GOPHISH

I. Présentation

Ici, nous allons voir comment utiliser le Framework open source Gophish pour créer une campagne de phishing (hameçonnage) dans le but d'évaluer le niveau de vigilance des utilisateurs.

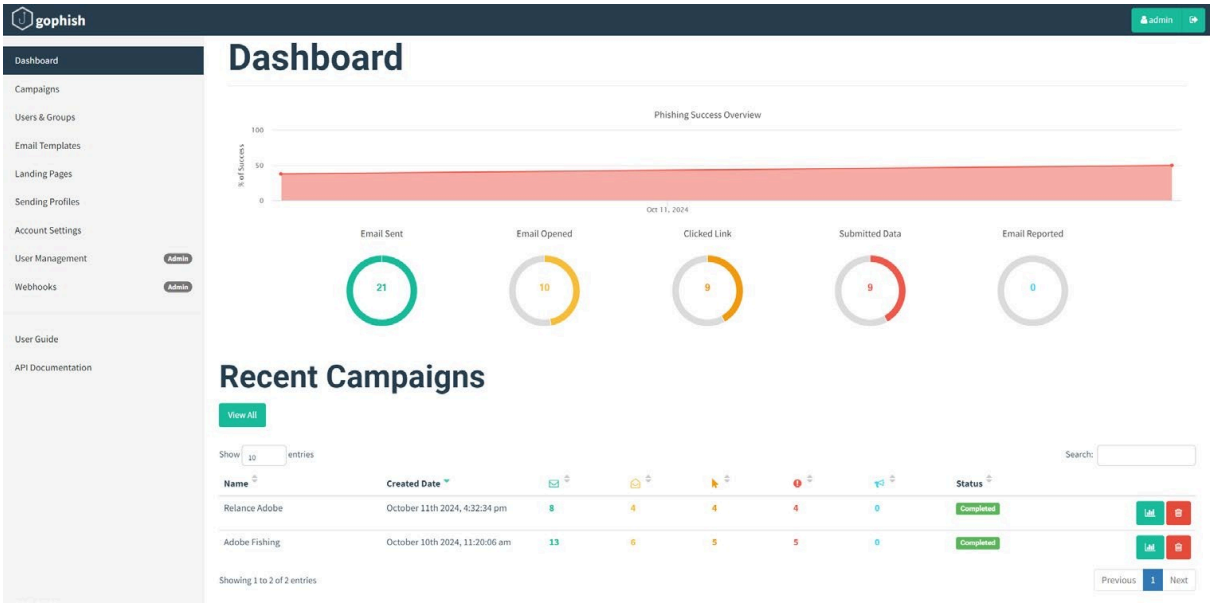
Grâce à Gophish, vous allez pouvoir créer différentes campagnes de phishing et les diffuser auprès de vos utilisateurs, dans le but de les sensibiliser, de les entraîner, afin qu'ils soient capables d'adopter les bons réflexes lorsqu'ils se retrouvent face à un e-mail douteux.

Voici les fonctionnalités principales de Gophish :

- Création d'utilisateurs et de groupes d'utilisateurs (cibles).
- Création de Template pour les e-mails de vos campagnes.
- Création de landing page pour vos campagnes (exemple : un formulaire de connexion).

- Envoyer des campagnes de phishing avec suivi des e-mails (e-mail envoyé, e-mail ouvert, clic sur le lien, données récoltées via le formulaire) pour chaque utilisateur.
- Reporting sur les campagnes
- API pour interroger Gophish à distance et récupérer des informations

Voici à quoi ressemble le tableau de bord de Gophish, accessible à partir d'un navigateur :



Bien sûr, un tel outil peut être détourné pour créer des campagnes malveillantes, mais ce n'est clairement pas l'objectif de cet article.

De nombreuses attaques informatiques débutent par un e-mail malveillant et un utilisateur piégé ! Je vous encourage à utiliser Gophish (ou un autre outil) pour sensibiliser et entraîner vos utilisateurs ! Rien de mieux que la pratique pour vérifier s'ils ont bien compris la session de formation visant à les sensibiliser.

II. Installation de Gophish

Pour ma part, je vais utiliser le binaire pour Linux. Je vais donc installer une machine en Debian 12 avec un serveur web (Apache2 pour moi) afin de faire ce test de phishing.

J'ai fait les mises à jour de la VM.

```
sudo apt update && sudo apt upgrade -y
```

Ensuite, on va télécharger le fichier binaire de gophish et on obtient un fichier ZIP qu'il suffit de décompresser. Moi, je vais le décompresser dans le dossier que l'on souhaite ; pour ma part, ça sera le dossier /opt/gophish car c'est ici que nous installons tous nos logiciels.

```
sudo wget https://https://github.com/gophish/gophish/releases/download/v0.
gophish-v0.12.1-linux-64bit.zip
sudo unzip gophish-v0.12.1-linux-64bit.zip /opt/gophish/
```

Il faut installer les commandes go afin de pouvoir lancer Gophish (apt-get install golang), puis, une fois cela fait, exécuter la commande (go build) pour qu'elle puisse lancer le logiciel Gophish.

```
apt install golang
go build
```

Pensez à modifier le fichier de configuration :

- fichier “config.json”:

Changez l’adresse IP par défaut et mettez celle de votre machine, puis enregistrez le fichier.

Pour lancer Gophish, il vous suffira d’exécuter la commande suivante. Au premier démarrage, il y a quelques informations intéressantes à relever.

