



Août

# Maisons connectées

## Chez soi en toute sécurité

### Des objets, des objets et encore des objets

Les maisons intelligentes sont de plus en plus courantes de nos jours, avec divers appareils de l'Internet des objets (IdO) – téléviseurs, thermostats, ampoules, appareils ménagers et même les prises électriques accessibles à partir d'un téléphone intelligent. Ces formidables appareils, permettent aux gens de rester connectés et en contrôle de leur maison. Mais avoir un accès facile à divers appareils facilite également l'accès aux renseignements personnels pour les pirates informatiques. Pour demeurer connecté en toute sécurité, voici quelques éléments à garder en tête.

### Vulnérabilités des maisons intelligentes

- **Réseaux sans fil et routeurs non sécurisés** – Les pirates peuvent passer par des réseaux sans fil et des routeurs non sécurisés pour pirater les maisons intelligentes.
- **Appareils à sécurité minimale** – De nombreux appareils IdO ne sont pas conçus pour être mis à jour, ce qui les rend vulnérables aux cyberattaques.
- Les caractéristiques de **sécurité** ne sont pas toujours **activées** par défaut.

### Meilleures stratégies pour sécuriser vos appareils IdO et votre maison intelligente

- **Connectez les appareils IdO à un câble Ethernet**, si possible, plutôt qu'à un réseau sans fil. Autrement, assurez-vous que ce réseau est protégé par un mot de passe.
- Modifiez le et nom le **mot de passe par défaut** de votre réseau sans fil et de votre routeur. Les mots de passe par défaut sont faibles et faciles à pirater.
- **Limitez-vous aux appareils IdO essentiels** dans votre maison plutôt qu'aux appareils que vous voulez ) – considérez les risques de piratage de chaque appareils. Quel niveau de risque êtes-vous prêt à assumer?
- Allez vers des **marques et produits de confiance**. Consultez les renseignements et les commentaires sur les produits en ligne. Assurez-vous que les appareils intègrent des caractéristiques de sécurité.
- **Utilisez l'authentification à deux facteurs**, si disponible – cette mesure renforce la sécurité. En plus d'un nom d'utilisateur et d'un mot de passe, une deuxième méthode de vérification s'ajoute, comme un code envoyé par téléphone.
- Gardez vos **appareils et applications à jour**. Installez les dernières mises à jour sur vos appareils et applications.



Pour plus d'informations : [www.ecno.org/cyber-sensibilisation](http://www.ecno.org/cyber-sensibilisation)

© Imprimeur du Roi pour l'Ontario 2023

Ontario