

Projet de sensibilisation sur le phising.
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 executable

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 groupe d'utilisateur

Figure 10 : Creation du template email

Figure 11 : modification de la partie url

Figure 12 : Création du landing page

Figure 13 : Création du sending profile

Figure 14 : Création de la campagne

Figure 15 : Première résultat

Figure 16 : Ouverture de l'email

Figure 17 : Observation apres ouverture

Figure 18 : Renseignement des informations confidentielles

Figure 19 : Observation final

Résumé

Une campagne de phising a été simuler 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 où 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 redirigé quand il aura cliqué sur le lien.

Sending profile : Le profil de celui qui envoie l'email.

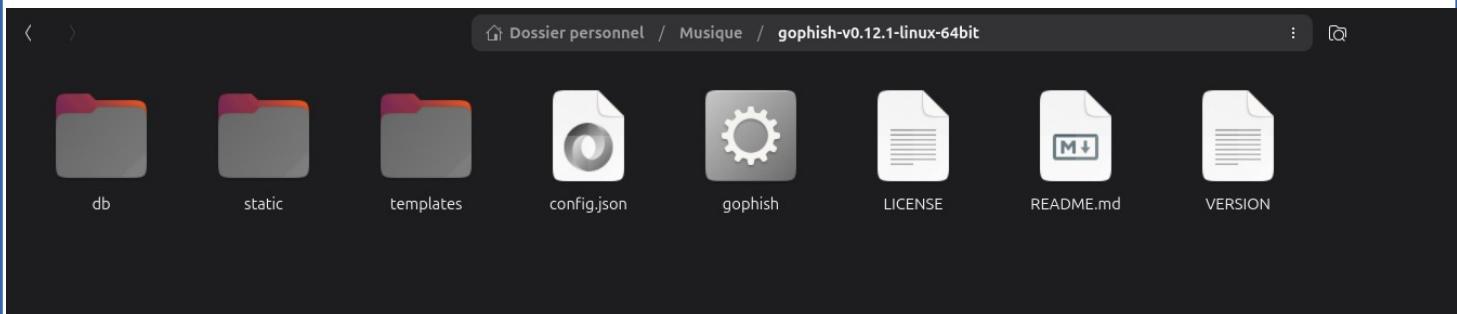
Introduction Général

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$ 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
moustapha@moustapha:~/Musique/gophish-v0.12.1-linux-64bit$ nano config.json
GNU nano 8.3
{
    "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 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

admin

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

The screenshot shows the 'Campaigns' section of the gophish web application. On the left, a sidebar menu includes 'Dashboard', 'Campaigns' (which is selected and highlighted in dark blue), 'Users & Groups', 'Email Templates', 'Landing Pages', 'Sending Profiles', 'Account Settings', 'User Management' (with an 'Admin' badge), 'Webhooks' (with an 'Admin' badge), 'User Guide', and 'API Documentation'. The main content area has a title 'Campaigns' and a green button '+ New Campaign'. Below it are tabs for 'Active Campaigns' and 'Archived Campaigns', with 'Active Campaigns' currently selected. A message at the bottom states 'No campaigns created yet. Let's create one!'. The top right corner shows a user icon and the word 'admin'.

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

The screenshot shows the 'New Group' dialog box over a blurred background of the 'Users & Groups' page. The dialog has a title 'New Group'. It contains a 'Name:' input field with 'Groupe1' typed in. Below it is a red button '+ Bulk Import Users' and a link 'Download CSV Template'. There are four buttons labeled 'cloud', 'ioustapha', 'cloudmoustapha.s.', and 'Caissier', with the last one being red. Underneath are buttons for 'Show' (set to 10) and 'Search'. A table header row shows columns for 'First Name', 'Last Name', 'Email', and 'Position'. One entry is visible: 'Moustapha sy awsmoustapha... RH'. At the bottom are 'Previous' and 'Next' buttons, and at the very bottom are 'Close' and 'Save changes' buttons.

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

The screenshot shows the gophish web application interface. On the left, there's a sidebar with various menu items like Dashboard, Campaigns, Users & Groups, Email Templates, Landing Pages, Sending Profiles, Account Settings, User Management, and Webhooks. The 'Email Templates' item is currently selected. In the center, there's a large button labeled '+ New Template'. Below it, a message says 'No templates yet. Let's create one!'. A modal window titled 'Import Email' is open, displaying raw HTML code for a LinkedIn phishing template. The code includes a logo for LinkedIn and a link to a landing page. Below the code, there's a checkbox labeled 'Change Links to Point to Landing Page'. At the bottom of the modal are 'Cancel' and 'Import' buttons. A preview window below the modal shows the plain text version of the email body.

Ensuite, on a créer une email template.

The screenshot shows the 'New Template' dialog box. It has fields for 'Name' (set to 'Template'), 'Envelope Sender' (set to 'moustaphasy844@gmail.com'), and 'Subject' (set to 'Samba vir'). A 'Link' dialog is open, showing a 'Display Text' field with 'lien' and a 'URL' field with '{{.URL}}'. The main preview window shows a LinkedIn message with a placeholder URL. Below the preview, there are buttons for 'Add Tracking Image' and 'Add Files'.

