

Les produits intelligents peuvent améliorer notre quotidien, mais ils posent aussi des risques.

De plus en plus de personnes achètent pour leur domicile des produits intelligents connectés à Internet. Ces appareils connectés peuvent apporter d'énormes bénéfices, notamment sur les plans de l'efficacité, de la praticité et des connaissances, ainsi que la possibilité de contrôler les appareils à distance. Cependant, avec ces bénéfices viennent aussi des risques.

Découvrez nos conseils pour une connexion intelligente !



S'INFORMER sur les éventuels risques liés à la sécurité et à la confidentialité avant d'acheter

Renseignez-vous sur le produit sur internet en consultant les évaluations ou articles de presse qui mettent en évidence des problèmes de sécurité et de confidentialité. Voyez si vous pouvez sécuriser votre appareil en changeant de mot de passe et en ajustant les paramètres de confidentialité. Vérifiez que l'appareil reçoit des mises à jour logicielles régulières pour combler les éventuelles failles de sécurité.



METTRE EN PLACE un mot de passe fort et unique pour chaque appareil

Les mots de passe génériques par défaut sont faciles à trouver et permettent aux pirates d'accéder à vos appareils. Créez un mot de passe fort et unique pour chaque appareil et service et pour le routeur de votre foyer. Plus le mot de passe est long, mieux c'est ; mélanger les majuscules, les minuscules, les chiffres et les caractères spéciaux pour le sécuriser davantage.



AJUSTER LES PARAMÈTRES pour un maximum de sécurité et de confidentialité

De nombreux appareils et services sont fournis avec, par défaut, une protection de sécurité minimale et récupèrent une quantité non négligeable d'informations importantes à votre sujet, alors ajustez vos paramètres pour renforcer votre sécurité et votre confidentialité. Prévoyez également de réinitialiser votre appareil régulièrement. Si des pirates parviennent à accéder à votre appareil, un code malveillant sera souvent stocké dans sa mémoire ; une réinitialisation permettra de l'effacer. Si vous découvrez un incident qui pourrait nuire à votre appareil, rendez-vous sur le site du constructeur ou contactez le revendeur à qui vous l'avez acheté pour connaître la procédure à suivre.



RÉGULIÈREMENT METTRE à jour le logiciel

Si l'appareil ou l'application peut se mettre à jour automatiquement, activez cette fonctionnalité. Apprenez à vérifier si des mises à jour logicielles sont disponibles pour chacun de vos appareils et faites-le une fois par mois. La plupart des fabricants déploient des mises à jour quand ils sortent un correctif pour combler des failles de sécurité. Acceptez également les mises à jour des applications de votre téléphone portable qui contrôlent votre appareil.



TOUJOURS DÉSACTIVER les fonctionnalités inutiles et éteindre votre appareil quand il ne sert pas

Beaucoup de fonctionnalités de votre appareil continuent à vous surveiller même quand vous ne le soupçonnez pas ou n'en avez pas besoin. Pour l'éviter, désactivez les appareils photo, microphones et applications de géolocalisation quand vous n'êtes pas en train de les utiliser. Et quand vous n'utilisez pas votre appareil, éteignez-le.