



Projet de sensibilisation sur le phishing.
Sous le thème de :

Simulation d'une attaque par phishing

Présenté par :

Moustapha SY



Table de matières

Table des figures.....	1
Résumé.....	2
Glossaire.....	3
Introduction générale.....	4
Installation de Gophish.....	5
Mise en place de campagne.....	6
Collecte des clics et réponses des utilisateurs.....	7
Plan de sensibilisation.....	8
Conclusion.....	9

Table des figures

Figure 1 : Dézippage du fichier gophish

Figure 2 : Rendre le programme exécutable

Figure 3 : modification du fichier config.json

Figure 4 : Autorisation du port 3333

Figure 5 : lancement de gophish

Figure 6 : Page de connexion de gophish

Figure 7 : Interface Gophish

Figure 9 : Création d'un groupe d'utilisateur

Figure 10 : Création du template email

Figure 11 : modification de la partie url

Figure 12 : Création de la landing page

Figure 13 : Création du sending profile

Figure 14 : Création de la campagne

Figure 15 : Premiers résultats

Figure 16 : Ouverture de l'email

Figure 17 : Observation après ouverture

Figure 18 : Renseignements des informations confidentielles

Figure 19 : Observation finale

Résumé

Une campagne de phishing a été simulée à l'aide de l'outil Gophish afin d'évaluer la réaction du personnel face à un email frauduleux. Le scénario choisi imitait une notification LinkedIn indiquant à l'utilisateur qu'il a reçu un message de la plateforme. L'email invitait à cliquer sur le bouton "Voir message", redirigeant la victime vers une fausse page de connexion reproduisant l'interface de connexion de LinkedIn.

Deux employés ont été ciblés dans cette simulation : l'un d'eux a ignoré le message, tandis que l'autre a non seulement cliqué sur le lien, mais a également saisi son identifiant et son mot de passe sur la page frauduleuse. Les résultats obtenus démontrent la capacité des attaquants à exploiter la confiance accordée aux plateformes professionnelles et soulignent l'importance de renforcer la formation du personnel.

Glossaire

Phishing : Technique de cyberattaques ou l'on tente de récupérer des informations personnelles.

Email template : Ce que verra l'utilisateur quand il recevra l'email

Landing page : La page que l'utilisateur aura été rediriger quand il aura cliquer sur le lien.

Sending profile : Le profile de celui qui envoyer l'email.

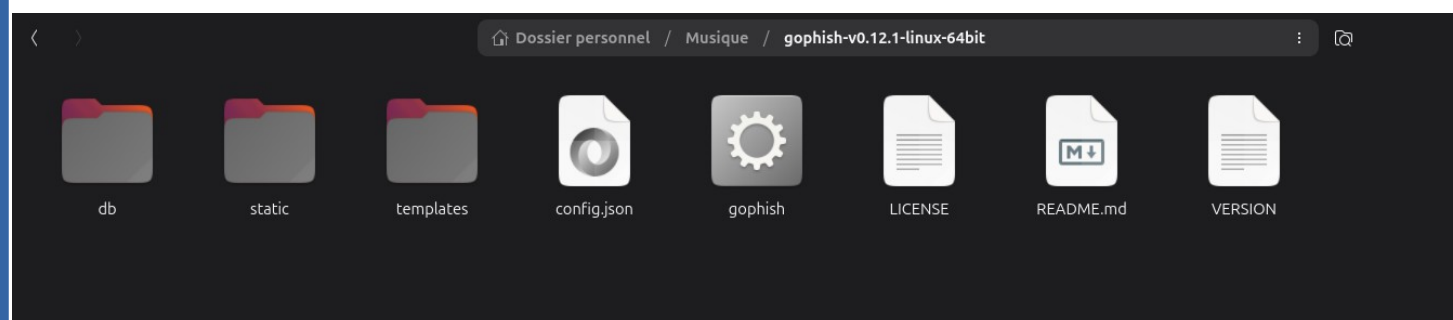
Introduction Général

La direction a souhaité évaluer le niveau de vigilance des employés face aux attaques de phishing. Le phishing demeurant l'un des vecteurs d'intrusion les plus utilisés par les attaquants, il est essentiel pour toute organisation d'en mesurer l'impact potentiel et la capacité de détection des utilisateurs. Le présent projet consiste à mettre en place une simulation d'attaque contrôlée en reproduisant un scénario réaliste, depuis la création d'un faux email frauduleux jusqu'à l'analyse du comportement des utilisateurs ciblés. Cette approche permet d'identifier les faiblesses humaines, de comprendre les mécanismes de manipulation utilisés dans ce type d'attaque et d'élaborer, à partir des résultats observés, un plan de sensibilisation destiné à réduire efficacement les risques futurs.

Installation de Gophish

Premièrement on télécharger le fichier zip disponible dans <https://github.com/gophish/gophish/releases>.

Après on dézippe le fichier



voici ce qu'on va avoir, apres avoir dézipper le fichier.

```
moustapha@moustapha: ~/Musique/gophish-v0.12.1-linux-64bit
moustapha@moustapha: ~/Musique/gophish-v0.12.1-linux-64bit
moustapha@moustapha:~/Musique/gophish-v0.12.1-linux-64bit$ sudo chmod +x gophish
[sudo] Mot de passe de moustapha :
moustapha@moustapha:~/Musique/gophish-v0.12.1-linux-64bit$ ls
config.json db gophish gophish_admin.crt gophish_admin.key gophish.db LICENSE README.md static templates VERSION
moustapha@moustapha:~/Musique/gophish-v0.12.1-linux-64bit$
```

