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.

ASSOVICA
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.

Réf. : 2006176 1024 - Solutions Graphiques - Crédit photo : Adobe Stock.

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

AXA Prévention

# Se préserver des attaques par Ingénierie sociale

ASSOVICA
ASsociation de SOutien aux VIctimes de Cyber Attaques

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

# Se préserver des attaques par ingénierie sociale

## Qu'est-ce que l'ingénierie sociale ?

L'ingénierie sociale en matière de cybercriminalité regroupe l'ensemble des techniques psychologiques pour manipuler les individus et les inciter à divulguer des informations sensibles, propager des programmes malveillants ou octroyer un accès à des systèmes contrôlés.

## Comment fonctionne l'ingénierie sociale ?

- Le cybercriminel collecte tout d'abord des informations sur sa cible (personne ou entreprise) à la recherche de faiblesses ou de points d'entrée potentiels afin de s'infiltrer en établissant une relation d'un certain niveau de confiance avec elle.
- Puis il passe à l'attaque en effectuant des demandes spécifiques (identifiants de connexion, données sensibles ou accès à des environnements). Il joue sur les émotions pour manipuler la victime en utilisant le registre de la crainte, la curiosité, l'envie, l'autorité.
- Après avoir obtenu ce qu'il cherchait, l'attaquant fait disparaître les traces de sa présence pour éviter d'être détecté.

## Les fondamentaux

1. Sensibiliser régulièrement les employés aux menaces d'ingénierie sociale en rappelant souvent que tout ce que l'on publie peut être utilisé par un cybercriminel.
2. Vérifier systématiquement l'identité de toute personne qui demande des informations sensibles ou une opération impactante pour l'entreprise.
3. Ne jamais effectuer d'opérations sensibles sans s'assurer par un autre moyen de communication de l'identité du donneur d'ordre.
4. Ne jamais cliquer sur des liens ou ouvrir des pièces jointes particulièrement attirants provenant de sources non vérifiées ou inattendues.
5. Signaler immédiatement toute tentative suspecte ou communication très inhabituelle au responsable de l'informatique.

### Actions à mettre en œuvre

- Mettre en place des formations régulières sur la cybersécurité pour renforcer la vigilance face aux tentatives d'ingénierie sociale.
- Développer des procédures internes pour valider les demandes de transfert de fonds ou de partage d'informations sensibles.
- Utiliser l'authentification à deux facteurs (2FA) pour sécuriser l'accès aux serveurs et aux données confidentielles.
- Instaurer une culture de la méfiance face aux communications imprévues ou pressantes.
- Mettre en œuvre des simulations d'attaques de phishing pour tester et améliorer la capacité de détection des employés.