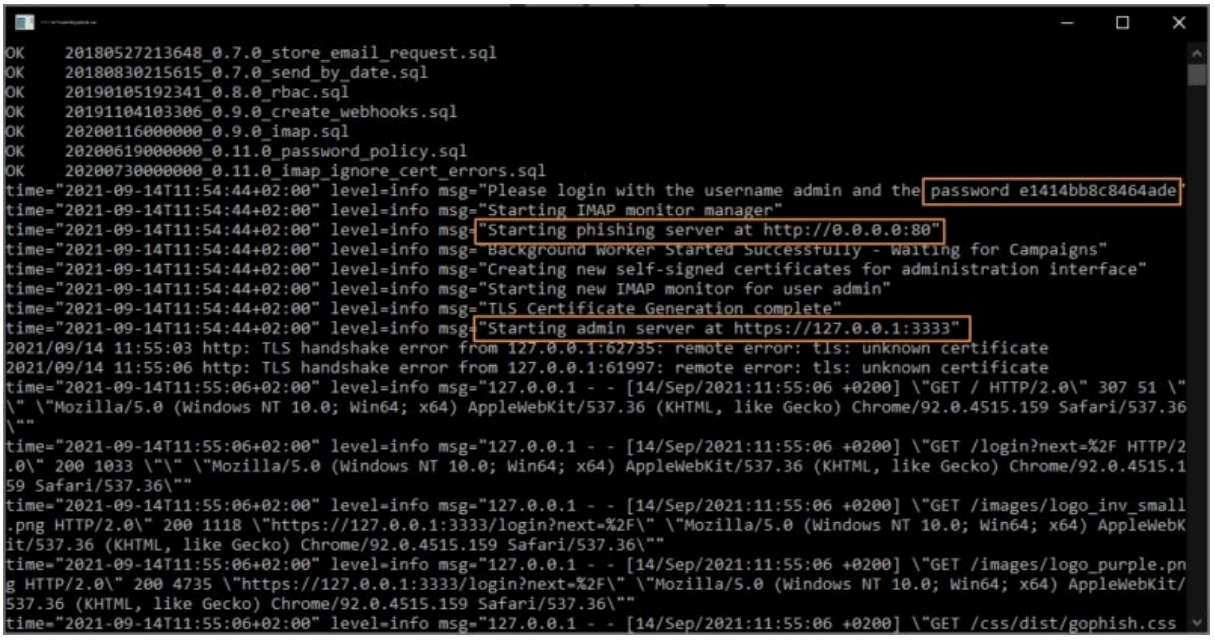
```
./gophish
```

Le compte par défaut se nomme "admin" et le mot de passe généré aléatoirement est communiqué dans la console (il faudra le changer à la première connexion).

L'interface de Gophish pour afficher les pages web de vos campagnes est accessible sur le port 80/HTTP.

L'interface d'administration de Gophish est accessible en HTTPS sur le port 3333.

Exemple de démarrage de Gophish :

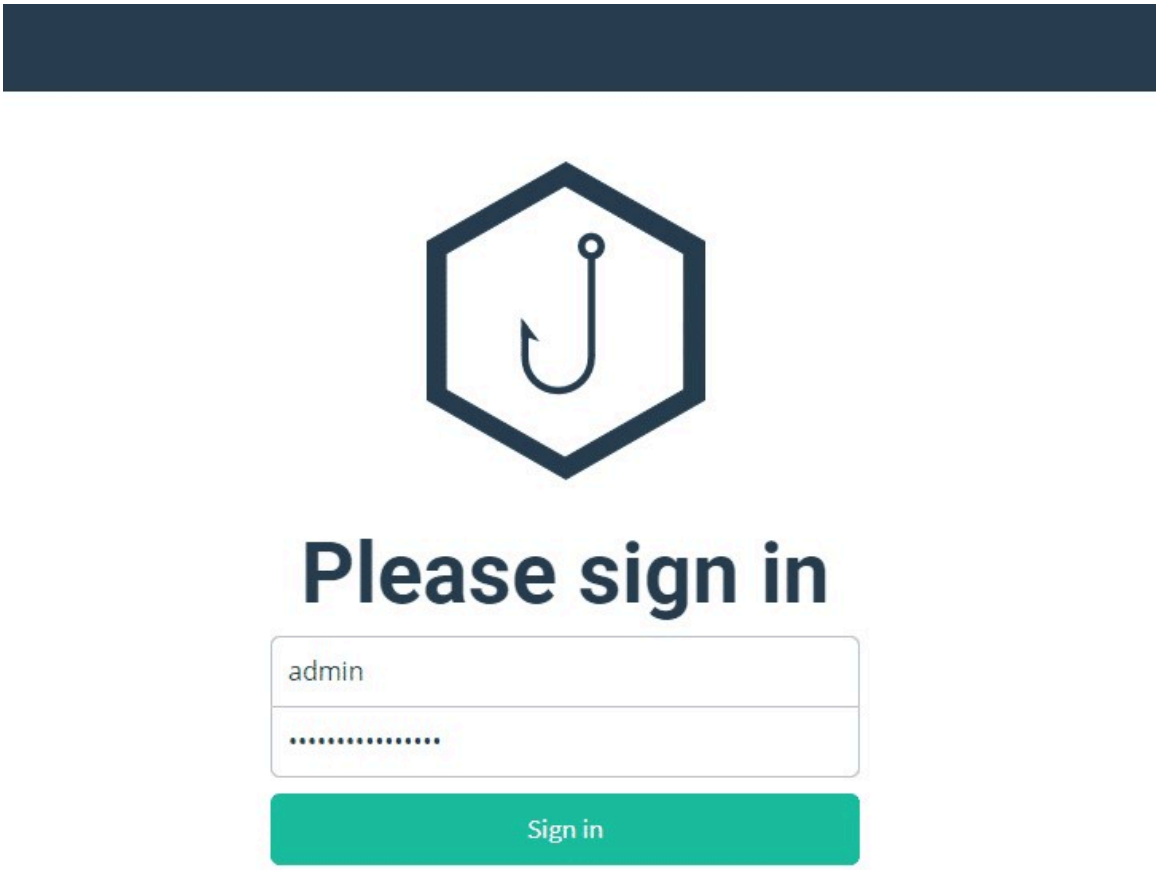


Laissez Gophish tourner et connectez-vous sur l'interface d'administration.

