

Sensibiliser ses équipes : le facteur humain

La meilleure technologie ne rattrape pas un clic malheureux. Construire une culture sécurité qui tient dans la durée.

9 min de lecture · Niveau Essentiel · cyberionis.fr/ressources/sensibilisation-equipe

Plus de 8 incidents sur 10 impliquent une action humaine : un clic, une pièce jointe, un mot de passe donné au téléphone. Vos collaborateurs ne sont pas le maillon faible — mal informés, ils sont la surface d'attaque ; bien formés, ils deviennent votre premier système de détection.

1. Pourquoi les formations classiques échouent

La présentation annuelle de deux heures que tout le monde subit en pensant à autre chose ne change aucun comportement. Ce qui fonctionne : des messages courts, concrets, répétés dans le temps, ancrés dans le quotidien du poste de chacun — la comptable n'a pas les mêmes risques que le commercial.

2. Un programme simple et efficace

- À l'embauche : 30 minutes sur les règles de base et la charte informatique
- Chaque trimestre : un rappel court sur un thème (phishing, mots de passe, mobilité...)
- Une à deux fois par an : un exercice de faux phishing, suivi d'un débriefing bienveillant
- En continu : partager les tentatives réelles reçues par l'entreprise — rien n'est plus parlant
- Pour les fonctions exposées (direction, comptabilité, RH) : une session dédiée aux fraudes ciblées

3. La culture du signalement sans blâme

Le pire scénario n'est pas le collaborateur qui clique : c'est celui qui clique et n'ose pas le dire. Chaque heure de silence laisse l'attaquant progresser. La règle d'or à répéter : signaler immédiatement, sans crainte de sanction. Un signalement rapide est une réussite, pas une faute — et ceux qui remontent les tentatives méritent d'être valorisés.

4. Mesurer les progrès

- Taux de clic aux exercices de phishing (l'évolution compte plus que le chiffre)
- Taux de signalement : combien remontent l'email suspect ? C'est l'indicateur le plus précieux
- Adoption du gestionnaire de mots de passe et de la MFA
- Délai entre réception d'une menace réelle et premier signalement

5. Des supports qui marchent (et gratuits)

- Le MOOC SecNumacadémie de l'ANSSI : formation en ligne complète et gratuite, avec attestation
- Les kits de sensibilisation de Cybermalveillance.gouv.fr : affiches, vidéos, quiz, prêts à diffuser
- Vos propres incidents et tentatives reçues, anonymisés : rien ne parle plus qu'un vrai exemple « de chez nous »
- Les fiches réflexes affichées près des postes : le rappel permanent qui ne coûte rien
- Ce centre de ressources : des guides à partager selon le poste de chacun

BON À SAVOIR

La direction donne le ton : un dirigeant qui utilise le gestionnaire de mots de passe, valide la MFA et respecte la procédure virement rend les règles légitimes. Un dirigeant qui s'en exempte (« pas le temps pour ces trucs ») les tue — et c'est pourtant lui la cible n° 1 des attaquants.

L'essentiel à retenir

- 01 Intégrer 30 minutes de sensibilisation au parcours d'embauche
- 02 Planifier des rappels courts chaque trimestre
- 03 Organiser un exercice de faux phishing annuel avec débriefing bienveillant
- 04 Instaurer explicitement le signalement sans blâme
- 05 Suivre le taux de signalement plutôt que de punir les clics
- 06 Impliquer la direction : elle applique les mêmes règles, visiblement

Questions fréquentes

Combien de temps et de budget faut-il y consacrer ?

Beaucoup moins qu'on ne l'imagine : 30 minutes à l'embauche, 15 minutes par trimestre, un exercice annuel — l'équivalent de deux heures par personne et par an. Les supports publics (ANSSI, Cybermalveillance) sont gratuits ; seuls les exercices de phishing simulé et les formations sur mesure représentent un vrai budget, et ils se mutualisent via un prestataire.

Nos équipes ne sont « pas informatiques ». Par où commencer ?

Justement pas par la technique : commencez par les histoires. Une session qui raconte trois vraies attaques de PME (fraude au président, ransomware, phishing) marque plus que tous les schémas réseau. Les gestes concrets viennent ensuite, un par un : ce trimestre le gestionnaire de mots de passe, le suivant les réflexes phishing.

Un collaborateur clique systématiquement aux exercices. Que faire ?

Ni sanction ni moquerie — un accompagnement individuel : souvent la personne n'a simplement jamais eu d'explication adaptée à son quotidien. Si la fonction est exposée (comptabilité, direction, RH), renforcez aussi les garde-fous techniques et procéduraux autour d'elle : la sécurité ne doit jamais reposer sur l'infaillibilité d'une personne.

La sensibilisation est-elle obligatoire légalement ?

De plus en plus : le RGPD impose la sensibilisation des personnes qui traitent des données personnelles, NIS2 exige la formation à la gestion des risques cyber (direction comprise) pour les entités concernées, et les assureurs cyber en font une condition de garantie. Au-delà de l'obligation, c'est l'investissement sécurité au meilleur rendement.

Pour aller plus loin

SecNumacadémie — le MOOC gratuit de l'ANSSI — secnumacademie.gouv.fr

Cybermalveillance.gouv.fr — kit de sensibilisation — www.cybermalveillance.gouv.fr/tous-nos-contenus/kit-de-sensibilisation

Structurer sans vous noyer dans la paperasse ?

Audit, mise en conformité, chartes et sensibilisation des équipes : un accompagnement à la taille de votre entreprise.

contact@cyberionis.fr · 06 64 90 07 74 · cyberionis.fr