Sécurité technologique Canada

Internet des objets et appareils connectés

Une note sur la langue

Dans cette trousse, nous utiliserons parfois le mot femme et les pronoms féminins par souci de simplicité et pour reconnaître l'impact significatif de la violence facilitée par la technologie sur les femmes et les filles. Nous reconnaissons que la VFGFT a également un impact sur les personnes trans, non binaires et bispirituelles. Nous espérons que toutes les personnes touchées par la VFGFT trouveront ces documents utiles.

Aperçu de l'Internet des objets et des appareils connectés

Qu'est-ce que l'Internet des objets?

L'Internet des objets (IdO) désigne un réseau d'appareils connectés entre eux, et à un appareil ou une appli qui contrôle le réseau. Ces appareils peuvent être connectés par Internet, Bluetooth ou d'autres moyens. Malheureusement, ces appareils et systèmes peuvent constituer une autre façon, très intrusive, d'utiliser la technologie à mauvais escient pour surveiller, harceler, menacer ou nuire. En revanche, ce sont également des outils qui peuvent contribuer à améliorer la sécurité.

Dispositifs de l'IdO les plus courants

Domotique et assistants personnels

Les appareils «intelligents» et «connectés» semblent se démultiplier dans nos maisons avec la promesse d'augmenter notre niveau de confort, de faire des économies d'énergie et de renforcer la sécurité personnelle. Il peut s'agir de l'éclairage, des thermostats, des caméras de sécurité, etc. La domotique de l'IdO permet le contrôle et la surveillance à distance.

Jouets intelligents et traceurs de localisation

Les jouets «intelligents» et «connectés» promettent de divertir, d'accroître la sécurité et de nous connecter à nos enfants et à nos animaux de compagnie lorsque nous ne sommes pas à la maison.

Voitures intelligentes et véhicules sans conducteur

Si les véhicules sans conducteur relèvent encore du fait divers pour plusieurs, de nombreuses voitures sont déjà «connectées», ce qui permet aux parents de contrôler les habitudes de conduite des jeunes et aux employeurs de surveiller celles de leur personnel. En outre, de petits gadgets peuvent être fixés à une voiture pour activer la surveillance et, dans certains cas, le contrôle à distance de certaines fonctions.

Santé connectée et dispositifs médicaux

De nombreux dispositifs médicaux et de santé sont désormais connectés et vous permettent de consulter les informations relatives à votre santé, voire de les envoyer à votre médecin.

Mesures à prendre pour accroître la sécurité et la confidentialité

Soyez consciente des risques lorsque vous utilisez un appareil intelligent et familiarisez-vous avec les mesures susceptibles de renforcer la sécurité et la confidentialité. Bien que chaque appareil intelligent soit différent, voici quelques conseils généraux.

1. Savoir comment fonctionne votre appareil

La première étape pour garantir votre sécurité et votre confidentialité lorsque vous utilisez un appareil intelligent est de comprendre son fonctionnement. Lorsque vous configurez un appareil intelligent, vous allez soit créer un compte pour cet appareil, soit y joindre une adresse courriel, soit le connecter à un réseau (généralement le réseau Wi-Fi de votre domicile) – ou peut-être tout cela à la fois. Une idée générale du fonctionnement de votre appareil et de ce à quoi il est connecté vous permettra de déterminer quelles informations sont partagées et comment y accéder, ce qui vous aidera à identifier et minimiser les risques.

2. Limitez les connexions à votre appareil intelligent

Examinez comment et à quoi il est connecté. S'il est connecté par Wi-Fi, éteignez-le lorsque vous ne l'utilisez pas. Si c'est impossible, déconnectez-le d'Internet. Si l'appareil dispose d'autres types d'accès, tels que Bluetooth, désactivez l'accès à la connexion. S'il est éteint ou non connecté, personne ne peut y accéder à distance.

3. Limitez les informations personnelles partagées depuis votre appareil intelligent

Vos informations sont stockées soit sur l'appareil, soit dans un compte, soit auprès de l'entreprise. Si vous craignez que quelqu'un y ait accès, déterminez si vous pouvez limiter les informations personnelles stockées ou partagées via l'appareil. Il peut s'agir d'éteindre l'appareil lorsqu'il n'est pas utilisé, de désactiver les caméras ou les microphones, ou de

revoir les paramètres et de limiter la quantité d'informations que l'entreprise peut recueillir sur vous. Lisez la politique de confidentialité de l'entreprise pour savoir comment elle partage vos données personnelles.

