

# L'importance de la sensibilisation des salariés pour les PME

Dans une entreprise, la prévention contre les risques cyber ne peut pas se limiter à des mesures d'ordre technique et organisationnel. Celles-ci sont importantes, certes, mais pour une approche globale du problème de la cybersécurité, elles doivent être accompagnées de mesures de formation et de sensibilisation (awareness). Tous les collaborateurs de l'entreprise doivent en effet être en mesure de bien utiliser les outils mis à leur disposition et connaître les règles de sécurité à respecter au travail.

La sensibilisation des salariés des PME passe par un certain nombre de points essentiels :

- création de guides d'utilisation faciles à mettre en œuvre
- organisation régulière de formations et campagnes de sensibilisation à l'attention des salariés
- utilisation de différents canaux et outils de communication pour atteindre l'ensemble des collaborateurs.
- exhortation des salariés à signaler les anomalies, infractions, etc.

## Pourquoi la sensibilisation est-elle si importante dans une PME?

Il suffit de jeter un œil sur les statistiques pour se rendre compte à quel point le facteur humain est déterminant pour le succès d'une cyberattaque. Lors des attaques [d'ingénierie sociale](https://www.ebas.ch/fr/ingenierie-sociale-social-engineering/) ou de [phishing](https://www.ebas.ch/fr/le-phishing/) par exemple, la personne humaine est manipulée pour divulguer des données sensibles ou effectuer une action involontaire. Des rapports de suivi rédigés par des entreprises diverses montrent qu'il ne suffit pas de sommer les collaborateurs d'appliquer telle ou telle mesure de sécurité. En effet, ils les appliqueront d'autant mieux et d'autant plus facilement qu'ils en comprendront l'importance et le but.

Pour élever le niveau de conscience des collaborateurs en termes de sécurité informatique et en faire une priorité au sein de l'entreprise, il convient d'organiser des activités de sensibilisation destinées à l'ensemble du personnel. À ce propos, il existe plusieurs stratégies permettant de forger une culture de la sécurité au sein d'une entreprise. Pour un succès durable, il est essentiel d'adapter la communication au groupe cible et de répéter régulièrement les messages.

## Comment sensibiliser les salariés d'une PME?

Il est recommandé d'élaborer une stratégie de sensibilisation au sein de l'entreprise afin de minimiser les coûts et de maximiser les résultats. Indépendamment de la quantité de ressources mises à disposition pour la réaliser, ce qui compte, c'est que les activités soient le mieux coordonnées et harmonisées possible. Dans ce contexte, il est essentiel que l'équipe dirigeante soutienne toutes les activités de sensibilisation et donne l'exemple au reste des salariés.

Voici quelques exemples d'activités qui permettent d'améliorer la sensibilisation dans les PME :

- **Organisation de formations, séminaires, ateliers, etc.:** la formation continue des collaborateurs sur ces sujets leur permet de rester au courant sur les dernières évolutions.
- **Communication interne:** échanger régulièrement sur les nouveautés, les changements ou les informations importantes favorise la prise de conscience et la compréhension des collaborateurs.
- **Promouvoir la culture du feedback:** il est important que les collaborateurs sachent à qui s'adresser ou disposent d'une plateforme pour signaler des anomalies ou toute entorse aux règles de l'entreprise, mais aussi pour exprimer leurs doutes ou préoccupations, poser leurs questions et faire des suggestions.
- **Faire appel à des experts externes:** il peut être utile d'inviter des prestataires externes spécialisés dans les thèmes de la sécurité informatique, pour bénéficier de leurs connaissances plus approfondies.
- **Mettre en place une plateforme de sensibilisation:** en tant qu'entreprise, vous avez également la possibilité d'adhérer à une plateforme d'awareness afin de faciliter la sensibilisation parmi les collaborateurs.
- **Intégrer l'awareness dans la culture d'entreprise:** la sensibilisation ne doit pas se limiter à une action ponctuelle. Au contraire, celle-ci doit être intégrée dans les processus de travail quotidiens et dans la culture de l'entreprise.

Pour une entreprise, la sensibilisation de ses salariés doit être vue comme un investissement pour l'avenir, qui lui permet non seulement de se protéger contre les risques juridiques et d'atteinte à sa réputation en cas de cyberattaque, mais aussi de favoriser un environnement de travail positif tout en augmentant la productivité. Dans un monde toujours plus numérisé, une solide culture de la sécurité représente un atout décisif pour une entreprise.

### En savoir plus

Le [manuel sur la sécurité de l'information \(https://www.sihb.ch/\)](https://www.sihb.ch/) est un ouvrage de référence et fournit, dans sa partie consacrée à la sensibilisation des collaborateurs, de bonnes pistes de réflexion avec des exemples éclairants. (Les personnes ayant participé à la [formation pour les PME \(https://www.ebas.ch/fr/formation-pour-les-pme/\)](https://www.ebas.ch/fr/formation-pour-les-pme/) bénéficient d'une réduction de 30% sur l'achat de ce manuel et peuvent le commander dès maintenant au prix préférentiel de CHF 68.— (frais d'envoi non compris.)

«eBanking – en toute sécurité!» propose également aux [PME une formation en ligne \(https://www.ebas.ch/fr/formation-pour-les-pme/\)](https://www.ebas.ch/fr/formation-pour-les-pme/), pour leur exposer les principales mesures techniques et organisationnelles à mettre en œuvre.

*Dans le contexte de la sécurité de l'information, le terme « sensibilisation » (ou « awareness » en anglais) fait référence au niveau de conscience que peuvent avoir les salariés d'une entreprise vis-à-vis des risques liés à la cybersécurité, et à leur capacité à adopter les bons comportements face à ces menaces.*