Ici on rend executable le programme 'gophish' avec la commande 'chmod +x gophish'

```
moustapha@moustapha: ~/Musique/gophish-v0.12.1-linux-64bit
GNU nano 8.3 config.json
{
  "admin_server": {
    "listen_url": "0.0.0.0:3333",
    "use_tls": true,
    "cert_path": "gophish_admin.crt",
    "key_path": "gophish_admin.key",
    "trusted_origins": []
  },
  "phish_server": {
    "listen_url": "0.0.0.0:80",
    "use_tls": false,
    "cert_path": "example.crt",
    "key_path": "example.key"
  },
  "db_name": "sqlite3",
  "db_path": "gophish.db",
  "migrations_prefix": "db/db_",
  "contact_address": "",
  "logging": {
    "filename": "",
    "level": ""
  }
}
```

Dans notre fichier config.json, on modifie 127.0.0.1 par 0.0.0.0, pour pouvoir accéder à gophish depuis l'extérieur.

```
moustapha@moustapha: ~/Musique/gophish-v0.12.1-linux-64bit
moustapha@moustapha:~/Musique/gophish-v0.12.1-linux-64bit$ nano config.json
moustapha@moustapha:~/Musique/gophish-v0.12.1-linux-64bit$ sudo ufw allow 3333
Omission de l'ajout de la règle existante
Omission de l'ajout de la règle existante (v6)
moustapha@moustapha:~/Musique/gophish-v0.12.1-linux-64bit$ sudo ufw status
État : actif

Vers                Action              De
----                -
5044/tcp            ALLOW              Anywhere
5601/tcp            ALLOW              Anywhere
9200/tcp            DENY              Anywhere
5044                ALLOW              Anywhere
8220                ALLOW              Anywhere
3333                ALLOW              Anywhere
5044/tcp (v6)       ALLOW              Anywhere (v6)
5601/tcp (v6)       ALLOW              Anywhere (v6)
9200/tcp (v6)       DENY              Anywhere (v6)
5044 (v6)           ALLOW              Anywhere (v6)
8220 (v6)           ALLOW              Anywhere (v6)
3333 (v6)           ALLOW              Anywhere (v6)

moustapha@moustapha:~/Musique/gophish-v0.12.1-linux-64bit$
```

Ici on autorise le port 3333 avec la commande ‘sudo ufw allow 3333’.

```
moustapha@moustapha: ~/Musique/gophish-v0.12.1-linux-64bit
moustapha@moustapha:~/Musique/gophish-v0.12.1-linux-64bit$ sudo ./gophish
time="2025-12-06T14:44:19Z" level=warning msg="No contact address has been configured."
time="2025-12-06T14:44:19Z" level=warning msg="Please consider adding a contact_address entry in your config.json"
goose: no migrations to run. current version: 20220321133237
time="2025-12-06T14:44:19Z" level=info msg="Starting IMAP monitor manager"
time="2025-12-06T14:44:19Z" level=info msg="Starting phishing server at http://0.0.0.0:80"
time="2025-12-06T14:44:19Z" level=info msg="Starting admin server at https://0.0.0.0:3333"
time="2025-12-06T14:44:19Z" level=info msg="Background Worker Started Successfully - Waiting for Campaigns"
time="2025-12-06T14:44:19Z" level=info msg="Starting new IMAP monitor for user admin"
time="2025-12-06T14:44:44Z" level=info msg="127.0.0.1 - - [06/Dec/2025:14:44:44 +0000] \"GET / HTTP/2.0\" 307 51 \"\" Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:145.0) Gecko/20100101 Firefox/145.0\""
time="2025-12-06T14:44:44Z" level=info msg="127.0.0.1 - - [06/Dec/2025:14:44:44 +0000] \"GET /login?next=%2F HTTP/2.0\" 200 1033 \"\" Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:145.0) Gecko/20100101 Firefox/145.0\""
time="2025-12-06T14:44:44Z" level=info msg="127.0.0.1 - - [06/Dec/2025:14:44:44 +0000] \"GET /images/logo_inv_small.png HTTP/2.0\" 200 1118 \"https://127.0.0.1:3333/login?next=%2F\" Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:145.0) Gecko/20100101 Firefox/145.0\""
time="2025-12-06T14:44:44Z" level=info msg="127.0.0.1 - - [06/Dec/2025:14:44:44 +0000] \"GET /images/logo_purple.png HTTP/2.0\" 200 4735 \"https://127.0.0.1:3333/login?next=%2F\" Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:145.0) Gecko/20100101 Firefox/145.0\""
time="2025-12-06T14:44:44Z" level=info msg="127.0.0.1 - - [06/Dec/2025:14:44:44 +0000] \"GET /css/dist/gophish.css HTTP/2.0\" 200 52514 \"https://127.0.0.1:3333/login?next=%2F\" Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:145.0) Gecko/20100101 Firefox/145.0\""
time="2025-12-06T14:44:45Z" level=info msg="127.0.0.1 - - [06/Dec/2025:14:44:44 +0000] \"GET /js/dist/vendor.min.js HTTP/2.0\" 200 324943 \"https://127.0.0.1:3333/login?next=%2F\" Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:145.0) Gecko/20100101 Firefox/145.0\""
time="2025-12-06T14:44:45Z" level=info msg="127.0.0.1 - - [06/Dec/2025:14:44:45 +0000] \"GET /images/favicon.ico HTTP/2.0\" 200 1150 \"https://127.0.0.1:3333/login?next=%2F\" Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:145.0) Gecko/20100101 Firefox/145.0\""

```

On lance le programme avec la commande ‘sudo ./gophish’
NB : Lors du premier lancement, un mot de passe vous sera donné afin de vous connecter avec admin/votre_mot_de_passe