4. Sécuriser le compte associé à votre appareil

Certains appareils vous demandent de les configurer avec un compte, vous invitant à créer un nom d'utilisateur et un mot de passe. Créez un nom d'utilisateur et un mot de passe que personne d'autre (y compris l'auteur de violence) ne peut deviner. Certains comptes peuvent proposer une vérification en deux étapes. Ainsi, si quelqu'un essaie d'accéder à votre compte à partir d'un autre appareil ou d'un autre lieu, il devra fournir un code de vérification supplémentaire (généralement transmis par SMS).

Si l'appareil ne nécessite pas de nom d'utilisateur ou de mot de passe, sachez comment il se connecte et si quelqu'un d'autre pourrait accéder.

5. Renforcer la sécurité de votre routeur

Les appareils intelligents étant fréquemment connectés à un réseau Wi-Fi, assurez-vous que votre routeur est sécurisé. Voici quelques mesures à prendre pour améliorer la sécurité du routeur:

- Créez un code d'accès pour le réseau Wi-Fi à la maison
- Assurez-vous de modifier le nom d'utilisateur et le mot de passe par défaut du routeur
- Utiliser le cryptage WPA2
- Désactiver la gestion à distance sur le routeur

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 consulter hebergementfemmes.ca pour trouver une maison d'hébergement près de chez vous afin de discuter de vos options et de 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.

Adapté pour le Canada avec la permission du Tech Safety Project de WESNET, d'après leur ressource Smart Devices and Internet of Things.

Domotique: Risques et stratégies en matière de protection de la confidentialité

Nos maisons, nos lieux de travail et nos véhicules se remplissent rapidement d'appareils «intelligents» et «connectés» qui promettent d'accroître le confort, d'améliorer les économies d'énergie et de renforcer la sécurité personnelle. Ces appareils et systèmes offrent aux survivantes des outils pour accroître stratégiquement leur sécurité. Malheureusement, ces appareils et les systèmes qui les contrôlent constituent un autre moyen très intrusif d'utiliser la technologie pour surveiller, harceler, menacer ou porter préjudice aux survivantes.

Pour plus d'informations et de conseils généraux sur l'Internet des objets et les appareils connectés, consultez notre document de présentation.

Exemples de domotique

La domotique comprend des équipements, des systèmes ou des applis qui permettent de contrôler les appareils connectés à distance. En voici quelques exemples:

- Assistants personnels (Google Home, Amazon Echo/Alexa, etc.). Ces appareils sont activés par la voix et proposent de régler l'éclairage, de diffuser de la musique, de passer des appels téléphoniques, de lire des SMS, de rechercher des informations, etc.
- Systèmes domotiques (Nest, Arduino, etc.). Ces systèmes reposent souvent sur un thermostat ou des interrupteurs et peuvent également inclure d'autres appareils connectés. Certaines marques ne permettent la connexion qu'avec des appareils de la même marque, tandis que d'autres offrent une meilleure compatibilité.
- Les applis s'associent aux objets connectés et permettent un contrôle à partir d'appareils mobiles. Nombre de ces applis sont fournies avec les dispositifs IdO, et certaines fonctionnent avec plusieurs marques. Ces applis peuvent vous avertir si le détecteur de fumée est déclenché, si une personne est à la porte ou si vous avez oublié d'éteindre un appareil.
- Des routines préprogrammées peuvent être intégrées et dépendre ou non de votre accès à distance pour s'exécuter. Par exemple, lorsque votre téléphone s'approche de la maison, la porte d'entrée peut se déverrouiller, des lumières s'allumer, la musique commencer et le thermostat se régler selon vos préférences.

Appareils connectés

Ces appareils courants peuvent également faire partie du réseau:

- Thermostat
- Ampoules intelligentes
- Prises électriques intelligentes (avec des lampes ou d'autres appareils branchés dans ces prises)
- Systèmes de divertissement (stéréo, télévision, haut-parleurs, etc.)
- Haut-parleurs intelligents situés sur une table de chevet, dans un placard ou à d'autres endroits de la maison, qui se connectent à l'assistant personnel domestique
- Caméras de sécurité et détecteurs de mouvement
- Détecteurs de fumée
- Sonnettes vidéo
- Serrures intelligentes
- Appareils ménagers (réfrigérateur, aspirateur, etc.)
- Distributeurs de nourriture, caméras, jouets et traceurs pour animaux de compagnie
- Jouets et traceurs pour enfants

L'usage de la domotique comme tactique de violence

Les équipements et systèmes domotiques peuvent être utilisés à mauvais escient pour surveiller, harceler, isoler et nuire aux survivantes. La technologie permet de savoir qui se trouve dans la maison et ce que font ces personnes. Cette surveillance peut être effectuée secrètement ou ouvertement, afin de contrôler le comportement en capturant des images, en conservant des journaux d'activité et en accédant aux courriels ou à d'autres comptes liés aux appareils connectés.