III. Configuration de Gophish

Pour se connecter depuis la machine locale, il suffit d'accéder à l'adresse

"https://ipdelamachine:3333" à partir d'un navigateur. Connectez-vous avec le compte admin et modifiez le mot de passe.



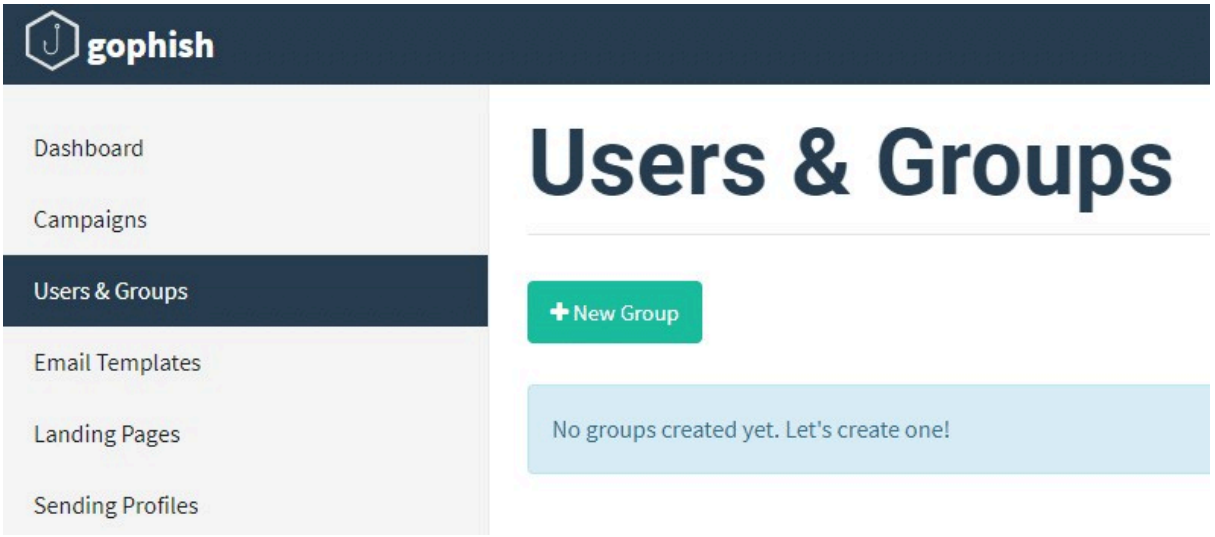
Mon objectif est de créer une campagne de phishing en reprenant un e-mail d'Adobe qui renvoie vers une page Web avec un formulaire.

Avant de pouvoir envoyer notre première campagne de phishing, il va falloir préparer un certain nombre d'éléments : c'est ce que nous allons faire, étape par étape !

IV. Création des utilisateurs et des groupes

Nous devons commencer par créer nos utilisateurs et nos groupes. On peut imaginer qu'un groupe correspond aux utilisateurs d'un service ou d'un site. Lorsqu'une campagne de phishing sera envoyée, il faudra cibler un ou plusieurs groupes.

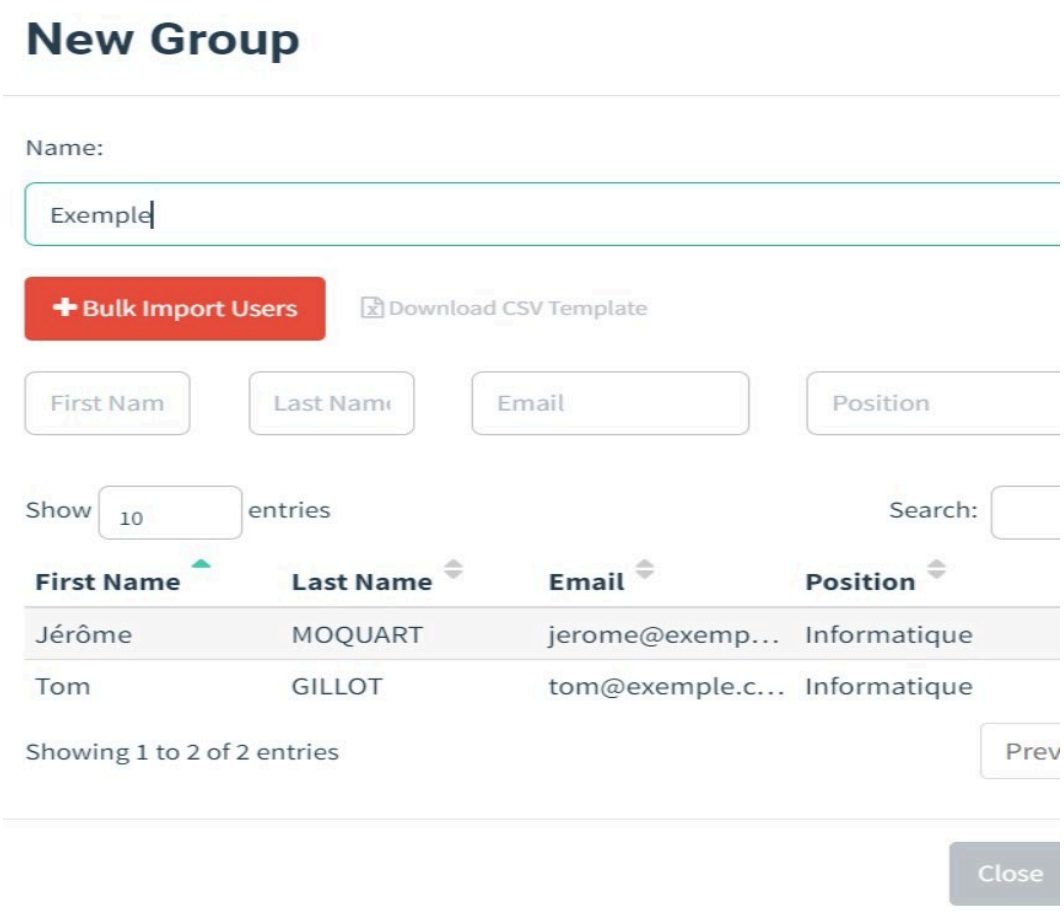
Cliquez sur "Users & Groups", puis sur "New Group".