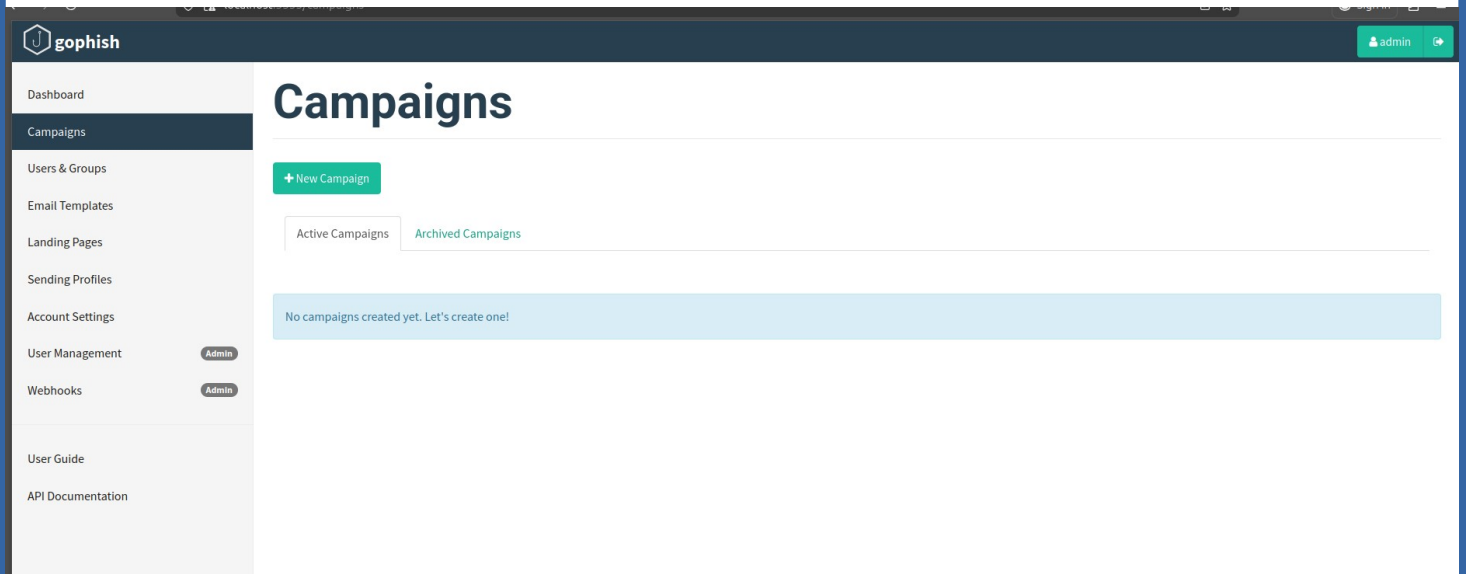


Please sign in

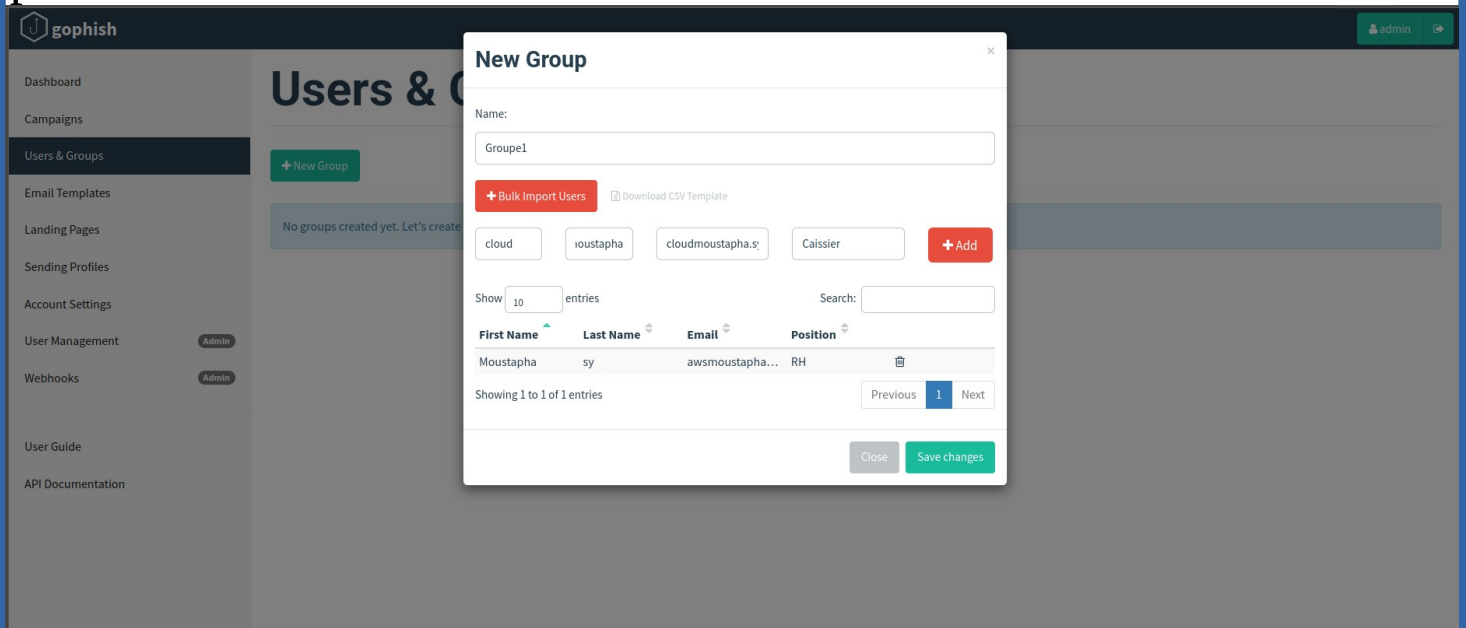
Sign in

Une fois lancé le programme gophish, on se rend dans le navigateur et saisi l'adresse <https://localhost:3333> , puis se connecter avec notre login et mot de passe (qui sera changer apres)