La domotique peut également être utilisée pour causer détresse et préjudices en allumant ou éteignant les lumières et les appareils, en réglant la température à des niveaux inconfortables, en diffusant de la musique non désirée ou en changeant le volume, en déclenchant les différents détecteurs et alertes et en verrouillant ou déverrouillant les portes. Ce type de harcèlement peut perturber considérablement le sommeil et déclencher des réactions traumatiques.

La domotique peut également servir à isoler une survivante en menaçant ses visiteurs, en publiant des vidéos ou des images privées et en bloquant l'accès physique. Par exemple, les serrures intelligentes pourraient être contrôlées à distance, limitant ainsi la capacité d'une survivante à quitter la maison ou à revenir chez elle. Une sonnette vidéo pourrait être utilisée non seulement pour surveiller les personnes qui se présentent à la porte, mais aussi pour les harceler ou, en combinaison avec une serrure intelligente, les empêcher d'entrer.

Les personnes en situation de handicap peuvent subir un préjudice supplémentaire lorsqu'un proche aidant, un membre de la famille ou un·e colocataire prend le contrôle, limite l'accès ou endommage le système ou les appareils, comme cela peut se produire avec d'autres technologies d'assistance.

Planification de la sécurité et abus domotiques

La planification de sécurité doit tenir compte de l'expérience et des priorités de chaque survivante. Identifier la technologie utilisée à mauvais escient et prendre des mesures pour réduire les risques qui y sont liés demande du temps, de l'énergie et un accès à l'information.

Si vous soupçonnez qu'un appareil est utilisé pour vous nuire, documentez les incidents sans plus tarder. Notre journal de la violence facilitée par la technologie vous aidera à documenter chaque événement. Ces journaux peuvent être utiles pour révéler des tendances et déterminer les prochaines étapes, et pour constituer un dossier si vous décidez d'intenter des poursuites.

Posez des questions qui peuvent aider à identifier les schémas de comportement, par exemple:

- Existe-t-il des schémas quant au moment où les appareils sont utilisés à mauvais escient (le moment de la journée, les événements connexes tels que les contacts, les visites, les procédures judiciaires, etc.)?
- La personne qui abuse de la technologie a-t-elle accès au domicile, aux comptes des services publics, aux appareils, etc.? Est-ce que l'auteur de violence y a eu accès par le passé?
- Suis-je en mesure de faire une liste des appareils dans la maison?
- Qu'est-ce qui pourrait être caché?

Une fois que les équipements et les services suspects ont été identifiés, et notamment le type de système qui pourrait contrôler les appareils, l'étape suivante consiste à reprendre le contrôle. Par exemple, s'il s'agit d'un dispositif d'assistance personnelle, pouvez-vous accéder au compte et changer le mot de passe pour empêcher l'accès non autorisé? S'il s'agit d'une appli, le système, le réseau ou les appareils peuvent-ils être reconfigurés pour verrouiller l'accès?

Voici quelques approches pour régler ces problèmes:

- Contacter l'entreprise qui a fabriqué l'appareil ou qui gère le logiciel pour modifier la propriété du compte et l'accès.
- Modifier les paramètres du routeur ou du réseau. Pour plus d'informations, consultez notre document sur la sécurité Wi-Fi.
- Remplacer les dispositifs (ampoules, thermostat, prises de courant ou autres appareils connectés) pour soit les retirer du système, soit en reprendre le contrôle.

NOTE: Il est important de planifier la sécurité en tenant compte du fait que le fait d'interrompre le contrôle à distance peut aggraver un comportement violent.

La domotique au service de la sécurité

Ces mêmes systèmes et appareils qui peuvent être utilisés pour nuire aux survivantes peuvent également servir à renforcer la sécurité et protéger la confidentialité. Voici quelques exemples:

- Les caméras de sécurité, les sonnettes vidéo et autres dispositifs de sécurité peuvent avertir une femme lorsque quelqu'un s'approche ou entre dans la maison. Ces appareils peuvent également recueillir des preuves pour documenter les violations d'une ordonnance de protection ou d'autres comportements criminels.
- Les ampoules intelligentes peuvent rassurer une femme en éclairant la maison ou une pièce avant qu'elle n'y entre.
- Les caméras et les distributeurs d'aliments pour animaux de compagnie peuvent apporter soutien ou réconfort lorsqu'elle n'est pas chez elle, ou la rassurer sur la santé ou la sécurité d'un animal.
- Les dispositifs d'économie d'énergie peuvent contribuer à réduire la charge financière et renforcer l'indépendance.
- La domotique peut aider les femmes en situation de handicap, en diminuant le niveau de soutien nécessaire de la part des proches aidants et en améliorant l'autonomie.