Nommez votre groupe en renseignant le champ "Name", et ensuite vous avez deux options :

- Créez vos utilisateurs un par un, en remplissant le formulaire et en cliquant sur "Add". Cela peut vite être chronophage...
- Créez vos utilisateurs à l'aide d'un fichier CSV que vous pouvez importer avec le bouton "Bulk Import Users". Cela me plaît un peu plus et de toute façon, on ne peut pas établir de connexion avec un annuaire externe.

Dans notre cas, vu que nous avons une entreprise assez petite, nous allons les créer à la main.

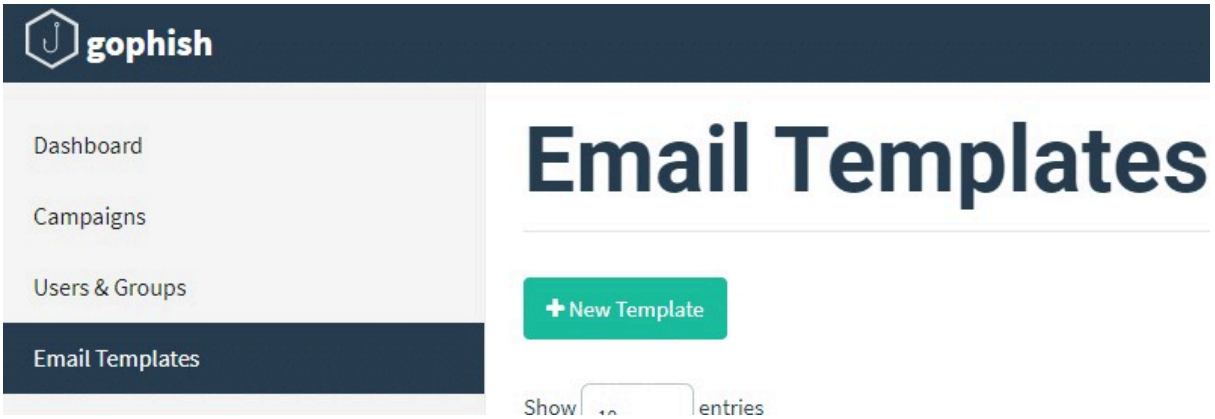


Pour sauvegarder cela, cliquez sur le bouton “Save changes”.

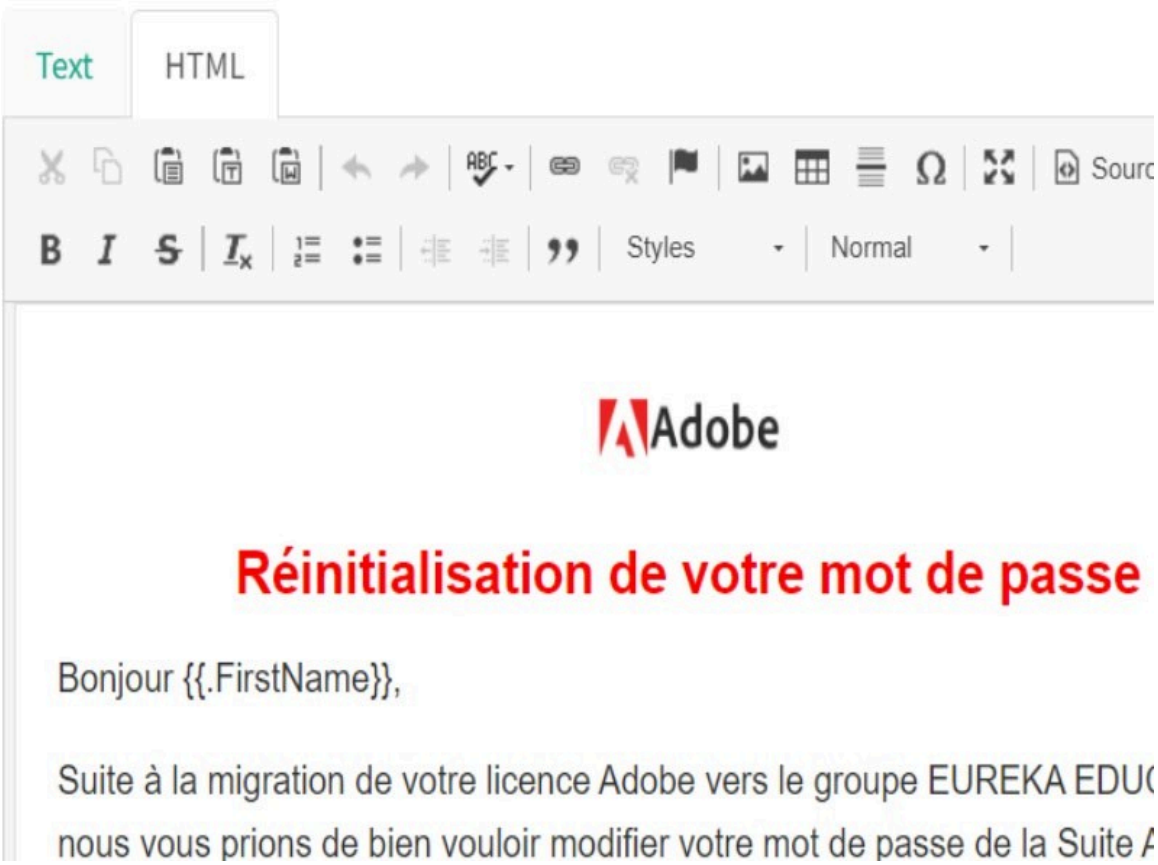
V. Créer l'e-mail pour la campagne de phishing

Seconde étape : la création du modèle d'e-mail que l'on va envoyer aux utilisateurs dans le cadre de cette campagne de phishing.

