Les fiches Stoïk : outils de cybersécurité

Simulateur Phishing

À quoi sert-il ?

- Sensibiliser les collaborateur à la technique d'attaque par phishing
- Réduire le facteur de risque humain

Pourquoi sensibiliser au phishing ?

Le phishing, ou hameçonnage, est le premier vecteur d'attaque : 73 % des cyberattaques sont rendues possibles par le phishing.

Une simple erreur d'inattention peut conduire à des conséquences graves pour toute l'entreprise.

Comment fonctionne l'outil ?

Rendez-vous dans l'onglet phishing de l'espace client :

- Se connecter à Google Workspace pour synchroniser les adresses e-mail des collaborateurs avec l'outil.
- Choisir une simulation en sélectionnant un des deux modèles disponibles (Google, GitHub).
- Sélectionner les collaborateurs qui recevront chaque type de simulation.
- Programmer la temporalité : 1 mail par mois ou par trimestre, avec la possibilité de suspendre la campagne à tout moment.
- Si besoin, générer un rapport complet via l'application.

En cas d'hameçonnage, les collaborateurs sont redirigés vers un mini-espace de formation aux bonnes pratiques contre le phishing.

CONSEILS D'UTILISATION

→ **Activez des simulations adaptées aux métiers de des collaborateurs.**

Par exemple, sélectionnez le modèle de simulation GitHub pour tester vos équipes informatiques. Restez sur le modèle Google si vous n'utilisez aucun des autres outils.

DÉVELOPPEMENT DE L'OUTIL

→ **Disponibilité sur Microsoft à venir.** Pour l'instant, l'outil est uniquement disponible via un compte Google.

→ **Développement d'autres modèles.** Après Google, Notion et Github, d'autres modèles sont en cours de développement pour diversifier les campagnes.