Considérations relatives aux nouveaux dispositifs

Lorsque vous envisagez d'acheter de nouveaux dispositifs ou appareils, demandez-vous:

- Cet appareil particulier doit-il être «intelligent» ou «connecté»?
- Est-ce que les avantages l'emportent sur les risques?
- Quel est le niveau de sécurité de l'appareil et de son appli?
- La sécurité peut-elle être renforcée dans ce cas?

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 consulter hebergementfemmes.ca pour trouver une maison d'hébergement près de chez vous afin de discuter de vos options et de 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.

Adapté pour le Canada avec la permission du Safety Net Project de NNEDV, d'après leur ressource Internet of Things Home Automation: Survivor Privacy Risks and Strategies.

Jouets intelligents et géolocalisation: Problèmes de sécurité et de confidentialité associés aux enfants et aux animaux de compagnie

Les jouets «intelligents» et «connectés» qui promettent de divertir, d'accroître la sécurité et de nous connecter à nos enfants et à nos animaux de compagnie en tout temps sont omniprésents sur le marché. Ces appareils et systèmes offrent aux survivantes des outils pour améliorer leurs stratégies de sécurité. Malheureusement, ces appareils et les systèmes qui les contrôlent constituent un autre moyen très efficace d'utiliser la technologie à mauvais escient pour surveiller, harceler, menacer ou blesser les survivantes.

Pour plus d'informations et de conseils généraux sur l'Internet des objets et les appareils connectés, consultez notre document de présentation.

Jouets intelligents

Nous pouvons désormais acheter des jouets qui écoutent nos enfants et leur parlent, lisent des histoires, posent des questions et font des recherches sur Internet. Certains jouets sont équipés de caméras, de microphones et de haut-parleurs afin de pouvoir interagir avec l'enfant.

La reconnaissance vocale peut présenter des risques pour la sécurité et la confidentialité, car elle peut servir à se faire passer pour un enfant. La reconnaissance vocale peut être utilisée à mauvais escient par un auteur de violence pour verrouiller et contrôler certaines fonctions des jouets intelligents, y compris installer des fonctions de localisation. Il est important de comprendre la différence entre «reconnaissance vocale» et «reconnaissance de parole». La *reconnaissance vocale* est la capacité de l'appareil à déterminer qui parle: un adulte par rapport à un enfant, par exemple, ou même des personnes spécifiques dans la maison. La *reconnaissance de parole* est la capacité de l'appareil à comprendre les mots prononcés. Cette fonction est incorporée dans des appareils mobiles ou des assistants personnels domotiques comme Alexa d'Amazon ou Google Home.

Le *principal risque associé à ces jouets concerne une éventuelle surveillance par un auteur de violence, un voisin ou toute autre personne*. De nombreux appareils ne sont pas dotés d'une protection suffisante contre ce genre de méfaits. Par exemple, certains appareils peuvent être connectés par Bluetooth, ce qui permet à des personnes à proximité, comme des voisins, d'accéder au jouet.

D'autres offrent une sécurité contre les tiers ou les étrangers, mais peuvent permettre un accès vidéo ou audio non autorisé à la personne qui offre le jouet en cadeau, par exemple. Les informations recueillies peuvent servir pour traquer, contrôler ou harceler les survivantes.

Les petits drones utilisés pour les loisirs sont un autre jouet de plus en plus populaire. Ces appareils minuscules, souvent appelés «nano-drones», tiennent dans la paume de la main et peuvent coûter moins de 50$. Les drones de taille moyenne destinés à la course ou à d'autres compétitions sont beaucoup plus chers et peuvent inclure des microphones

ou des caméras. Certains drones sont contrôlés à distance, comme l'ancienne génération de jouets télécommandés, mais de nouveaux modèles peuvent être contrôlés par des appareils mobiles.

Autres appareils de l'IdO pour les familles

Outre les jouets intelligents, de nombreux autres appareils ciblent les parents et les familles avec des publicités les présentant comme un moyen d'accroître la sécurité de leurs enfants. Ceux-ci peuvent ne pas disposer de modes de sécurité adéquats ou être utilisés pour surveiller ou nuire à un enfant ou à un autre membre de la famille.

