Votre interlocuteur AXA

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

ASSociation de SOutien aux VIctimes de Cyber Attaques

ASSOVICA apporte 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. : 2006459 1224 - Solutions Graphiques - Crédit photo : Adobe Stock.

AXA Prévention

Vous préparer mentalement avec vos équipes à affronter un acte de cybermalveillance

ASSO VICA
ASsociation de SOutien aux VIctimes de Cyber Attaques

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

Vous préparer mentalement avec vos équipes à affronter un acte de cybermalveillance

Faut-il se poser la question suivante: Serai-je un jour visé par une cyberattaque?

Que ce soit du phishing, un rançongiciel, une usurpation d'identité, un appel, un sms, ou encore un mail frauduleux, la question n'est plus de savoir si l'on sera attaqué un jour, mais de savoir quand et comment réagir.

Comme pour des secouristes lors d'un accident de la route, les premières minutes sont primordiales, les réactions doivent être rapides, justes et coordonnées.

Ceci demande une certaine préparation pour ne pas impacter la vie de l'entreprise et de ses collaborateurs.

Quelques règles de base:

- Comprendre que toutes les organisations, quels que soient leur but et taille, peuvent être ciblées (personne libérale, artisan, TPE, PME, grand groupe, associations, hôpitaux…).
- Intégrer les bonnes pratiques de cybersécurité dans la culture de l'entreprise. Chaque collaborateur doit se sentir concerné par la sécurité des systèmes et des données.
- Réaliser régulièrement des audits pour identifier les problèmes liés au système informatique dans sa globalité ou des comportements humains.
- Élaborer un plan clair qui définit les étapes à suivre en cas d'attaque, les rôles des équipes, ainsi que les contacts clés (experts externes, assurances, police, gendarmerie…).
- Être en mesure de communiquer de manière claire et efficace avec les collaborateurs, les différents partenaires et les clients lors d'une crise afin de limiter l'impact sur l'organisation du travail.

Se préparer :

- Organiser des exercices pratiques de réponse à des cyberattaques (ex. phishing, arnaque au président…) pour tester les plans d'urgence et préparer les équipes.
- Veiller à ce que tous les logiciels et matériels soient à jour pour minimiser les risques liés aux vulnérabilités connues.
- Cadrer une politique stricte de gestion des accès, comme le principe du moindre privilège, pour limiter les dommages potentiels en cas de compromission.
- Effectuer des sauvegardes fréquentes des données critiques, les stocker de manière sécurisée et tester régulièrement leur restauration.
- Travailler avec des consultants en cybersécurité pour renforcer ses défenses et répondre efficacement en cas de cybermalveillance. Prendre un contrat d'assurance en lien avec la cyberprotection.
- Maintenir une formation régulière des collaborateurs pour les tenir informés des nouvelles menaces et des moyens de s'en prémunir.
- Documenter les incidents et les leçons apprises pour améliorer les processus et réduire les risques futurs.