Votre interlocuteur AXA

AXA Prévention

Créée en 1984, **AXA Prévention** est une association à but non lucratif. Sa mission est d'étudier et de mettre en œuvre toutes les mesures de nature à développer la culture de prévention des Français afin de prévenir et réduire les risques auxquels ils sont exposés en santé, sur la route, à la maison, devant les écrans, dans le milieu professionnel et face au réchauffement climatique.

ASSO VICA

ASsociation de SOutien aux VIctimes de Cyber Attaques

L'ASSociation de SOutien aux VIctimes de Cyber Attaques (ASSOVICA) est une association à but non lucratif créée en 2023 par un collectif composé d'expert(e)s techniques et non techniques afin d'aider et accompagner au mieux les victimes d'actes de cybermalveillance. L'une de ses missions est d'apporter aide et soutien aux victimes professionnelles des cyber attaques ciblant les organisations.

AXA Prévention : Association à but non lucratif - Loi 1901 - 313 Terrasses de l'Arche - 92727 Nanterre Cedex - service.axaprevention@axa.fr

Réf. : 2006460 0625 - CARJOCA - Crédit photo : Adobe Stock.

AXA Prévention

Limiter ma surface d'exposition aux risques cyber

ASSO VICA

ASsociation de SOutien aux VIctimes de Cyber Attaques

Retrouvez tous nos conseils et services de prévention sur : **axaprevention.fr**

Limiter ma surface d'exposition aux risques cyber

Aujourd'hui, dans notre quotidien, au travail comme dans notre vie privée, les objets dit « connectés » nous accompagnent partout.

Pour surveiller notre maison, nous aider à pratiquer un sport, retrouver nos clés, ou tout simplement nous divertir.

Pour réduire les risques de comportement malveillant, il est essentiel de limiter l'exposition de ces appareils.

> **Plus vous avez d'appareils connectés, plus vous offrez de points d'entrée potentiels aux cyberattaques.**

La clé est de rester vigilant et de ne pas tout brancher sans discernement, tout en assurant une maintenance régulière de vos dispositifs pour garantir leur sécurité, et donc la vôtre.

Découvrez comment !

Pour limiter votre surface d'exposition aux risques cyber, il est crucial de suivre quelques principes fondamentaux :

- Tout d'abord, réduire le nombre d'appareils connectés à votre réseau. Chaque appareil supplémentaire représente une probable voie d'accès.
- S'assurer que tous vos appareils et logiciels sont à jour avec les derniers correctifs de sécurité. Les mises à jour corrigent souvent des vulnérabilités qui pourraient être exploitées par des attaquants. Il est également important d'utiliser des mots de passe forts et uniques pour chaque appareil et service. Les mots de passe doivent être complexes et être différents pour chaque compte afin de limiter les risques en cas de compromission. Il existe des générateurs de mots de passe gratuits pour vous y aider.
- Il est primordial de fractionner votre réseau en créant des sous-réseaux pour isoler les appareils critiques des autres : cela limite la propagation d'une éventuelle attaque.
- Enfin, sensibiliser les utilisateurs aux bonnes pratiques de cybersécurité. Une formation régulière peut aider à prévenir les erreurs humaines, qui sont souvent à l'origine des failles de sécurité.

Quelles actions concrètes ? Un bref récapitulatif :

- Déconnecter ce qui n'est pas nécessaire : n'activer que les appareils connectés indispensables à votre activité.
- Protéger les objets connectés : changer les mots de passe par défaut et mettre à jour les firmwares (logiciels internes) régulièrement.
- Utiliser des mots de passe à 12 caractères ou plus, qui ne comprennent pas une suite de chiffre logique (par exemple 123456) ou un mot du dictionnaire.
- Identifier les composants vulnérables : faire un audit pour repérer et sécuriser les équipements susceptibles d'être exploités.
- Segmenter les réseaux : éviter que les objets connectés partagent le même réseau que vos systèmes critiques.
- Éduquer les utilisateurs : expliquer les risques liés à chaque appareil connecté pour un usage plus conscient.