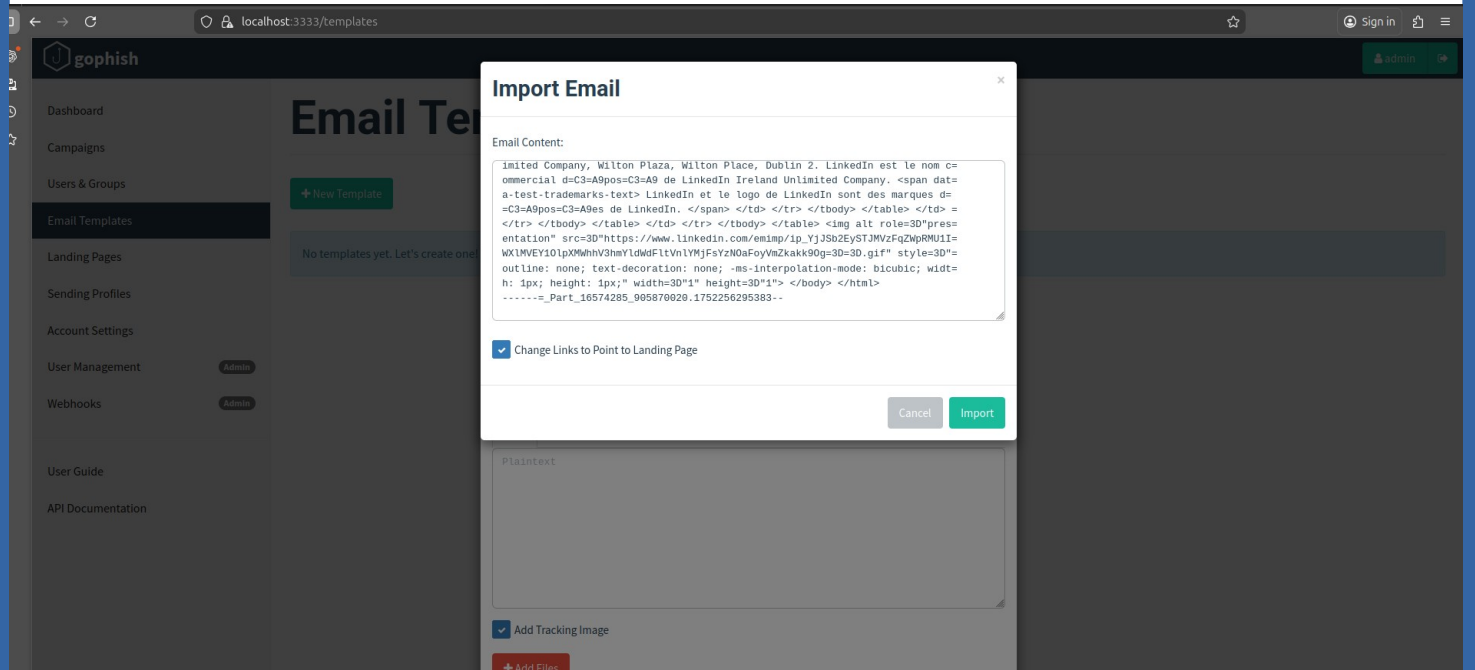
Mise en place de la campagne



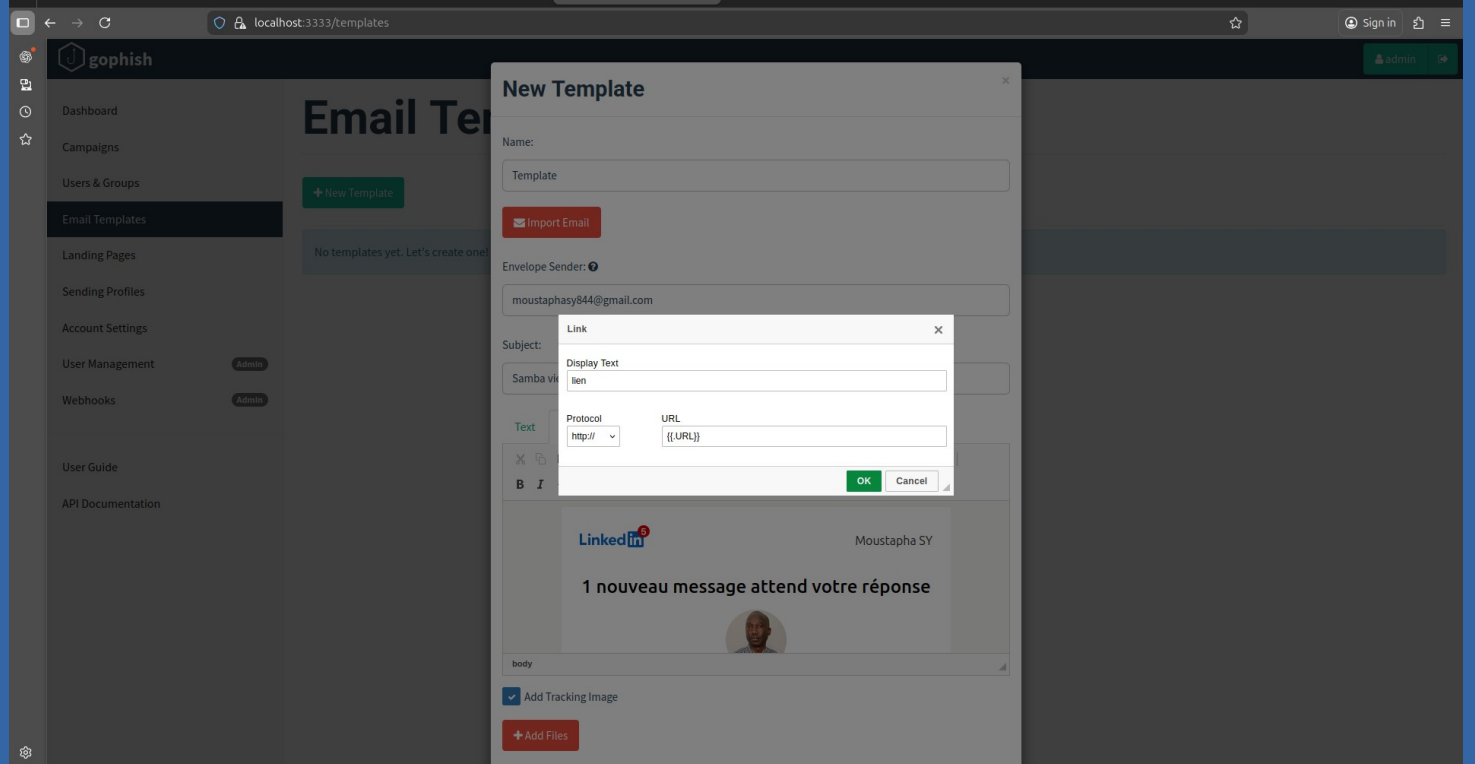
Avant de créer la campagne, on doit d'abord créer un groupe d'utilisateurs, un email template, un landing page et un sending profile.



