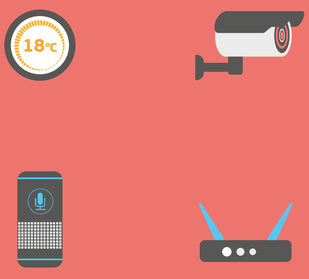
Conseils pour assurer la cybersécurité de votre foyer

L'Internet des Objets, IdO, est le réseau de tous les appareils qui peuvent être connectés à l'internet. Vous penserez automatiquement à votre ordinateur portable ou à votre télévision intelligente, mais l'IdO comprend également, par exemple, les consoles de jeu, les assistants domestiques, l'alarme de votre maison ou le moniteur de votre bébé.

Et même si ces appareils peuvent améliorer la qualité de notre vie et de notre travail, rappelez-vous que tout ce qui est connecté à l'internet peut être vulnérable aux attaques de pirates informatiques.Voici quelques mesures que vous pouvez prendre pour protéger votre foyer.



1. Sécurisez tous vos appareils

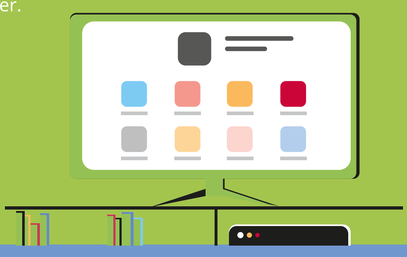
Assurez-vous que tous vos appareils sont protégés par des mots de passe robustes ou configurez une authentification à deux facteurs (A2F), disponible sur la plupart des appareils IdO.

Vous devriez également modifier le mot de passe et le nom de réseau fournis par défaut. Il est important de ne pas inclure dans le nom de votre réseau un élément qui donne des informations sur votre domicile ou votre famille, par exemple votre nom ou votre adresse.

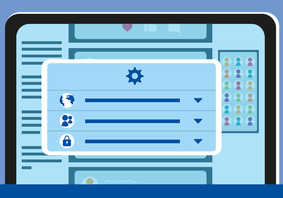
2. Veillez à la sécurité de vos applications

Télécharger des applications directement à partir du magasin d'applications officiel (Google Play, Apple App Store, etc.) est la façon la plus sûre de vous les procurer. En cliquant sur un lien aléatoire pour télécharger une application, vous pourriez infecter votre appareil.

Réfléchissez mûrement aux informations et autorisations que vous donnez avant d'installer une application. Passez régulièrement vos applications en revue, et supprimez ce qui est inutile.



3. Vérifiez les paramètres de confidentialité de vos comptes réseaux sociaux



Ouvrez les paramètres de confidentialité de votre compte et modifiez-les pour qu'ils vous conviennent.

Réfléchissez attentivement aux informations à inclure dans votre profil. Les plateformes peuvent vous demander des informations qu'il n'est pas nécessaire de leur fournir.

4. Sélectionnez l'option de mise à jour automatique sur tous vos appareils et sauvegardez vos données

Les appareils IdO sont vulnérables aux attaques des pirates informatiques. Disposer des dernières mises à jour est une condition essentielle de la sécurité de vos appareils. En sélectionnant la mise à jour automatique, vous n'aurez plus à vous souvenir de le faire vous-même.

Veillez à archiver des copies de tout ce qui est important pour vous, par exemple vos photos ou vos contacts, soit sur un support hors ligne, soit dans le cloud.

5. Séparez bien vos outils de travail et vos appareils privés

Nous vous conseillons d'utiliser des appareils séparés pour le travail et la vie privée. L'appareil que vous utilisez pour le travail ne doit servir qu'à des fins professionnelles, ce qui réduira les dommages en cas d'atteinte à la sécurité.

Si vous devez partager un appareil, veillez à ce que chaque utilisateur ait son propre profil.

enisa EUROPEAN UNION AGENCY FOR CYBERSECURITY

EUROPEAN CYBER SECURITY MONTH

#CyberSecMonth

#ThinkB4UClick