'auteur, les preuves et d'autres informations utiles.
- ☐ Voir le modèle de journal de la violence facilitée par la technologie d'HFC.
- ☐ Prenez des captures d'écran ou faites des enregistrements des comportements violents.
- ☐ Vérifiez si l'appli peut alerter l'auteur lorsque vous faites une capture d'écran.
    - Si oui, il peut être préférable de prendre une photo ou une vidéo avec un autre appareil.

- ☐ Veillez à inclure le profil et les autres informations d'identification de l'auteur dans les preuves.

- ☐ Assurez-vous que la date des actes abusifs y figure.

- ☐ En cas de courriel violent, conservez le courriel original, car il contient des métadonnées telles que l'adresse IP de l'expéditeur.

- ☐ En cas de publication de contenu préjudiciable, capturez-le avant que la personne ait le temps de le supprimer.

- ☐ Conservez des copies des preuves dans un endroit sécuritaire. Sauvegardez ces informations dans au moins un autre endroit.

- ☐ Si l'auteur a accès à l'appareil ou au service infonuagique où se trouvent les preuves, il peut les supprimer.

- ☐ Conservez à la fois des copies imprimées et des copies numériques des preuves.

La violence fondée sur le genre facilitée par la technologie (VFGFT) fait partie d'un continuum de violence qui peut se produire à la fois en ligne et en personne. Si vous ou l'une de vos connaissances faites face à la VFGFT, vous n'êtes pas seule. Vous pouvez utiliser hebergementfemmes.ca pour trouver une maison d'hébergement près de chez vous ou appeler ou envoyer un message texte à Jeunesse, J'écoute pour discuter de vos options et créer un plan de sécurité. Vous n'avez pas besoin de résider dans une maison d'hébergement pour accéder à un soutien et à des services gratuits et confidentiels.. Vous n'avez pas besoin de résider dans une maison

d'hébergement pour accéder à un soutien et à des services gratuits et confidentiels.

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

Adapté du projet Technology Safety de la BCSTH, d'après leur ressource Technology Safety Planning Checklist.

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
- ☐ Ordinateurs
- ☐ Gmail
- ☐ Courriel personnel et professionnel
- ☐ Messenger
- ☐ WhatsApp
- ☐ Signal
- ☐ Slack
- ☐ QQ
- ☐ Viber
- ☐ Télégram
- ☐ Messages instantanés, directs (MD) ou privés sur des plateformes en ligne

Vidéoconférence

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

Services infonuagiques

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

Garde d'enfants et animaux de compagnie

- ☐ Calendriers partagés
- ☐ Applis de suivi des enfants
- ☐ Interphone bébé
- ☐ Partage de photos
- ☐ Applis de planification
- ☐ Caméra pour animaux
- ☐ Traceur d'animaux (dispositif GPS dans le collier, etc.)

Finances

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

Factures et services publics

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

Comptes gouvernementaux

- ☐ Agence du revenu du Canada
- ☐ Applis de prise de rendez-vous
- ☐ Compte de prêt étudiant
- ☐ Mon compte (ARC)
- ☐ Compte des services provinciaux

Services de livraison de nourriture

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

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 en ligne ou non

Divertissement

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

Gaming

- ☐ Discord
- ☐ Twitch
- ☐ Switch
- ☐ Steam
- ☐ Xbox Live
- ☐ Réseau PlayStation
- ☐ Origin
- ☐ Applis de jeux

Santé et fitness

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

Voyage

- ☐ Cartes de points (Aeroplan, Air Miles, etc.)
- ☐ Airbnb
- ☐ Expedia
- ☐ TripAdvisor
- ☐ HostelInternational
- ☐ Compagnies aériennes
- ☐ Trains

Appareils connectés pour la maison

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

Appareils portables intelligents	Comptes liés à l'éducation
☐ Voiture intelligente	☐ Courriel de l'école
☐ GPS dans la voiture	☐ Plateforme de travaux scolaires
☐ Bluetooth dans la voiture	☐ Carte de bibliothèque
☐ Appli de suivi pour vélo	☐ Applis linguistiques
☐ Tiles	
☐ Trouver mon Téléphone	