Comment utiliser les réseaux wifi en toute sécurité

Réseaux sans fil **publics**

Les réseaux sans fil sont partout, mais leur utilisation comporte des risques, car ils peuvent être ciblés et attaqués à distance. Ils sont done vulérables aux cyberattaques.

Le réseau sans fil que vous utilisez à la maison est privé et peut être étroitement contrôlé. Le réseau sans fil que vous utilisez dans un café ou un aéroport est public. Vous risquez davantage de subir une cyberattaque lorsque vous utilisez un réseau public.

Voici quatre précautions à prendre lorsque vous utilisez un réseau sans fil public:

Utiliser des réseaux sans fil légitimes

Il peut arriver que des fraudeurs créent un faux réseau wifi qui ressemble au réseau que vous recherchez.

Utiliser un réseau privé virtuel (RPV)

Un RPV chiffre les données qui se rendent à votre appareil ou qui en sortent, ce qui rend le vol de vos renseignements plus difficile pour les fraudeurs.

Ne pas accéder à des renseignements personnels

Faites attention aux renseignements que vous partagez sur un reseau sans fil public, et évitez certaines tâches comme des transact.

Demeurer sur des sites https

« Https » est la version sécurisée de l'adresse http du site Web que vous visitez. Le« s » signifie « sécurise », et toutes les communications entre votre navigateur et le site Web sont chiffrées.

Comment utiliser les réseaux wifi en toute sécurité

Réseaux sans fil **privés**

Sécurisez votre réseau domestique pour une utilisation personnelle et avec vos appareils connectés à Internet (IdO). Vous devez d'abord sécuriser votre routeur wifi auprès de votre fournisseur de services wifi. Cet appareil contrôle les dispositifs qui peuvent se connecter à votre réseau domestique.

Tout d'abord, accédez au site Web de votre fournisseur d'accès Internet, ou encore utilisez l'adresse IP indiquée dans le manuel de votre appareil. Vous devriez trouver une section sur la gestion du réseau wifi ou vous pourrez apporter les changements suivants:

Rendre le réseau indétectable

Il est plus difficile pour les pirates informatiques d'exploiter les vulnérabilites potentielles de votre réseau lorsque vous changez son nom. N'utilisez pas votre nom, votre adresse résidentielle ou d'autres renseignements qui pourraient permettre de vous identifier.

Modifier le mot de passe par défaut

Remplacez-le par un mot de passe fort et unique, composé d'au mains huit caractères (de préférence beaucoup plus long) et d'un mélange de chiffres, de lettres et de caractères spéciaux.

Créer un réseau d'invités

Utilisez le réseau d'invités pour les appareils non fiables comme ceux de vos visiteurs à domicile et de vos appareils personnels pour maison intelligente.

S'assurer que le réseau est chiffré

Utilisez les paramètres de connexion sans fil WPA2 OU WPA3.

Installer les correctifs du micrologiciel

Activez les mises à jour automatiques de taus les appareils. Si les mises à jour automatiques ne sont pas possibles, ouvrez régulièrement une session sur le compte de votre fournisseur pour vérifier si des mises à jour sont offertes.