Mise en place d'une campagne de phishing

Avec l'outil GoPhish

1. Contexte et objectif

Ce document présente la mise en place d'une campagne de phishing à l'aide de l'outil open source GoPhish. L'objectif est de sensibiliser un utilisateur test aux techniques d'hameçonnage en reproduisant un scénario réaliste (usurpation d'une banque en ligne) et de mesurer les statistiques de la campagne : envoi, ouverture, clic et éventuelle soumission de données.

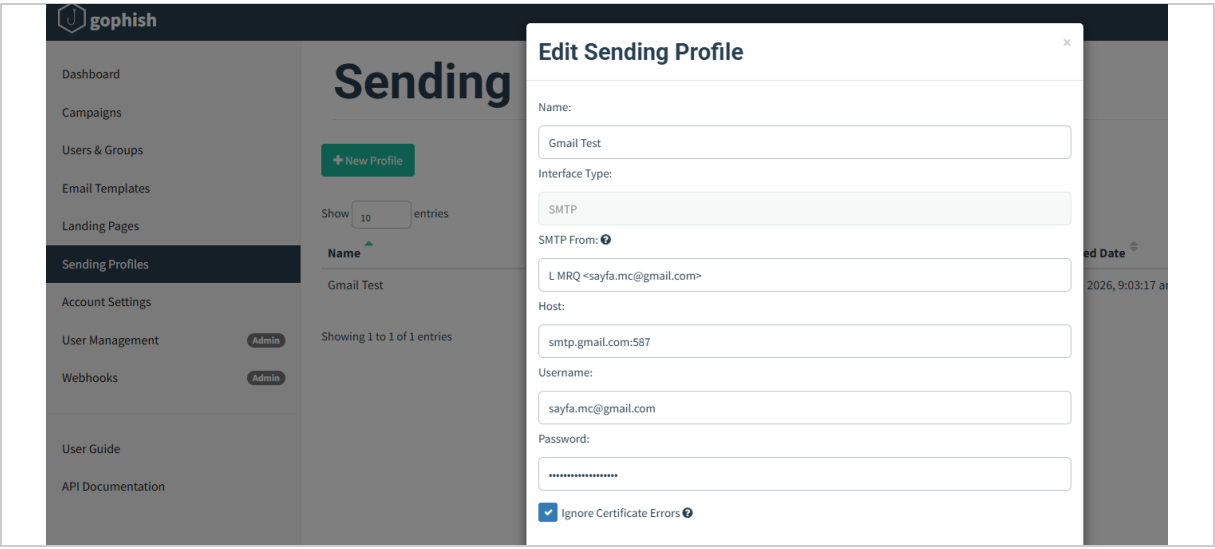
GoPhish est une plateforme dédiée à la simulation de campagnes de phishing. Elle permet de gérer, depuis une interface web, l'ensemble des éléments nécessaires : les cibles (Users & Groups), les modèles d'e-mails (Email Templates), les pages d'atterrissage (Landing Pages), les profils d'envoi SMTP (Sending Profiles) et le suivi des campagnes (Campaigns).

2. Configuration de l'environnement GoPhish

Avant de lancer une campagne, plusieurs éléments doivent être configurés dans GoPhish : le groupe de cibles, le modèle d'e-mail utilisé, et le profil d'envoi permettant d'expédier les messages.

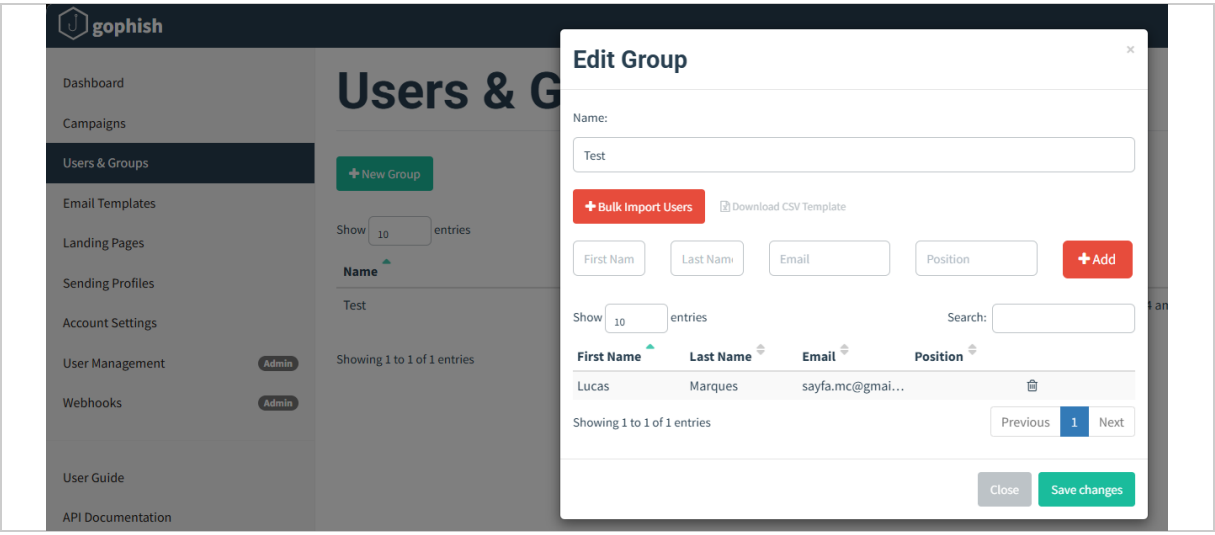
2.1 Création du profil d'envoi (Sending Profile)

Le profil d'envoi définit le serveur SMTP utilisé pour expédier les e-mails de la campagne. Ici, un compte Gmail a été utilisé comme relais d'envoi avec authentification par identifiant et mot de passe d'application.