- Les interphones bébés, dont les anciennes versions ont longtemps été vulnérables à la surveillance par ondes radio, sont désormais connectés à un combiné ou à l'appareil mobile d'un parent.
- Les appareils de localisation sont depuis longtemps commercialisés comme un moyen de retrouver les enfants ou les parents âgés si jamais ils s'aventurent trop loin. Autrefois basés sur la technologie GPS, les nouveaux appareils utilisent des technologies plus économes en énergie et plus durables, associées à la commodité d'une connexion à un appareil mobile ou Internet.

Les nouvelles versions de ces appareils étant connectées, elles présentent de nouveaux risques de surveillance par un auteur de violence conjugale ou d'abus sexuels sur des enfants, tant à l'intérieur qu'à l'extérieur du domicile.

Dispositifs de l'IdO pour animaux de compagnie

Un autre marché en pleine croissance s'adresse aux propriétaires d'animaux de compagnie.

- Les distributeurs de nourriture et d'eau sont associés à des caméras et à des haut-parleurs afin que les propriétaires puissent garder un œil sur leur animal en leur absence, voire jouer avec lui ou lui lancer une friandise.
- Certains appareils permettent de suivre la localisation ou les signes vitaux de l'animal, en relayant ces informations sur Internet ou par une appli.
- Comme pour ceux destinés aux enfants, les appareils de géolocalisation pour animaux de compagnie fonctionnaient jusqu'ici par GPS. Les appareils plus récents utilisent des technologies moins énergivores et plus durables, par le biais d'une connexion à un appareil mobile ou à une interface Web.

Ces appareils, comme les jouets intelligents, ont souvent des fonctions de sécurité inadéquates ou rendent la tâche de modifier les paramètres de sécurité par défaut plutôt difficile. Ces appareils pourraient être utilisés pour surveiller la maison par le biais d'une caméra ou pour suivre les déplacements d'une personne lorsqu'elle promène son animal de compagnie.

Avantages des appareils connectés et intelligents

Le contact à distance avec les enfants et les animaux de compagnie peut constituer un élément important du bien-être émotionnel. Le fait de pouvoir localiser les enfants et les animaux de compagnie et de veiller à leur sécurité peut contribuer à rassurer les femmes subissant la violence. En cas de violence ou de harcèlement à l'encontre d'une femme,

de ses enfants ou de ses animaux de compagnie, les caméras de ces appareils peuvent capturer des images qui pourront servir de preuve.

Questions sur les appareils connectés à l'IdO

Voici quelques questions à se poser lorsqu'on envisage d'acheter des jouets connectés ou de faire entrer ces appareils dans la maison:

- Est-ce nécessaire que cet appareil soit «intelligent» ou «connecté»?
- Est-ce que les avantages l'emportent sur les risques?
- Quel est le niveau de sécurité de l'appareil et de son appli?
- Existe-t-il des fonctionnalités sur mesure qui permettent d'accroître la sécurité et la confidentialité?

Stratégies pour accroître la sécurité et la confidentialité

Les précautions visant à renforcer la confidentialité et la sécurité des jouets intelligents consistent à se renseigner sur les options intégrées à l'appareil, à l'éteindre lorsqu'il n'est pas utilisé et à modifier les mots de passe par défaut ou autres paramètres de sécurité.

Si vous soupçonnez qu'un appareil est utilisé à mauvais escient, documentez les incidents dès maintenant. Notre journal de la violence facilitée par la technologie est un outil pour documenter chaque événement. Ces journaux peuvent être utiles pour révéler des schémas et déterminer les prochaines étapes, et peuvent éventuellement servir à constituer un dossier si vous choisissez d'intenter des poursuites.

Vous pouvez essayer d'accéder à des preuves par le biais de l'appareil, de l'appli ou du site qui lui est associé. Vous pouvez également essayer d'entrer en contact avec le fabricant pour reprendre le contrôle d'un appareil ou de son compte. Dans tous les cas, il importe de prendre des mesures pour renforcer la sécurité du réseau et du Wi-Fi. Pour plus d'informations, consultez notre document sur la sécurité Wi-Fi.

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 consulter hebergementfemmes.ca pour trouver une maison d'hébergement près de chez vous afin de discuter de vos options et de 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.

Adapté pour le Canada avec la permission du Safety Net Project de NNEDV, d'après leur ressource Smart Toys and Location Trackers: Privacy and Safety Concerns with Children and Pets.