Cliquez à gauche sur "Email Templates", puis sur le bouton "New Template".



Pour créer le modèle, vous pouvez partir de zéro ou importer le code HTML d'un e-mail existant (ce qui est intéressant pour gagner du temps) grâce au bouton "Import Email". Pour nous, j'ai repris un modèle que j'ai trouvé et que j'ai adapté à ma façon.



Pour renvoyer vers la landing page qui contient le formulaire, il faut ajouter un lien à l'e-mail. Sur ce lien, il faut indiquer l'URL "{{.URL}}", qui sera remplacée par Gophish par la bonne valeur.

Mon e-mail est prêt, voici un aperçu :

Adobe

Réinitialisation de votre mot de passe

Bonjour {{.FirstName}},

Suite à la migration de votre licence Adobe vers le groupe EUREKA EDUCATION, nous vous prions de bien vouloir modifier votre mot de passe de la Suite Adobe.

Pour réinitialiser votre mot de passe, cliquez sur le bouton ci-dessous :

Réinitialiser mon mot de passe

Une fois que la modification sera faite, veuillez l'indiquer à votre Service Informatique.

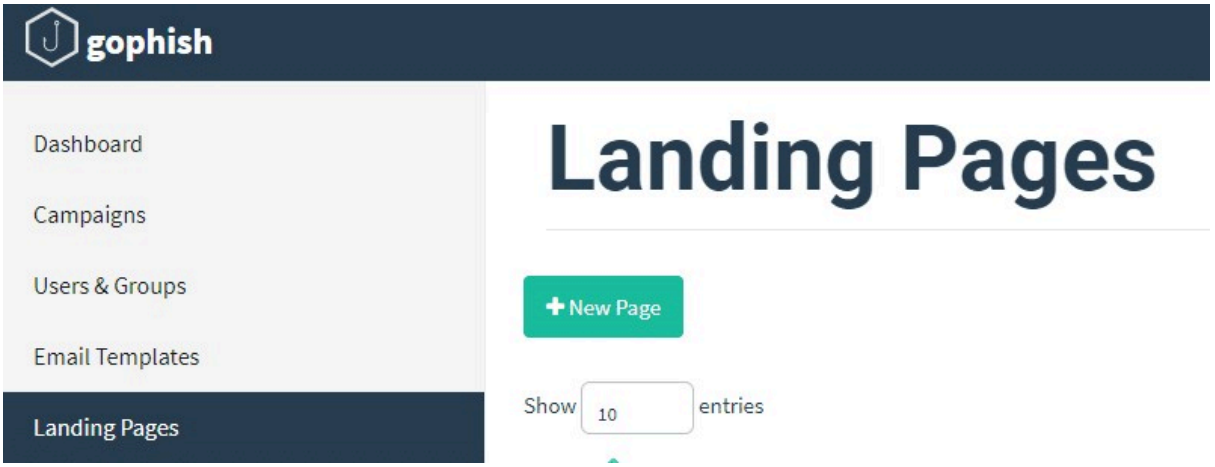
Merci,
L'équipe Adobe

Besoin d'aide ? Consultez notre centre d'aide.

VI. Créer la landing page pour récupérer les identifiants

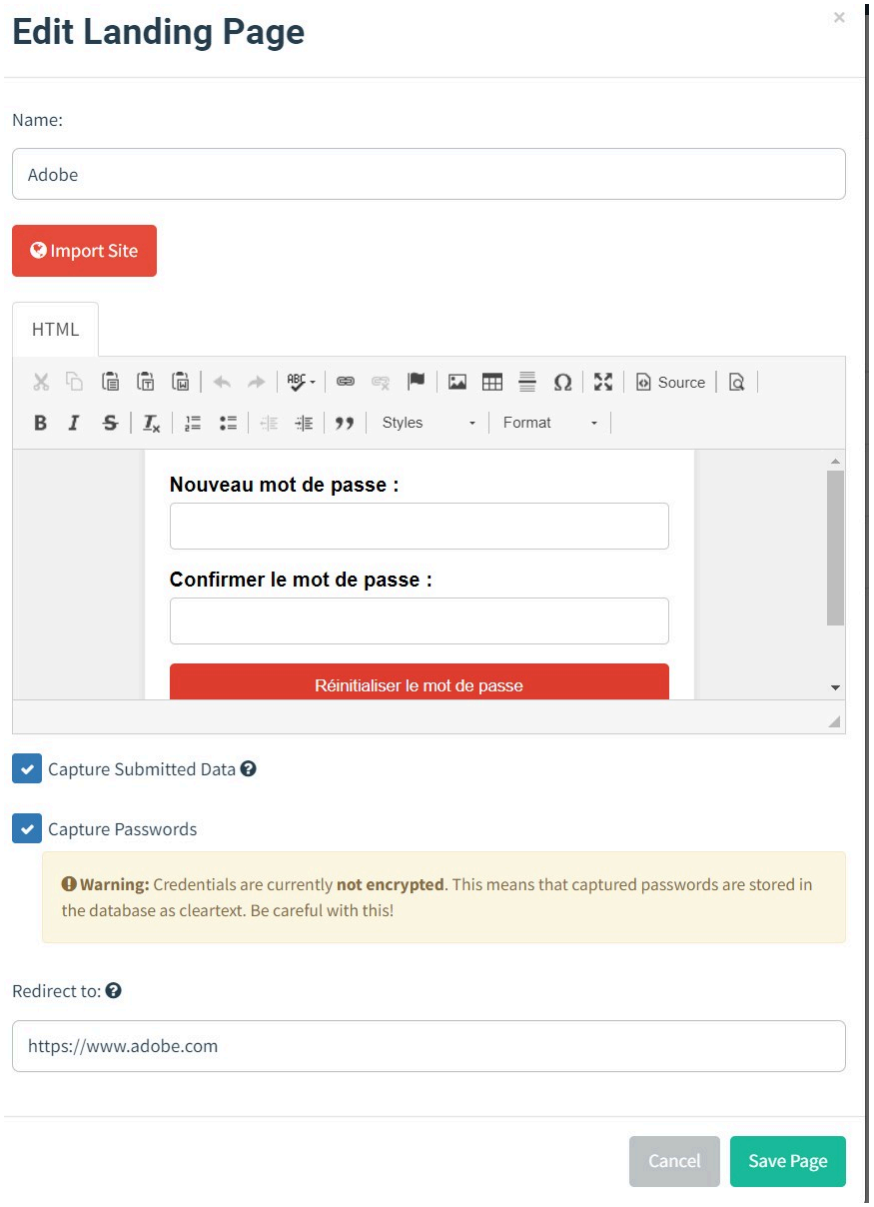
Troisième étape : création de la landing page, qui sera une page piégée, puisque si l'utilisateur complète le formulaire, nous allons le savoir ! S'il clique sur le lien, nous allons le savoir aussi !