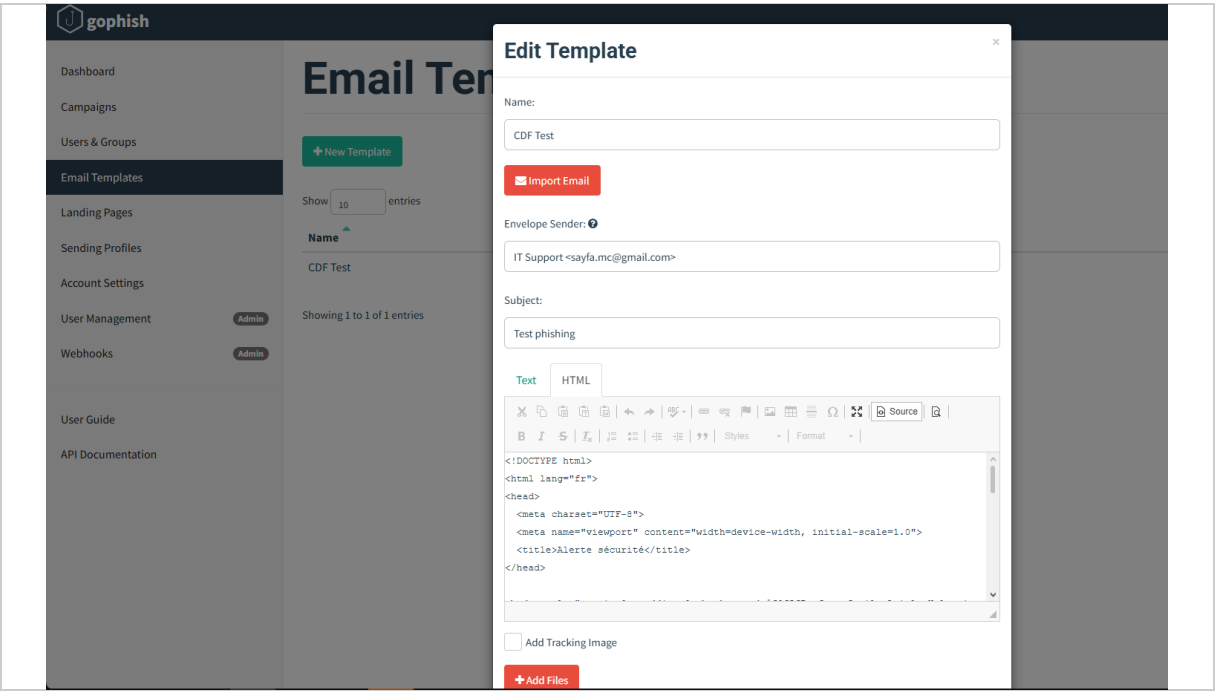
2.2 Création du groupe de cibles (Users & Groups)

Un groupe nommé "Test" a été créé afin d'y ajouter la cible de la campagne. Chaque utilisateur est renseigné avec son prénom, son nom, son adresse e-mail et éventuellement son poste.



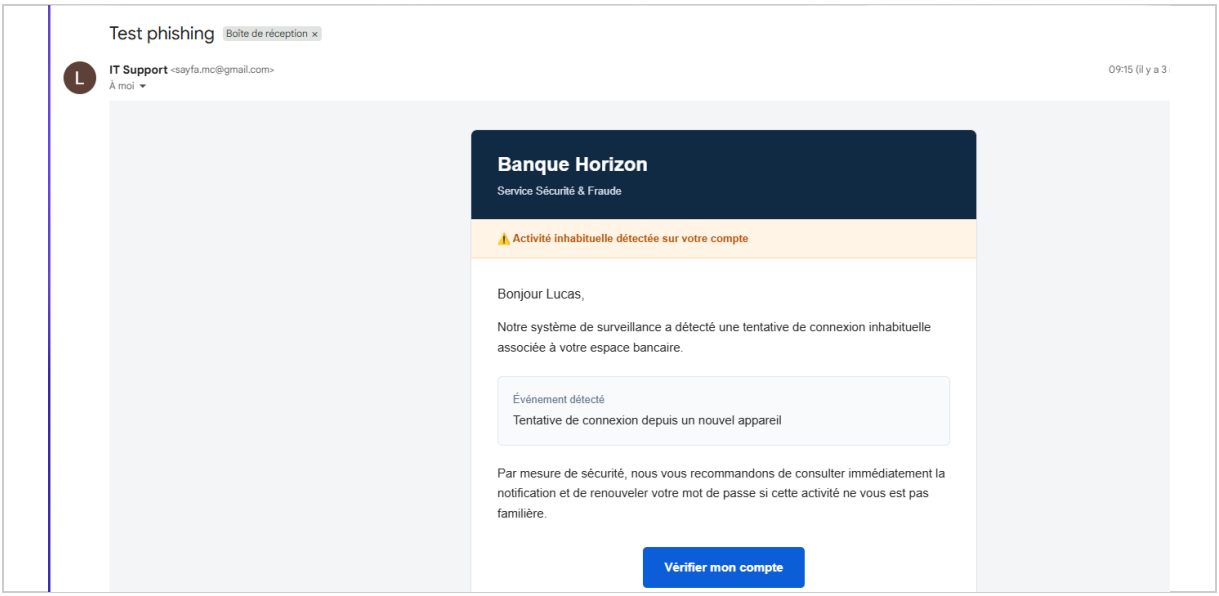
2.3 Création du modèle d'e-mail (Email Template)