Voitures connectées et véhicules sans conducteur: Problèmes de sécurité et de

confidentialité

Si les véhicules sans conducteur n'ont pas encore fait leur apparition sur les routes canadiennes, de plus en plus de voitures sont livrées déjà «connectées», ce qui permet notamment aux parents de surveiller les habitudes de conduite des jeunes et aux employeurs celles de leur personnel. En outre, de petits gadgets peuvent être fixés à une voiture pour permettre une surveillance à distance et, dans certains cas, un contrôle à distance.

Pour plus d'informations et de conseils généraux sur l'Internet des objets et les appareils intelligents ou connectés, consultez notre document de présentation.

Voitures sans conducteur

Certains fabricants automobiles, services de covoiturage et entreprises de livraison de marchandises font l'apologie des voitures sans conducteur. Ces voitures combinent une grande variété de capteurs et de systèmes qui permettent de diriger un véhicule dans le trafic urbain et sur de longs tronçons d'autoroute. Dans presque tous les cas, les voitures nécessitent la présence d'une personne sur le siège du conducteur pour prendre le relais en cas de problème. De nombreuses voitures en circulation aujourd'hui sont déjà dotées de fonctions de base d'assistance par ordinateur qui aide le conducteur à effectuer une tâche, par exemple à actionner automatiquement les freins.

Voitures connectées

Aujourd'hui, plusieurs services sur le marché sont conçus pour surveiller et contrôler les décisions de conduite du personnel des entreprises et des jeunes au volant. Ces services permettent de surveiller les habitudes de conduite et de repérer la localisation, puis de fournir un rapport électronique ou des mises à jour en temps réel. Les options permettant de contrôler une voiture à distance ou en fixant des limites prédéfinies comprennent les limites de vitesse et du volume audio, ou le blocage des SMS ou des alertes d'applis sur le téléphone de l'adolescent·e. Ces options peuvent également être utilisées par un auteur de violence pour contrôler le véhicule d'une femme.

Un nombre limité de véhicules sont équipés de ces services, tandis que de nombreux autres fonctionnent en branchant un petit appareil sur la prise de diagnostic de bord (OBD). Le système OBD est une partie de la voiture qui passe souvent inaperçue. Il s'agit d'un ordinateur qui peut suivre les émissions, le kilométrage, la vitesse et d'autres données. Certaines applis permettent également de recourir directement à l'appareil mobile du conducteur pour recueillir et envoyer des informations et bloquer les messages entrants.

Risques pour la sécurité et la confidentialité

Le principal risque de sécurité des voitures connectées concerne la possibilité de les contrôler à distance. Le plus grave serait de provoquer un accident en prenant le contrôle de la direction, du freinage ou de l'accélération. Parmi les autres risques, citons la prise de contrôle du volume du système de son, de l'éclairage, du klaxon, des essuie-glaces et d'autres fonctions susceptibles de distraire ou de perturber, risquant ainsi de provoquer des accidents. Des pirates informatiques ont démontré qu'il était possible de prendre le contrôle de toutes ces fonctions dans les voitures actuellement en circulation.

Les risques pour la confidentialité découlent de la surveillance et du partage des informations sur les habitudes de conduite et la localisation. Les fonctions intégrées, celles nécessitant une connexion physique, ainsi que les applis pour appareil mobile, peuvent partager des informations à distance, offrant ainsi une possibilité de surveillance et de contrôle. Les fabricants stockent également les informations recueillies sur les véhicules, ce qui peut poser un risque d'accès non autorisé.

Avantages des appareils connectés et intelligents

Si les risques liés aux voitures connectées sont très inquiétants, il existe des moyens d'utiliser cette technologie de manière stratégique pour accroître la sécurité. Une femme qui souhaite localiser un véhicule ou ses passagers, se rassurer ou diriger les services d'urgence en cas de vol ou d'enlèvement peut partager sa position. Une femme peut également choisir de partager sa position avec des proches ou des membres de sa famille. Enfin, les déplacements ou les habitudes de conduite d'un auteur de violence peuvent être utilisés comme preuves.

Questions sur l'IdO

Voici quelques questions à se poser lorsqu'on envisage l'achat de voitures connectées, d'équipements à brancher sur les voitures ou d'applis:

- Cet appareil particulier doit-il absolument être «intelligent» ou «connecté»?
- Est-ce que les avantages l'emportent sur les risques?
- Quel est le niveau de sécurité de l'appareil et de l'appli qui le fait fonctionner?
- Existe-t-il des fonctionnalités qui permettent de personnaliser et d'accroître la sécurité et la confidentialité?

