RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

ADOPTER LES BONNES PRATIQUES

SÉCURITÉ DES **OBJETS CONNECTÉS** (IoT)

Un objet connecté (*Internet of Things* ou *IoT* en anglais) est un matériel électronique connecté directement ou indirectement à Internet. C'est-à-dire qu'il est capable d'envoyer ou de recevoir des informations par Internet. Enceintes, montres, téléviseurs, réfrigérateurs, jouets, caméras, « baby-phones », etc., les objets connectés font aujourd'hui de plus en plus partie de notre vie numérique personnelle et professionnelle. Comme tout équipement informatique communicant, ces objets peuvent présenter des vulnérabilités susceptibles d'entraîner des risques comme leur piratage ou le vol d'informations personnelles. Souvent insuffisamment sécurisés, ils peuvent représenter le maillon faible de votre environnement numérique. **Voici 10 bonnes pratiques à adopter pour utiliser au mieux vos objets connectés en sécurité.**

1 AVANT L'ACHAT, RENSEIGNEZ-VOUS SUR L'OBJET CONNECTÉ

Informez-vous sur les caractéristiques de l'objet, son fonctionnement, ses interactions avec les autres appareils électroniques ou les données collectées lors de son utilisation. Vérifiez également que l'objet ne présente pas de failles de sécurité connues qui, si elles sont utilisées, pourraient permettre de prendre le contrôle de l'objet ou d'ouvrir une brèche dans votre environnement numérique et sur vos données. Pour cela, renseignez-vous auprès de sites Internet spécialisés, consultez le site Internet du fabricant ainsi que les avis de consommateurs qui peuvent fournir de précieuses informations.

2 MODIFIEZ LES MOTS DE PASSES PAR DÉFAUT DE VOS OBJETS CONNECTÉS

Les mots de passe, codes PIN, etc. générés par défaut par les fabricants sont généralement trop faibles : trop peu de caractères utilisés, faciles à 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. En savoir plus sur les mots de passe.

3 METTEZ À JOUR SANS TARDER VOS OBJETS CONNECTÉS ET LES APPLICATIONS ASSOCIÉES

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 savoir plus sur les mises à jour.

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.

EN PARTENARIAT AVEC :
MINISTÈRE DE L'INTÉRIEUR
AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

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.

8 SÉCURISEZ VOTRE CONNEXION WI-FI

Si vos objets connectés envoient ou reçoivent des informations par le biais de votre connexion Wi-Fi, il est essentiel de la sécuriser pour réduire les risques de piratage et de prise de contrôle à distance de vos objets. Pour cela, utilisez un mot de passe solide et vérifiez que votre connexion utilise le chiffrement en « WPA2 » qui est aujourd'hui la méthode de chiffrement du Wi-Fi la plus sûre.

9 LIMITEZ L'ACCÈS DE VOS OBJETS CONNECTÉS AUX AUTRES APPAREILS ÉLECTRONIQUES OU INFORMATIQUES

Pour limiter les risques de piratage, n'autorisez l'association (ou « appairage ») de vos objets connectés qu'aux seuls appareils nécessaires aux fonctionnalités dont vous avez besoin. Par exemple, la poupée connectée de votre enfant n'a pas forcément besoin de dialoguer avec votre réfrigérateur connecté. Si vous en avez la possibilité, il est également recommandé d'utiliser ses objets connectés sur un réseau distinct (réseau privé virtuel ou VLAN) des autres équipements informatiques de votre environnement.

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 observait et parlait à l'enfant pour l'effrayer quand elle était seule.

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 thermomètre connecté insuffisamment sécurisé d'un aquarium de l'établissement.

10 SUPPRIMEZ VOS DONNÉES ET RÉINITIALISEZ VOTRE OBJET LORSQUE VOUS NE VOUS EN SERVEZ PLUS

Si vous êtes amené à vous séparer de votre objet connecté (vente, panne…), et afin d'éviter que l'on puisse accéder à vos informations personnelles qu'ils peuvent contenir, effacez vos données sur l'objet connecté et supprimez le compte en ligne auquel il peut être associé. Si l'objet est associé à vos différents comptes en ligne comme vos comptes de réseaux sociaux, supprimez également cette association. Par ailleurs, réinitialisez l'objet dans ses paramètres par défaut (configuration usine) si cela est possible pour réduire les risques d'accès à des données personnelles qu'il pourrait contenir comme par exemple votre mot de passe Wi-Fi.

RETROUVEZ TOUTES NOS PUBLICATIONS SUR :
www.cybermalveillance.gouv.fr

Version 2.0