Le modèle d'e-mail constitue le leurre envoyé à la cible. Ici, il reprend la base d'une banque fictive "Banque Horizon" et simule une alerte de sécurité invitant l'utilisateur à vérifier son compte. L'expéditeur a été personnalisé en "IT Support" afin de renforcer la crédibilité du message.



3. Envoi et réception de l'e-mail de phishing

Une fois le groupe, le modèle et le profil d'envoi configurés, la campagne a été lancée. L'e-mail a bien été reçu dans la boîte de réception de la cible, avec l'expéditeur usurpé "IT Support" et le contenu prévu : un bandeau d'alerte, un message personnalisé au nom du destinataire "Bonjour Lucas" et un bouton d'appel à l'action "Vérifier mon compte" renvoyant vers la fausse page d'authentification.

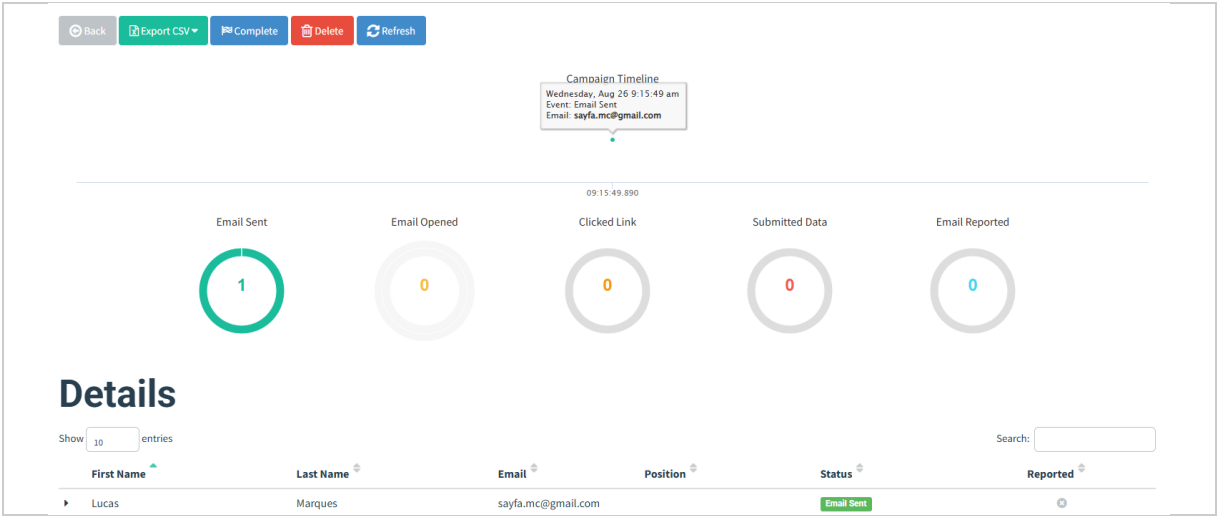


4. Suivi et résultats de la campagne

GoPhish fournit un tableau de bord dédié à chaque campagne, accessible depuis le menu "Campaigns". Il affiche les événements ainsi que cinq indicateurs clés représentés sous forme d'anneaux de progression :

- Email Sent : nombre d'e-mails envoyés avec succès
- Email Opened : nombre d'ouvertures détectées (via l'image de suivi)
- Clicked Link : nombre de clics sur le lien piégé
- Submitted Data : nombre de formulaires soumis (identifiants saisis)
- Email Reported : nombre de signalements de l'e-mail comme suspect

Un tableau "Details" recense, pour chaque cible, son statut individuel (ici "Email Sent") ainsi qu'un éventuel signalement. Ces données permettent d'évaluer objectivement la vulnérabilité des utilisateurs face à ce type d'attaque.



5. Conclusion

Cette mise en pratique a permis de configurer un environnement GoPhish complet, profil d'envoi SMTP, groupe de cibles, modèle d'e-mail réaliste — et de suivre en temps réel les statistiques d'une campagne de sensibilisation au phishing.