Cliquez sur "Landing Pages" sur la gauche du menu puis sur "New Page".



Donnez un petit nom à votre Template et ensuite, il faut passer à la construction.

Vous pouvez partir de zéro comme pour l'e-mail ou importer un site à partir d'une URL et du bouton "Import Site".



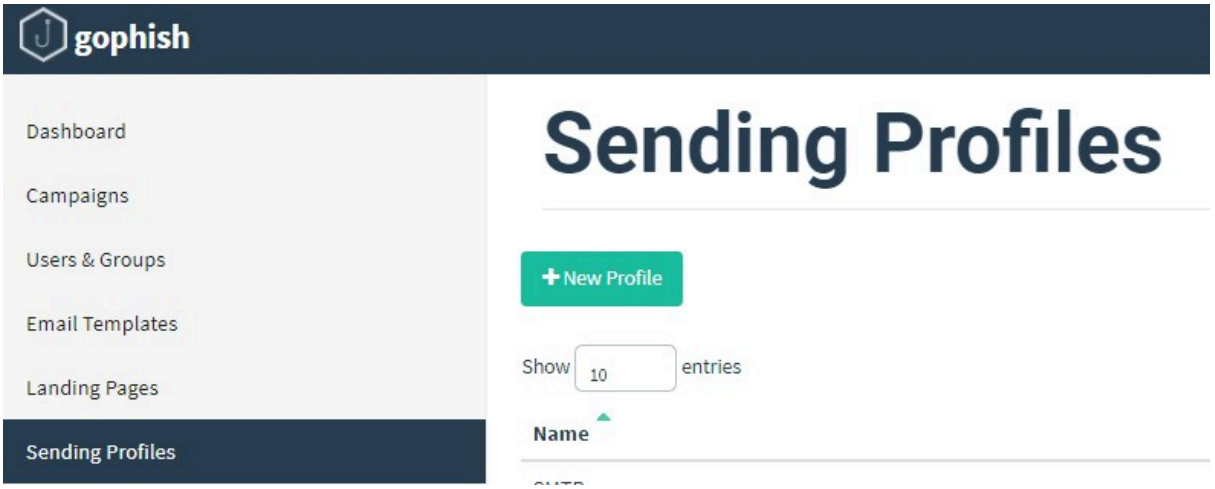
Pour ma part, j'ai créé une page qui ressemble beaucoup à Adobe, mais basique.

Si vous souhaitez récupérer les informations saisies par les utilisateurs, cochez les cases "Capture Submitted Data" et "Capture Passwords" pour le mot de passe.

