deviner ou publiquement connus, ils n'assurent pas un niveau de sécurité suffisant. Il est donc indispensable de changer le mot de passe par défaut dès la première utilisation et d'utiliser un mot de passe suffisamment long et complexe pour sécuriser votre objet connecté. Ce conseil est également applicable à l'ensemble des appareils de votre réseau numérique.

3. Mettez à jour sans tarder vos objets connectés et les applications associées

« Pourquoi dit-on mot de passe et pas mot de passoire ? » – Vidéo réalisée en partenariat avec le groupe France Télévisions

Réalisez les mises à jour de sécurité de vos objets connectés et des applications qui peuvent leur être associées dès qu'elles sont disponibles pour éviter que des cybercriminels utilisent des failles de sécurité pour prendre le contrôle de l'objet ou vous dérober des informations personnelles sensibles. Si cela est possible, configurez votre objet connecté pour que les mises à jour se téléchargent et s'installent automatiquement.

En 2019, une petite fille de 3 ans confie à ses parents qu'une voix lui parle dans le baby-phone vidéo qu'ils ont installé dans sa chambre. Les parents s'aperçoivent que la caméra change toute seule d'orientation. Un pirate, qui avait pris le contrôle à distance de l'objet connecté, les observaient et parlait à l'enfant pour l'effrayer quand elle était seule.

4. Protégez vos informations personnelles

Pour protéger votre identité numérique et si votre objet connecté nécessite la création d'un compte en ligne, protégez-le par un mot de passe solide et différent de vos autres comptes. Ne communiquez que le minimum d'informations nécessaires (date de naissance aléatoire, âge approximatif, etc.). Utilisez le plus souvent des pseudonymes au lieu de vos noms et prénoms. Créez-vous, si possible, une adresse de messagerie (mail) spécifique pour vos objets connectés afin d'éviter de voir polluée votre adresse principale par des messages indésirables.

5. Vérifiez les paramètres de sécurité de vos objets connectés et de leurs applications

Vérifiez que l'objet ne permet pas à d'autres personnes de s'y connecter en vous assurant que la connexion avec un autre appareil (téléphone mobile, tablette, ordinateur, etc.) ou sur Internet ne peut se faire qu'au travers d'un bouton d'accès sur l'objet ou par l'utilisation d'un mot de passe. Par ailleurs, désactivez les fonctionnalités comme le partage des données sur les réseaux sociaux par exemple, si vous ne l'utilisez pas ou n'en avez pas besoin, pour réduire les risques de piratage et de fuite incontrôlée de vos données personnelles.

6. Éteignez systématiquement vos objets connectés lorsque vous ne les utilisez pas

Lorsque vos objets connectés ne sont pas ou plus en cours d'utilisation, pensez à les éteindre ou à les déconnecter pour réduire les risques de piratage, de vol de données ou d'intrusion malveillante.

7. Mettez à jour les appareils raccordés à vos objets connectés

Si vos objets connectés sont associés à d'autres appareils (téléphone mobile, tablette, ordinateur, etc.), effectuez également leurs mises à jour sans tarder pour éviter que des cybercriminels puissent accéder à ces appareils en utilisant une faille de sécurité et ainsi atteindre vos objets connectés. N'oubliez pas de mettre également à jour votre « box » Internet en la redémarrant régulièrement car c'est généralement par ce biais que vos objets se connectent à Internet.

En 2018, un casino s'est fait pirater la base de données de ses plus gros clients. Les pirates ont réussi à y accéder en passant par le