Sécurité technologique Canada

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

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.

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.

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