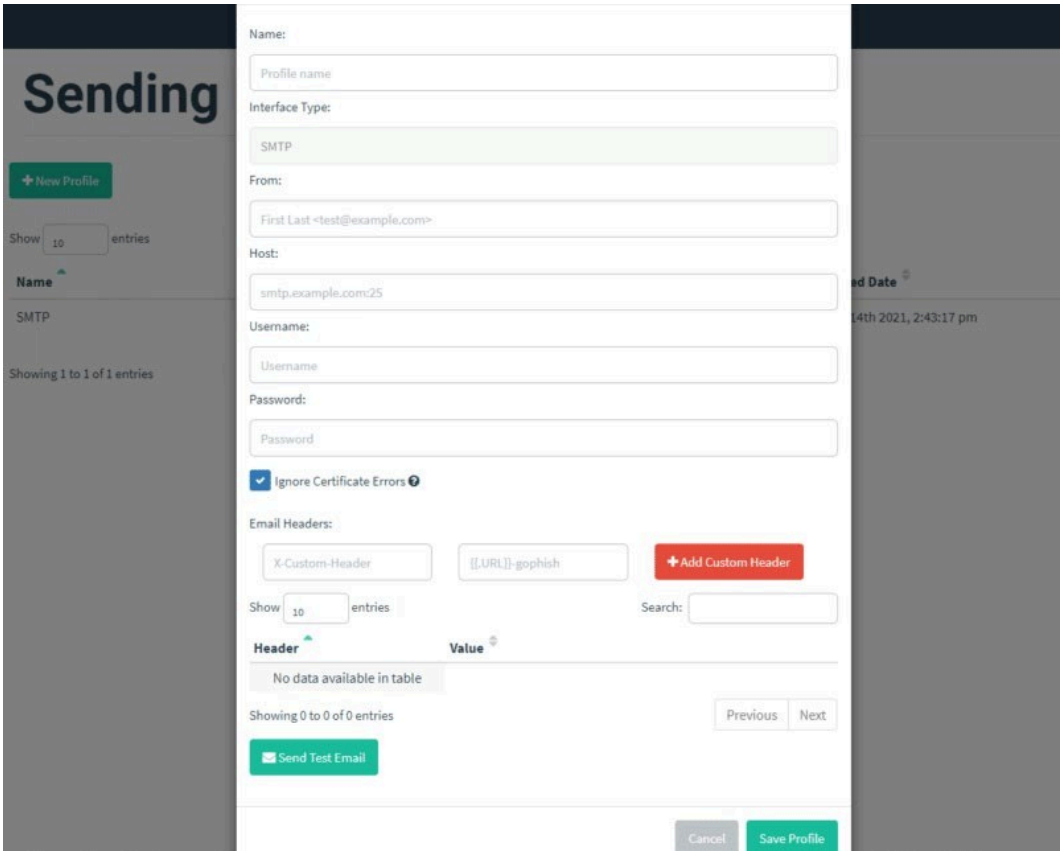
VII. Configurer le serveur SMTP

Avant de lancer la campagne, il nous reste une dernière étape : la configuration du serveur de messagerie (SMTP). Vous vous en doutez, il va servir à envoyer les e-mails de nos campagnes de phishing.

Sur la gauche, cliquez sur "Sending Profiles" puis sur "New Profile".



Ensuite, vous devez nommer votre profil et renseigner les informations en complétant le formulaire.



Voici quelques indications :

From : adresse e-mail utilisée pour envoyer les e-mails, c'est-à-dire l'expéditeur. S'il n'a rien à voir, ce sera plus facile pour les utilisateurs de voir qu'il s'agit d'un piège, mais ce sera aussi l'occasion de voir s'ils ont bien compris qu'il fallait vérifier l'e-mail de l'expéditeur.

Host : serveur SMTP à utiliser pour envoyer les e-mails, suivi du port (séparé par ":").

Username : compte utilisateur pour s'authentifier sur le serveur SMTP.

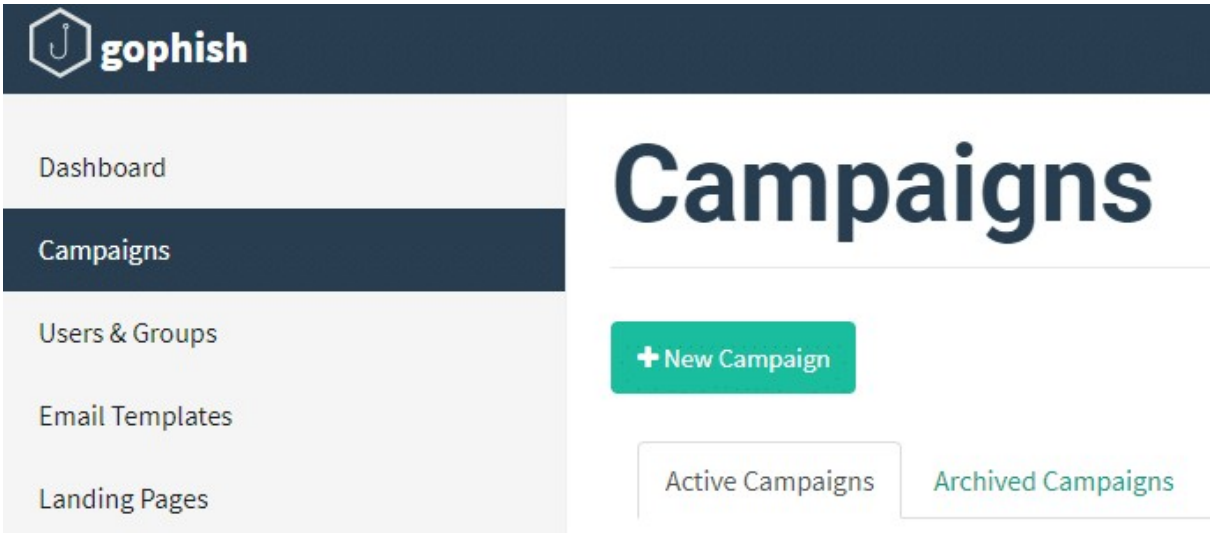
Password : le mot de passe de ce compte.

Pour valider que ça fonctionne, cliquez sur "Send Test Email". Si c'est bon, vous pouvez continuer.

