# LA MINUTE DU PSIR

## SÉCURITÉ DES OBJETS CONNECTÉS

Noël approche et on peut se poser la question : **investir dans un objet connecté** (enceinte, montre, ampoule, thermostat, téléviseur, réfrigérateur, jouet pour adulte ou enfant, caméra, alarme, « baby-phone », etc.), **est-ce une bonne idée ?**

Les années passent et les scandales de sécurité et de vie privée se succèdent à un rythme qui ne semble pas réduire et semblent concentrer la plupart des problèmes sur ces objets.

**Voici 10 bonnes pratiques à adopter pour utiliser au mieux ces objets en toute sécurité :**

1. **Avant l'achat, renseignez-vous sur l'objet connecté** auprès de sites Internet spécialisés. Consultez le site Internet du fabricant ainsi que les avis des consommateurs, cela peut fournir de précieuses informations.
2. M**odifiez les mots de passes par défaut** de vos objets connectés dès la première utilisation. Ils sont généralement trop faibles et connus de tous. *Ce conseil est également applicable à l'ensemble des appareils de votre réseau domestique.*
3. **Mettez à jour sans tarder vos objets connectés et les applications associées.** Réalisez les mises à jour de sécurité. *Si cela est possible, configurez votre objet pour que les mises à jour se téléchargent et s'installent automatiquement.*
4. **Protégez vos informations personnelle** par un mot de passe solide et différent de vos autres comptes. *Ne communiquez que le minimum d'informations nécessaires.*
5. **Vérifiez les paramètres de sécurité de vos objets connectés et de leurs applications** en vous assurant que la connexion avec un autre appareil 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.
6. **Éteignez systématiquement vos objets connectés lorsque vous ne les utilisez pas**. Cela limite les risques de piratage.
7. **Mettez à jour les appareils raccordés à vos objets connectés** pour éviter que des cybercriminels puissent y accéder en utilisant une faille de sécurité. *N'oubliez pas de mettre à jour votre « box » internet en la redémarrant régulièrement.*
8. **Sécurisez votre connexion Wi-fi**. Utilisez un mot de passe solide et vérifiez que votre connexion utilise un chiffrement en « WPA2 » qui est aujourd'hui la méthode de chiffrement 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.*
10. **Supprimez vos données et réinitialisez votre objet lorsque vous ne vous en servez plus**. Si vous êtes amené(e) 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.

DIFFICULTÉ

THÉMATIQUE

SÉCURITÉ INFORMATIQUE

PERSONNES CONSEILLÉES

*Pour en savoir plus, cliquer ici*

***Recommandations de sécurité relatives aux objets connectés***

***298 Ko***

cnrs
université lumière lyon 2
Maison de l'Orient et de la Méditerranée Jean Pouilloux