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. : 2006458 0625 - CAR/OCA - Crédit photo : Adobe Stock.

AXA Prévention

Les conséquences sociales d'une cyberattaque

ASSO VICA

ASsociation de SOutien aux VIctimes de Cyber Attaques

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

Les conséquences sociales d'une cyberattaque

Au fait, une cyberattaque, c'est quoi exactement ?

Une cyberattaque est une action malveillante visant à endommager, voler, exposer, modifier ou détruire des informations ou des systèmes informatiques via un accès non autorisé.

Ces attaques peuvent être menées par des individus, des groupes coordonnés, des organisations criminelles ou même des États.

Les motivations derrière ces attaques peuvent être variées, incluant des raisons pécuniaires, politiques, voire parfois personnelles.

Les conséquences psychosociales d'une cyberattaque vont bien au-delà des simples pertes financières ou techniques.

Elles affectent profondément les individus, les administrations et les entreprises, créant des perturbations parfois à long terme.

Il est crucial d'intégrer une approche humaine dans la gestion des cyberattaques, en tenant compte de leur impact psychologique et social pour consolider la résilience individuelle comme collective.

Conséquences sur les individus

- Stress et anxiété : peur de l'exposition des données personnelles.
- Perte de confiance : envers les systèmes et les institutions.
- Impact mental : troubles du sommeil, dépression, voire syndrome de stress post-traumatique.
- Baisse de productivité : perturbations opérationnelles.
- Climat de méfiance : impact sur la cohésion des équipes.
- Réputation dégradée : pertes à long terme.
- Érosion de la confiance dans les institutions publiques.
- Phobie numérique : réticence à utiliser les technologies.

Comment accompagner vos collaborateurs après une cyberattaque ?

- En premier lieu : se rapprocher des autorités pour déposer plainte. Ne pas hésiter à proposer aux salariés de vous accompagner s'ils veulent témoigner.
- Proposer des services de consultation avec des psychologues spécialisés pour aider les collaborateurs à gérer leur stress et leurs émotions.
- Organiser des sessions où les collaborateurs peuvent partager leurs expériences et se soutenir mutuellement.
- Formations post-incident : proposer des ateliers pour aider les collaborateurs à comprendre ce qui s'est passé et comment se protéger à l'avenir.
- Plan de suivi : élaborer un programme à long terme pour surveiller et soutenir la santé mentale des collaborateurs.
- Les unités médico-judiciaires (UMJ) peuvent offrir des consultations pour les victimes de violences. Ces consultations peuvent aider à établir des preuves pour des actions judiciaires, l'orientation vers ce service se fait en commissariat ou en gendarmerie.
- Organiser des entretiens individuels pour évaluer la situation du point de vue du collaborateur, couplés à une amélioration continue de la qualité de vie au travail.