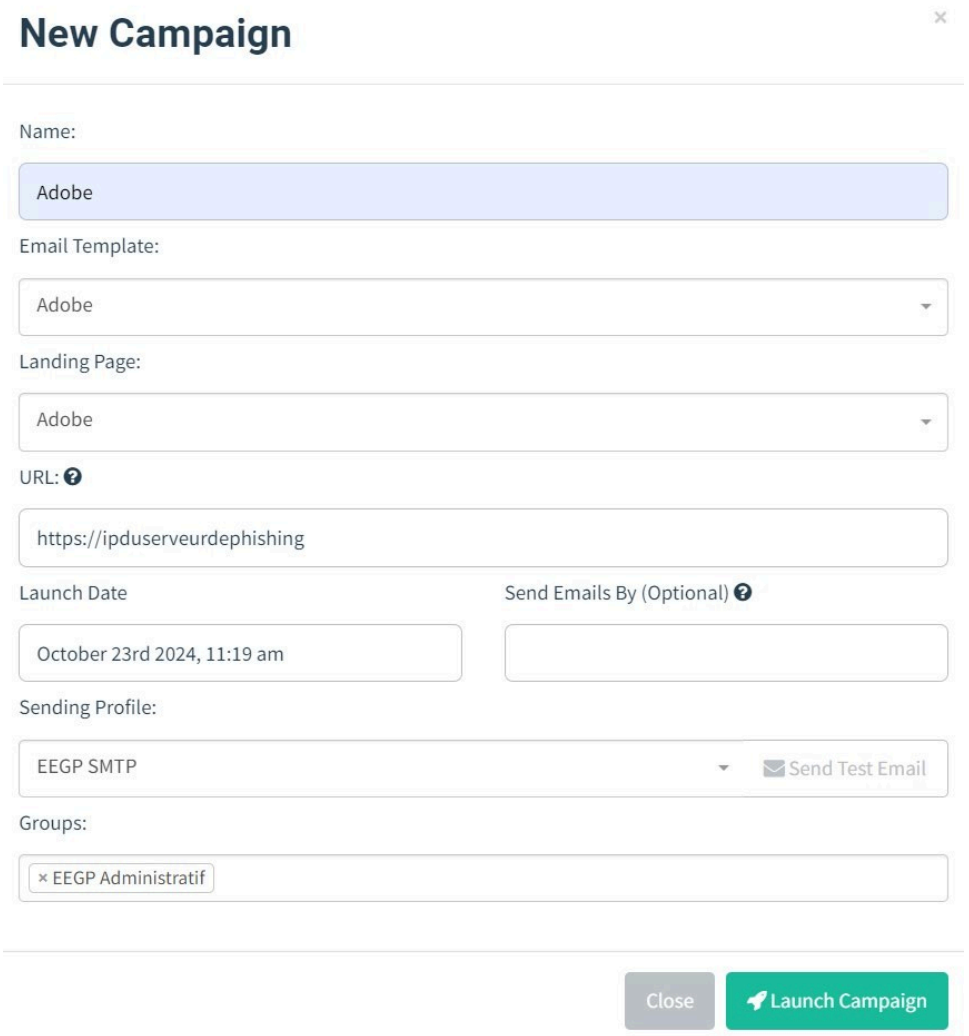
VIII. Lancer la campagne de phishing

Tout est prêt ! Nous allons pouvoir créer notre première campagne de phishing et tester nos utilisateurs !

Cliquez sur le menu "Campaigns", puis sur "New Campaign".



Pour créer cette campagne nommée "Adobe", on va réutiliser les éléments créés précédemment : "Email Template", "Landing Page" et "Sending Profile".



Concernant les autres options :

URL : indiquez le nom de domaine ou l'adresse IP où les utilisateurs pourront contacter votre serveur Gophish.

Launch Date : date à laquelle envoyer la campagne, par défaut c'est immédiatement. Si vous spécifiez aussi une date pour le champ "Send Emails By", Gophish enverra les e-mails à un moment donné entre la date de début ("Launch Date") et la date de fin ("Send Emails By"). Ainsi, tous les utilisateurs ciblés ne vont pas recevoir l'e-mail en même temps.

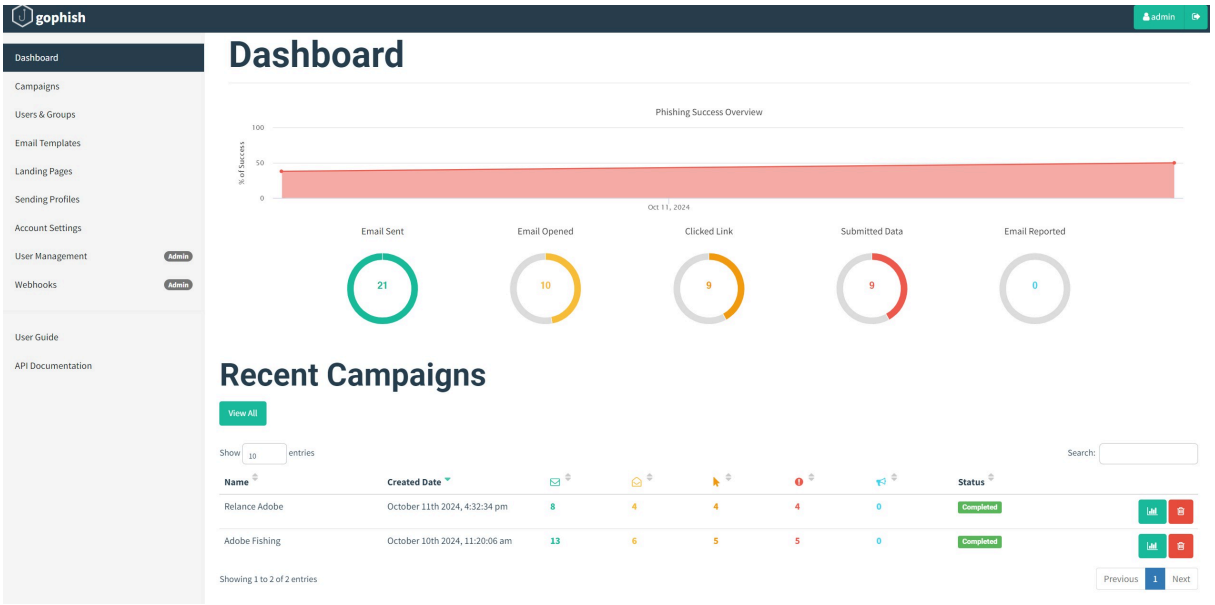
Groups : sélectionnez un ou plusieurs groupes d'utilisateurs que vous souhaitez cibler avec cette campagne. Créer une campagne dans Gophish.

Quand tous les champs sont complétés, cliquez sur "Launch Campaign" pour démarrer la campagne ! Le tableau de bord de la campagne va s'afficher et la section "Details" vous indique la "progression" pour chaque utilisateur.

IX. Consulter les résultats de la campagne de phishing

Sur l'interface de Gophish, on peut voir s'il y a un utilisateur qui a ouvert l'e-mail, qui a cliqué sur le lien et a envoyé des données.

En complément, la "Campaign Timeline" nous donne un aperçu des événements dans le temps, avec le nom d'utilisateur et l'action effectuée. C'est plutôt bien fait !



Gophish est très précis, vous pouvez voir qui et à quelle heure de façon très précise a ouvert l'e-mail, cliqué sur le lien et voir l’intégralité du mot de passe renseigné en clair.