Stratégies pour accroître la sécurité et la confidentialité

Pour améliorer la sécurité et la confidentialité, il faut notamment se renseigner sur les options de sécurité intégrées, désactiver ces fonctions lorsqu'elles ne sont pas utilisées et modifier les mots de passe ou autres paramètres de sécurité par défaut.

Si vous soupçonnez qu'un appareil est utilisé à mauvais escient, documentez les incidents sans plus attendre. Notre journal de la violence facilitée par la technologie est un outil pour documenter chaque événement. Ces journaux peuvent être utiles pour révéler des schémas et déterminer les prochaines étapes, et peuvent éventuellement servir à constituer un dossier si vous choisissez d'intenter des poursuites.

Vous pouvez également tenter d'accéder à des preuves par le biais de l'appareil ou de son appli ou compte. Vous pouvez également essayer d'entrer en contact avec le fabricant pour reprendre le contrôle d'un appareil ou de son compte. Avec ces appareils, il est également important de prendre des mesures pour renforcer la sécurité du réseau et du Wi-Fi. Pour plus d'informations, consultez notre document sur la sécurité Wi-Fi.

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 consulter hebergementfemmes.ca pour trouver une maison d'hébergement près de chez vous afin de discuter de vos options et de 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.

Adapté pour le Canada avec la permission du Safety Net Project du NNEDV, d'après leur ressource Connected Cars and Driverless Vehicles Safety and Privacy Concerns.

Santé connectée et appareils médicaux: Confidentialité, risques et stratégies pour les survivantes

De nombreux appareils médicaux et de santé sont désormais connectés, offrant la possibilité de consulter des informations, ou même d'envoyer des informations à un service de santé. Malheureusement, ces appareils et systèmes peuvent constituer un autre moyen très invasif d'utiliser la technologie à mauvais escient pour surveiller, harceler, menacer ou blesser les survivantes. Parallèlement, ils peuvent offrir des outils pour accroître stratégiquement la sécurité. Il existe des exemples de cas où les données de ces appareils ont été utilisées avec succès comme preuves dans des affaires criminelles.

Pour plus d'informations et de conseils généraux sur l'Internet des objets (IdO) et les appareils intelligents, consultez notre document de présentation.

Vous trouverez ci-dessous quelques exemples d'appareils médicaux et de santé connectés.

Électronique grand public

Un nombre croissant d'appareils proposent d'aider les gens à faire de l'exercice, perdre du poids et adopter un mode de vie sain. Les plus courants sont les traqueurs de pas et les montres intelligentes. Les appareils d'exercice proposent désormais de se connecter à un appareil mobile pour suivre et partager des informations sur la durée et l'intensité d'une séance d'entraînement, ainsi que sur des signes vitaux, comme la fréquence cardiaque. Les chaussures de sport peuvent également être connectées et partager des informations, notamment la localisation.

Appareils médicaux

Des appareils plus récents de suivi des signes vitaux collectent, analysent et partagent des informations, notamment des tensiomètres et des thermomètres pour le suivi de la fertilité. Des équipements médicaux tels que des fauteuils roulants, stimulateurs cardiaques et flacons de pilules peuvent être dotés de la capacité de suivre la position ou la fréquence d'utilisation et d'en informer votre médecin ou un établissement médical.

Risques pour la sécurité et la confidentialité

Si tout le monde peut être confronté à des risques d'atteinte à la vie privée en raison d'un accès non autorisé à des données provenant d'équipements médicaux et de santé, les femmes qui vivent la violence sont confrontées à des risques particuliers. Des informations sur la localisation, l'activité physique, les signes vitaux ou les habitudes générales pourraient être utilisées pour les menacer ou leur nuire. Des informations personnelles sensibles pourraient être partagées publiquement dans le but de ruiner leur réputation. Par exemple, les données d'utilisation des jouets sexuels connectés utilisés par une femme dans le cadre de sa guérison pourraient être partagées avec un employeur ou d'autres personnes. La sécurité intégrée des appareils et des données qu'ils recueillent est clairement insuffisante, ce qui suggère que les appareils peuvent être surveillés ou même désactivés à distance. En outre, les informations provenant des appareils connectés sont intégrées dans de vastes ensembles de données détenus par des entreprises et les gouvernements. Ces données peuvent contenir des informations identifiantes, inexactes et dommageables.