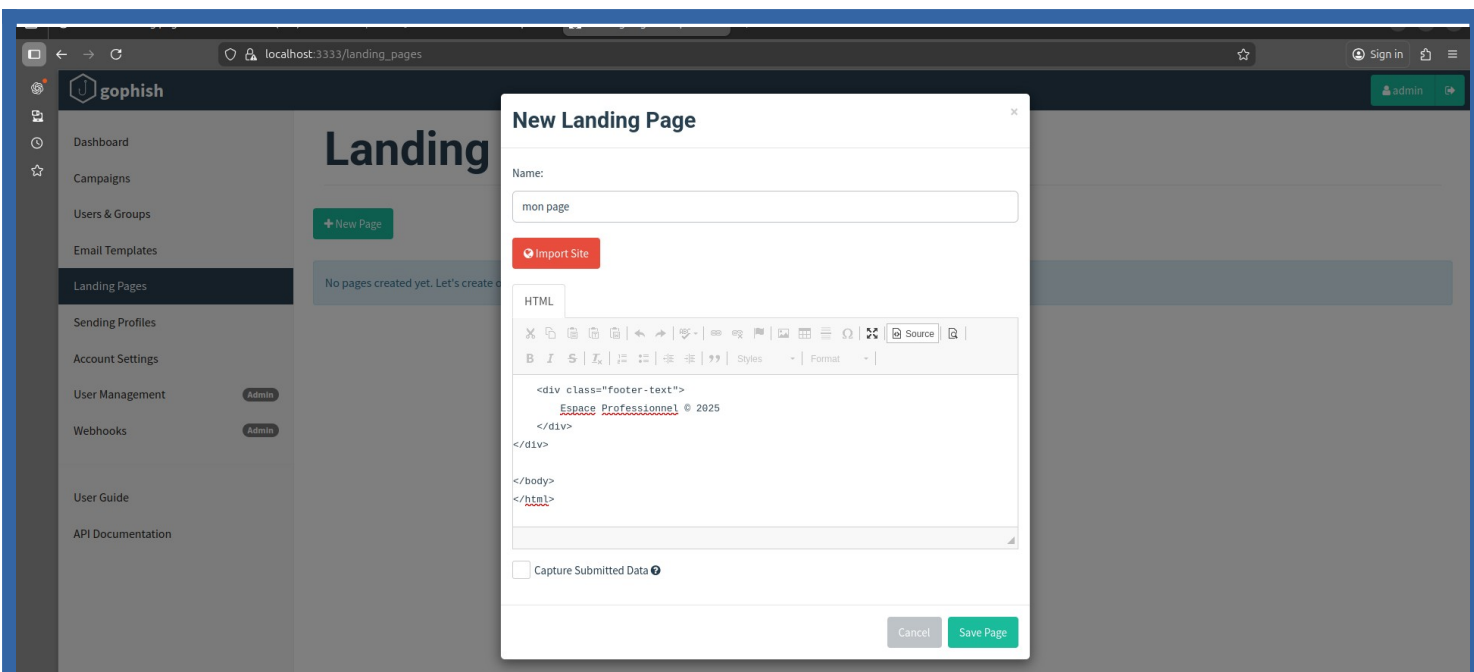
Ici nous avons créer un groupe nommé 'groupe1' avec deux utilisateurs



