CYBERMALVEILLANCE : POURQUOI ET COMMENT SÉCURISER SES OBJETS CONNECTÉS ? AVEC CYBERMALVEILLANCE.GOUV.FR

Date de publication : **27/10/2021 - Internet/multimédia**

Nicolas : "J’ai entendu dire qu’il y avait des risques de piratage sur les enceintes connectées ? Est-ce vrai ?".

Malheureusement oui Nicolas. Comme tout équipement informatique communicant, les objets connectés peuvent présenter des failles de sécurité. D'autant qu'ils sont parfois insuffisamment sécurisés.

Un objet connecté est un appareil électronique connecté à Internet directement, ou indirectement, via une liaison Wi-Fi, Bluetooth ou NFC (Near Field Communication), possède une portée très limitée, de quelques centimètres seulement, et un faible débit. Par exemple. Il peut s'agir d'une montre, d'une enceinte, ou d'un téléviseur connecté.

Pourquoi les sécuriser ?

Ces appareils sont reliés à votre réseau domestique. S'ils arrivent à s'y connecter, les pirates peuvent donc avoir accès à des informations personnelles, ou stocker des données frauduleuses sur vos appareils.

Peut-on vraiment se fier à ce genre d'appareil ?

Avant l'achat, renseignez-vous sur l'objet. Notamment sur ses interactions avec les autres appareils électroniques ou les données collectées lors de son utilisation. Vérifiez qu'il ne présente pas de failles de

sécurité connue. Pour cela, rendez-vous sur le site web du fabricant, sur des sites spécialisés, et consultez les avis d'utilisateurs.

Et une fois l'objet acheté, que peut-on faire pour le sécuriser ?

Pensez à modifier les mots de passe par défaut. En effet, ces derniers sont souvent trop faibles : faciles à deviner ou publiquement connus.
Utilisez un mot de passe suffisamment long et complexe, avec des chiffres et des majuscules.
Réalisez aussi régulièrement les mises à jour de sécurité ainsi que celle de tous les appareils et applications associées.

Et comment protéger les informations personnelles souvent collectées par ces objets ?

Si votre objet connecté nécessite la création d'un compte en ligne, créez un mot de passe solide et différent de vos autres comptes.
Ne donnez pas plus d'information personnelle que nécessaire : fournissez par exemple une date de naissance aléatoire, ou encore un pseudonyme.

Enfin, éteignez bien vos appareils lorsque vous ne les utilisez pas ! Et pour vous aider à sécuriser vos appareils et trouver de l'assistance en cas de piratage, rendez-vous sur le site Cybermalveillance.gouv.fr.

En résumé :

- renseignez-vous sur la sécurité de l'objet,
- changez le mot de passe par défaut,
- choisissez un mot de passe solide et différents des autres comptes,
- éteignez bien vos appareils.