Avantages pour les survivantes

Les femmes en situation de handicap ou confrontées à des problèmes médicaux complexes, qui peinent à se souvenir de tâches liées à la santé, ou qui souhaitent simplement améliorer leur santé, peuvent bénéficier d'appareils connectés. Les effets des traumatismes peuvent entraver la capacité à se souvenir des tâches quotidiennes, diminuer la motivation pour l'activité physique ou avoir un impact sur le rythme cardiaque et les autres signes vitaux. Les appareils connectés pourraient faire partie d'un plan visant à améliorer le bien-être ou à assurer le suivi des effets d'un traumatisme. L'utilisation d'appareils médicaux et de santé spécifiques peut contribuer à atténuer les symptômes et les maladies résultant d'un traumatisme ou d'une blessure physique. Tous ces avantages peuvent être compromis par un manque de sécurité et de confidentialité. Les femmes et les professionnels de la santé doivent donc tenir compte de ces facteurs lors du choix des appareils.

Preuves

De récents reportages ont fait état de cas dans lesquels des données provenant d'appareils médicaux et de santé ont été utilisées comme preuves dans des affaires criminelles aux États-Unis. Les informations relatives à la localisation, aux déplacements et aux signes vitaux sont susceptibles de servir à l'avenir pour étayer ou contrer une version des événements entourant des crimes. Ces mêmes preuves peuvent également servir dans un cadre juridique civil pour appuyer des demandes d'ordonnances de protection ou des affaires de droit de la famille.

Les preuves provenant des appareils médicaux et de santé connectés peuvent être stockées sur l'appareil lui-même, sur un appareil mobile, dans un compte ou sur le serveur d'un fabricant ou d'un fournisseur médical. Dans certains cas, une femme peut avoir accès aux données, et dans d'autres, une assignation à comparaître ou une ordonnance du tribunal peut s'avérer nécessaire.

Questions sur les appareils médicaux et de santé

Voici quelques questions à se poser sur les appareils médicaux et de santé connectés:

- Est-ce que cet appareil particulier doit être «intelligent» ou «connecté»?
- Est-ce que les avantages l'emportent sur les risques?
- Quel est le niveau de sécurité de l'appareil et de l'appli qui le fait fonctionner?
- Existe-t-il des fonctionnalités qui permettent d'individualiser et d'accroître la sécurité et la confidentialité?

Stratégies pour accroître la sécurité et la confidentialité

Pour améliorer la sécurité et la confidentialité, il faut notamment se renseigner sur les options de sécurité intégrées, désactiver l'appareil lorsqu'il n'est pas utilisé et modifier les mots de passe par défaut ou autres paramètres de sécurité. Demandez à votre médecin s'il est possible d'utiliser un appareil non connecté, ou des alternatives comme la tenue d'un journal manuscrit des informations qui seraient autrement partagées ou d'autres moyens de mettre en place des rappels pour prendre des médicaments ou faire de l'exercice.

Si vous soupçonnez qu'un appareil est utilisé à mauvais escient, documentez les faits dès à présent. Notre journal de la violence facilitée par la technologie est un outil pour documenter chaque événement. Ces journaux peuvent être utiles pour révéler des schémas et déterminer les prochaines étapes, et peuvent éventuellement servir à constituer un dossier si vous choisissez d'intenter des poursuites.

Vous pouvez également essayer d'accéder à des preuves par le biais de l'appareil ou de son appli ou compte. Vous pouvez également essayer d'entrer en contact avec le fabricant pour reprendre le contrôle d'un appareil ou de son compte. Il est également important de prendre des mesures pour renforcer la sécurité du réseau et du Wi-Fi. Pour plus d'informations, consultez notre document sur la sécurité Wi-Fi.

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 consulter hebergementfemmes.ca pour trouver une maison d'hébergement près de chez vous afin de discuter de vos options et de 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.

Adapté pour le Canada avec la permission du Safety Net Project de NNEDV, d'après leur ressource Connected Health and Medical Devices: Survivor Privacy Risks and Strategies.

Ce document fait partie du projet Sécurité technologique Canada d'Hébergement femmes Canada. Nous vous encourageons à visiter le site www.securitetech.ca pour trouver des informations et des ressources supplémentaires sur la violence facilitée par la technologie, la planification de la sécurité technologique et la préservation des preuves numériques. Ce document, ou toute partie de celui-ci peut être reproduit ou utilisé à condition de citer la source. Si vous souhaitez adapter le contenu, veuillez contacter Hébergement femmes Canada à l'adresse info@endvaw.ca.

Ce projet est rendu possible grâce au financement du ministère Femmes et Égalité des genres Canada (FEGC).

Femmes et Égalité des genres Canada | Women and Gender Equality Canada | Canada