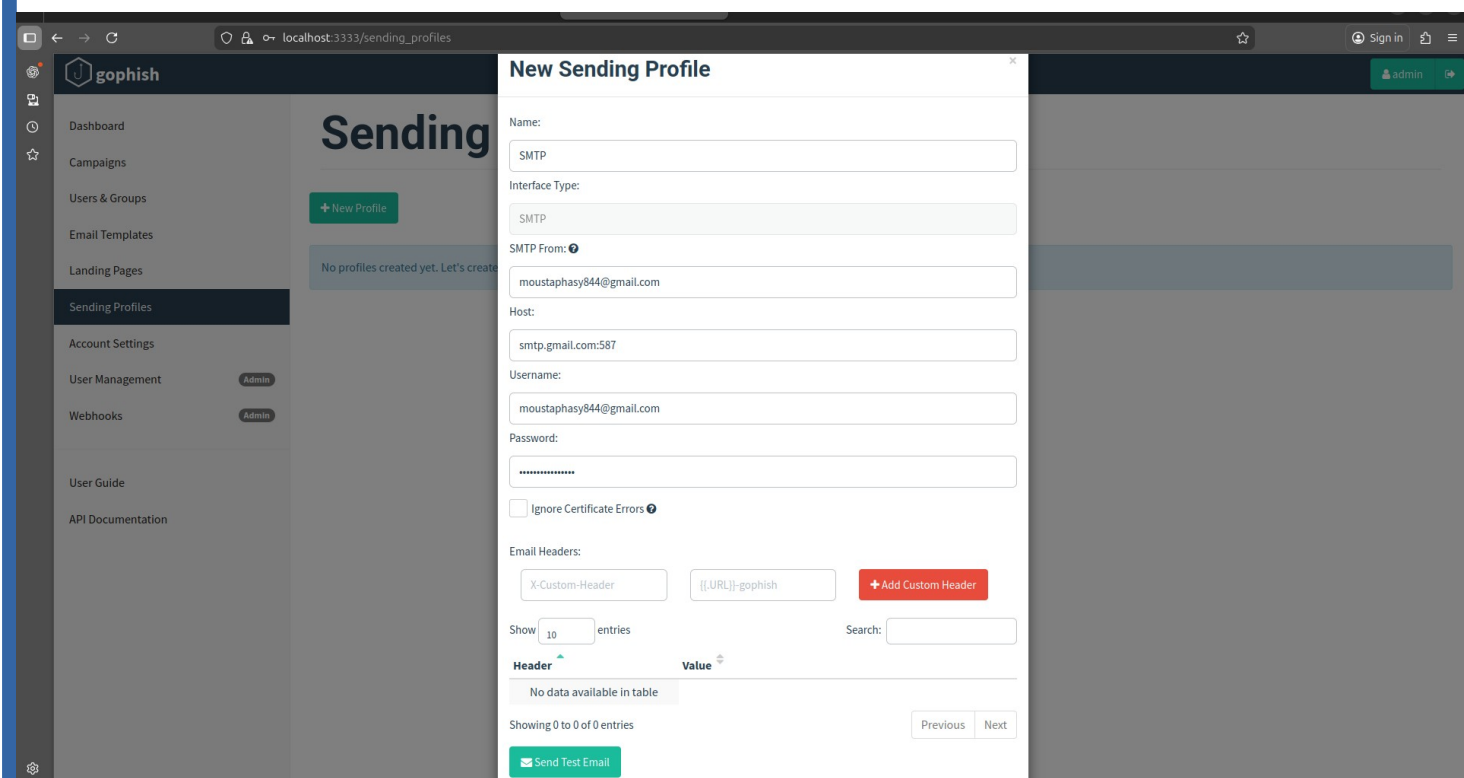
Ensuite, on a créer une email template.



Toujours dans l'email template , on ajoute l'url en mettant {{.URL}} (cette url sera spécifier lors de la création de la campagne)



Après l'email template , ici on va créer notre landing page.
Le landing page cest ce que verra l'utilisateur après avoir cliquer sur le lien, dans notre cas c'est une page de connexions.



Ici en crée le sending profile, qui est le profile de celui qui va envoyer le message.

Pour le username, il faut mettre l'adresse email de l'expéditeur, et le mot de passe , cest le mot de passe application qui sera générer dans <https://myaccount.google.com/apppasswords> .

New Campaign

Name:

Email Template:

Landing Page:

URL:

Launch Date:

Send Emails By (Optional):

Sending Profile:

Groups:

Après tout ca faite , on peut maintenant créer la campagne , en mettant comme url notre adresse ip (ou nom de domaine si existe)

Results for campaign1

Back Export CSV Complete Delete Refresh

Campaign Timeline

Email Sent: 2 | Email Opened: 0 | Clicked Link: 0 | Submitted Data: 0 | Email Reported: 0

