CLCV
CONSOMMATION
LOGEMENT ET
CADRE DE VIE
citoyens au quotidien

Objets connectés : 10 conseils pour protéger ses données personnelles

L'utilisation d'un objet connecté expose au risque du détournement des données personnelles qu'il collecte.
Afin de minimiser les risques, il convient de mettre en application dès l'achat des mesures de bon sens :

❶ Modifiez le mot de passe, ou le code PIN, de l'objet défini par défaut en sortie d'usine.

❷ Pensez à sécuriser les mots de passe de l'ensemble des éléments qui interviennent dans l'utilisation de l'objet connecté (le smartphone, le réseau WI-FI, le compte attaché à l'objet connecté).

❸ Utilisez un mot de passe « fort » constitué de lettres majuscules, minuscules et de chiffres. Une astuce pour retenir facilement son mot de passe consiste à :

. Mémorisez une phrase,
. Conservez-les initiales des mots,
. Choisissez une suite de chiffres ou une date importante pour vous,
. Alternez lettres et chiffres comme bon vous semble.

« Mon chéri est parti à St Nazaire » + 9 janvier 2004 donne : Mc09ep01aSN04.

❹ Mémorisez vos mots de passe et ne les stockez pas dans l'ordinateur, cela implique de ne pas accepter que le navigateur web enregistre les identifiants et mots de passe. Si vous ne pouvez vraiment pas les mémoriser, conservez les dans un lieu caché, à l'abri des regards.

❺ Recherchez sur la notice de l'objet les conditions d'accès aux données personnelles stockées et comment pouvoir les modifier et les supprimer.

❻ Vérifiez si le fabricant sort régulièrement des mises à jour de sécurité pour contrer les nouveaux risques de sécurité remontés par les utilisateurs.

Vous disposez d'un droit d'accès, de rectification et de suppression de vos données personnelles. Le professionnel doit vous indiquer un interlocuteur afin d'exercer ces droits. En cas de difficultés, vous pouvez adresser une réclamation auprès de la CNIL (www.cnil).

Mars 2019

❼ Réalisez systématiquement toutes les mises à jour de vos produits connectés mais également toutes les mises à jour de l'ensemble de votre système relié à internet.

❽ Evitez d'associer l'objet connecté à des réseaux sociaux et, si vous décidez de le faire, pensez à désactiver le partage automatique des données pour choisir au cas par cas ce que vous publiez sur lesdits réseaux sociaux.

❾ Eteignez l'objet quand il ne sert pas pour éviter d'envoyer des données sensibles sans en être pleinement conscient.

❿ Souvenez-vous, lorsque l'objet connecté nécessite l'ouverture d'un compte en ligne :

- ✓ de ne communiquer que le strict minimum des informations nécessaires au service,
- ✓ de se créer une adresse mail spécifique pour chaque objet,
- ✓ de sécuriser l'accès à ce compte en ligne par un mot de passe fort et différent de celui des autres comptes.

Avant de vous débarrasser d'un objet connecté, réinitialisez les paramètres d'usine si la fonction est disponible ou, à minima, effacez les données enregistrées sur l'objet. Supprimez également les comptes en ligne qui ne sont plus utilisés.

Mars 2019