



Comment se prémunir des risques liés aux caméras connectées

Les caméras connectées à Internet gagnent en popularité grâce à leurs nombreux usages, comme surveiller un bébé dans sa chambre ou voir qui se présente à la porte d'entrée.

Cependant, ces appareils comportent aussi des risques sérieux pour la vie privée.

Il est étonnamment facile pour des inconnus d'accéder aux images captées par ces caméras.

Ces appareils, comme les moniteurs pour bébé ou les systèmes de sécurité, peuvent également être piratés, exposant des données sensibles sur vos déplacements ou votre emplacement.

Heureusement, des mesures simples peuvent réduire ces risques.

Modifier le mot de passe par défaut est essentiel : ce dernier est souvent publié en ligne et représente une porte d'entrée facile pour les pirates. Choisissez un mot de passe sûr, activez l'authentification en deux étapes, si possible.

Évitez d'utiliser le même mot de passe pour plusieurs appareils. Désactivez toujours les anciens mots de passe après en avoir créé de nouveaux.

Protégez également votre routeur en modifiant son mot de passe et, si nécessaire, créez un réseau pour invités réservé à vos appareils connectés. Ainsi, vos ordinateurs et téléphones resteront isolés en cas de faille.

Pour renforcer encore votre sécurité, veillez à couvrir la caméra de votre ordinateur portable ou de votre tablette lorsqu'elle n'est pas utilisée. Utilisez une note adhésive ou un cache-caméra.

Configurez vos appareils pour qu'ils vous avertissent lorsque la caméra ou le microphone est activé, grâce à un voyant, par exemple.

Avant d'acheter une caméra connectée, renseignez-vous sur ses caractéristiques de sécurité et vérifiez si elle a fait l'objet de publications relatives à des vulnérabilités. Évitez les produits dont le fabricant ne fournit pas d'informations claires sur la confidentialité. Assurez-vous également que le micrologiciel de l'appareil peut être mis à jour, car ces mises à jour corrigent souvent des failles de sécurité.

Pour une protection supplémentaire, limitez l'utilisation de ces appareils dans des pièces privées comme la chambre ou la salle de bains.

Surveillez les caméras extérieures pour qu'elles ne captent pas des informations sensibles comme des numéros de rue ou de plaques d'immatriculation. Si des enfants utilisent ces appareils, soyez particulièrement vigilant et désactivez les fonctions dont vous n'avez pas besoin.

Enfin, restez prudent en ligne : évitez de cliquer sur des liens suspects qui pourraient introduire des virus ou donner un accès non autorisé à vos appareils.

En adoptant ces pratiques simples, vous réduirez considérablement les risques liés à l'utilisation de caméras connectées tout en profitant de leurs avantages.

UFC QUE CHOISIR TOULON. Tous droits réservés.