Details

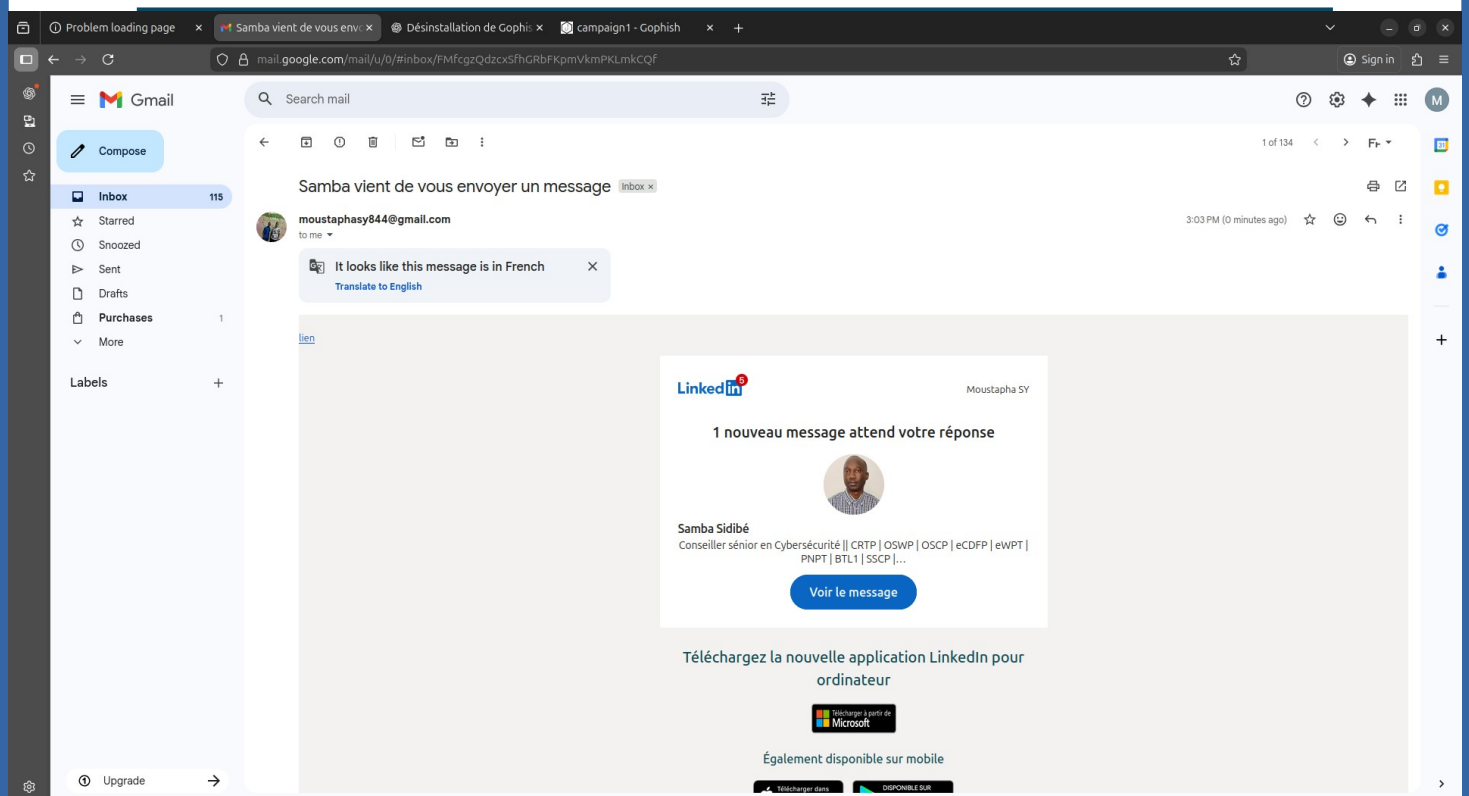
Show 10 entries

First Name	Last Name	Email	Position	Status	Reported
cloud	moustapha	cloudmoustapha.sy@gmail.com	Caissier	Email Sent	
Moustapha	sy	awsmoustapha@gmail.com	RH	Email Sent	

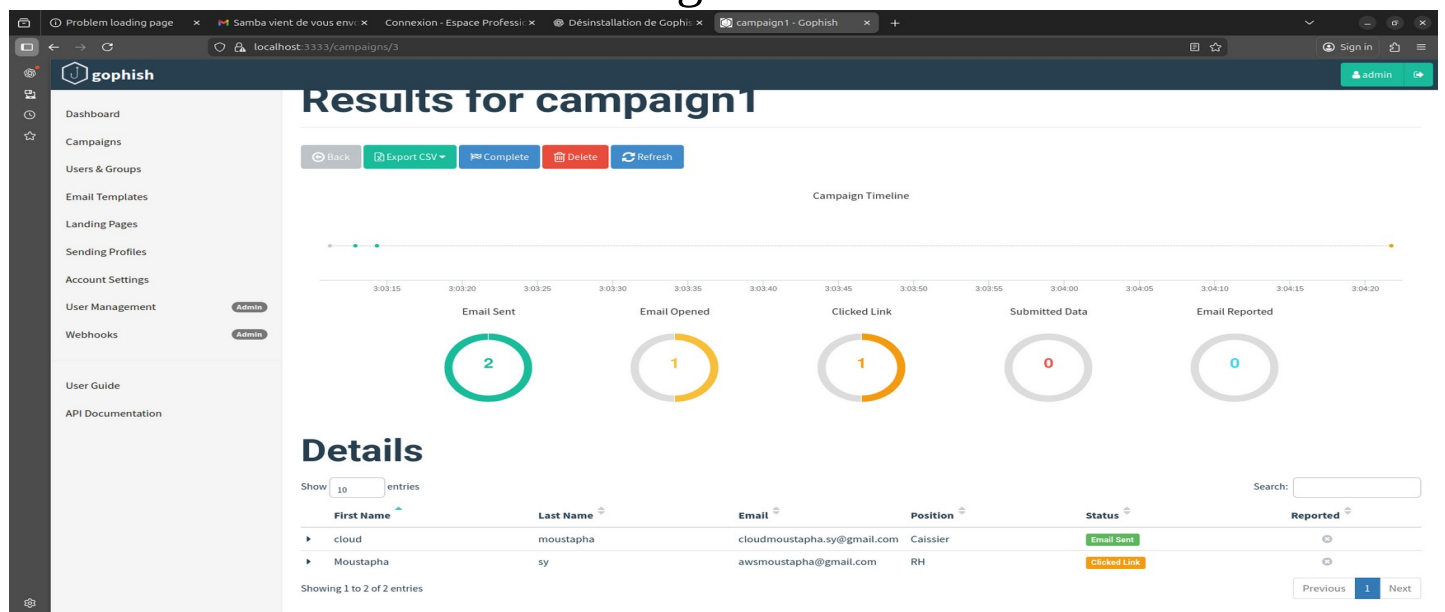
Showing 1 to 2 of 2 entries

Previous 1 Next

Collecte des clics et réponses des utilisateurs



voici l'email qui a été envoyer(le danger se trouve quand l'utilisateur clic sur 'voir message')



Dans le resultat de la campagne, on peut voir que l'email a été envoyer par deux utilisateurs et que l'une a cliquer sur le lien.

