

Sensibiliser et Former

Pourquoi est-il nécessaire de sensibiliser à la cybersécurité ?

Les menaces cyber ciblant les acteurs de la santé sont en augmentation et profitent principalement du manque de vigilance des employés ou de l'erreur humaine via des tentatives de phishing ou d'hameçonnage.

Il est donc impératif de souligner **l'urgence de sensibiliser et de former** les employés à la cybersécurité afin de réduire les risques cyber et donc de réduire la surface d'attaque des entreprises.

Quelles activités adopter pour la sensibilisation à la cybersécurité ?

L'adoption d'activités diversifiées, voire ludiques, peut s'avérer très efficace, car elles rendent l'apprentissage plus attrayant et plus mémorable. Voici quelques exemples d'activités à envisager :

- **Formation en ligne** via des cours interactifs sur la cybersécurité, avec des modules, des quiz et des scénarios pour permettre aux collaborateurs d'apprendre à leur propre rythme (ex : formation SecNumCloud de l'ANSSI).
- **Ateliers pratiques** au travers des ateliers où les collaborateurs peuvent apprendre à identifier les menaces, à utiliser des outils de cybersécurité et à appliquer de bonnes pratiques SSI.
- **Campagnes de sensibilisation** régulières via la diffusion d'affiches, de vidéos, de newsletters et d'autres supports pour rappeler aux collaborateurs les bonnes pratiques SSI (CERT Santé portail industriel de l'ANS).



Comment mesurer l'impact de la sensibilisation sur les collaborateurs ?

Pour garantir la pérennité d'un programme de sensibilisation à la SSI, il est nécessaire de mesurer son impact via un certain nombre d'indicateurs, notamment :

- **Le Phishing simulé** avant et après un programme de sensibilisation pour avoir une idée sur l'amélioration de la compréhension des menaces par les collaborateurs.
- **Feedback régulier des collaborateurs** pour collecter des informations sur les points forts et faibles d'un programme de sensibilisation et réaliser les ajustements nécessaires au fil du temps.
- **Simulations d'attaque via des exercices de gestion de crise** pour évaluer la capacité des collaborateurs à identifier et à signaler les menaces en situation réelle.

Des ressources pertinentes dans le cadre de la sensibilisation à la SSI

- **L'ENISA** qui fournit des guides de bonnes pratiques en matière de SSI [[Site Web](#)]
- **L'ANSSI** qui propose également des guides de bonnes pratiques en matière de SSI [[Site Web](#)]
- **L'OWASP** qui met à disposition des ressources pour sensibiliser aux vulnérabilités applicatives [[Site Web](#)]
- **PGSSI-S** qui regroupe l'ensemble du Corpus documentaire de la Politique Générale de Sécurité des Systèmes d'Information de Santé [[Site Web](#)]