Connexion à votre espace

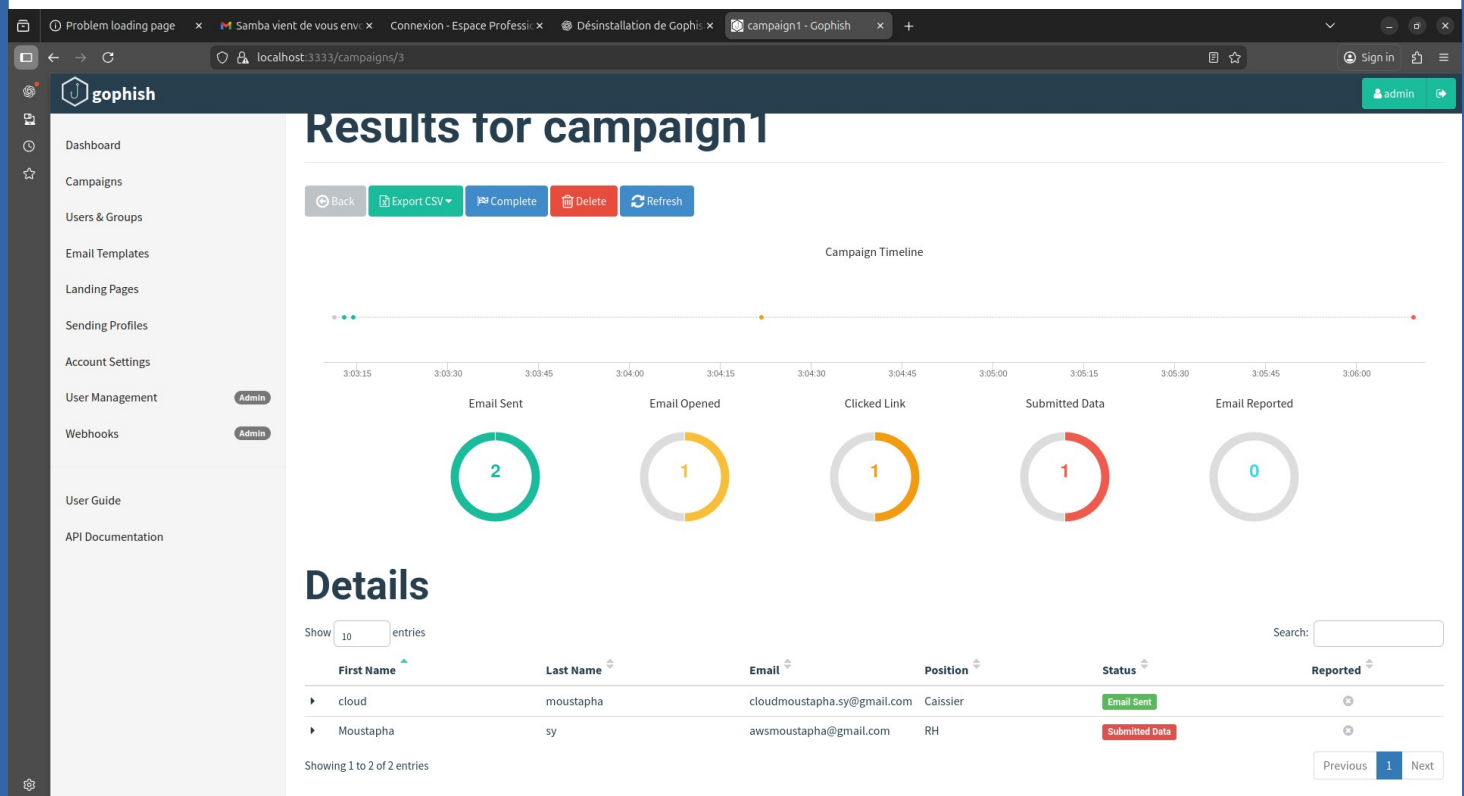
Adresse email

Mot de passe

Se connecter

Espace Professionnel © 2025

Une fois cliquer l'utilisateur verra ceci



D'apres les résultat, l'utilisateur a renseigner ces informations

gophish

Dashboard

Campaigns

Users & Groups

Email Templates

Landing Pages

Sending Profiles

Account Settings

User ManagementAdmin

WebhooksAdmin

User Guide

API Documentation

admin

First NameLast NameEmailPositionStatusReported

cloudmoustaphacloudmoustapha.sy@gmail.comCaissierEmail Sent

Moustaphasyawsmoustapha@gmail.comRHSubmitted Data

Timeline for Moustapha sy

Email: awsmoustapha@gmail.com

Result ID: Or5s0Jz

Campaign Created

December 6th 2025 3:03:11 pm

Email Sent

December 6th 2025 3:03:14 pm

Clicked Link

December 6th 2025 3:04:21 pm

Submitted Data

December 6th 2025 3:06:09 pm

Replay Credentials

View Details

Parameter	Value(s)
password	Teste123!
username	awsmoustapha@gmail.com

Showing 1 to 2 of 2 entries

Previous1Next

Et on peut voir les informations de l'utilisateur comme son username et mot de passe.

Plan de sensibilisation

Suite à la campagne de phishing réaliser via Gophish, il est essentiel en premier lieu d'informer le personnel sur les méthodes utilisées par les attaquants, les conséquences possibles d'un mail frauduleux. Une communication claire, accompagnée de fiche simple et de message interne, permet de rappeler régulièrement les réflexes essentiels. Il est également nécessaire de mettre en place un canal de signalement des emails suspects afin d'encourager les utilisateurs à alerter rapidement l'équipe informatique. Aussi les campagnes de phishing doivent être faite de façons régulières. Enfin, des mesures de techniques anti-phishing devrait être mis en place afin d'ajouter une couche supplémentaire de sécurité.

Conclusion

Cette simulation de phishing a permis de mettre en évidence la vulnérabilité persistante du personnel face aux attaques d'ingénierie sociale. Malgré le faible nombre de personnes ciblées, le fait qu'un employé ait cliqué sur le lien frauduleux et renseigné ses identifiants démontre qu'un attaquant aurait pu obtenir un accès critique en conditions réelles. Ce test confirme que la sensibilisation doit rester une priorité stratégique pour une organisation. Les résultats obtenus servent ainsi de base à la mise en place d'un programme de formation adapté, visant à renforcer les réflexes de vérification, améliorer la détection des messages suspects et instaurer une culture de vigilance durable. En poursuivant régulièrement ce type de campagne et en sensibilisant le personnel aux bonnes pratiques, une entreprise pourra significativement réduire les risques liés aux tentatives de phishing futures.