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

The screenshot shows the Gophish application's landing page creation interface. On the left, there's a sidebar with various administrative options like Dashboard, Campaigns, Users & Groups, Email Templates, Landing Pages (selected), Sending Profiles, Account Settings, User Management, Webhooks, User Guide, and API Documentation. The main area has a title 'Landing' and a button '+ New Page'. A modal window titled 'New Landing Page' is open, prompting for a 'Name' (set to 'mon page') and providing an 'Import Site' button. Below is a rich-text editor with an HTML tab showing the following code:

```
<div class="footer-text">  
    Espace Professionnel © 2025  
</div>  
  
</body>  
</html>
```

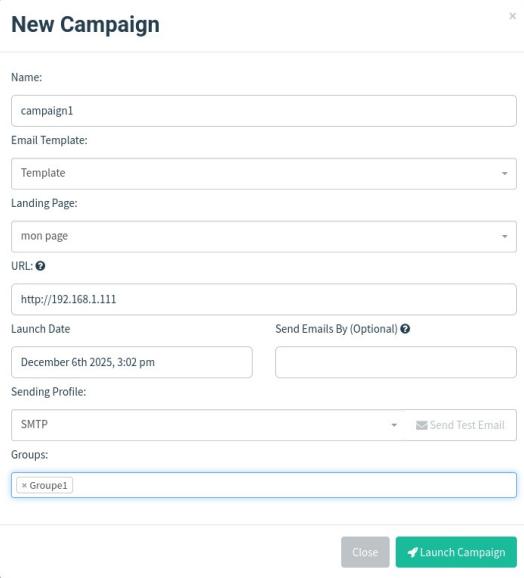
At the bottom of the modal are 'Cancel' and 'Save Page' buttons.

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.

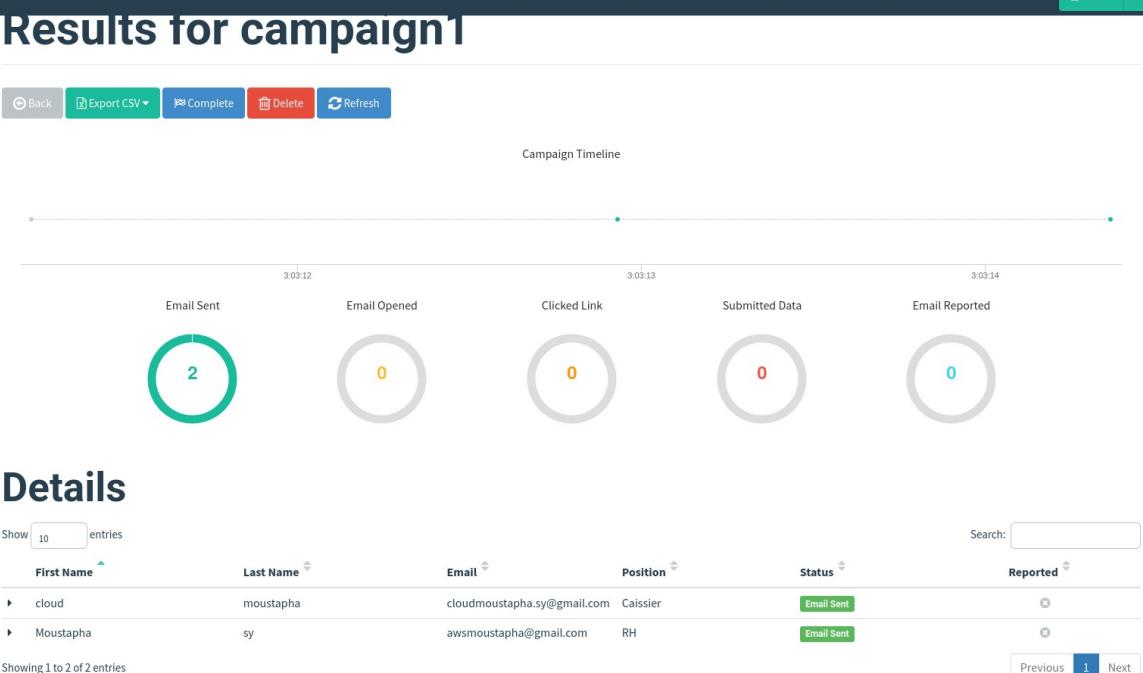
The screenshot shows the Gophish application's sending profile creation interface. The sidebar is identical to the previous one. The main area has a title 'Sending' and a button '+ New Profile'. A modal window titled 'New Sending Profile' is open, prompting for a 'Name' (set to 'SMTP'), 'Interface Type' (set to 'SMTP'), 'SMTP From:' (set to 'moustaphasy844@gmail.com'), 'Host' (set to 'smtp.gmail.com:587'), 'Username' (set to 'moustaphasy844@gmail.com'), and 'Password' (set to '*****'). There's also a checkbox 'Ignore Certificate Errors'. Below is a section for 'Email Headers' with a table and a '+ Add Custom Header' button. At the bottom are 'Show 10 entries', 'Search', 'Header', 'Value', and a table with the message 'No data available in table'. The footer includes 'Previous' and 'Next' buttons, and a 'Send Test Email' button.

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/app passwords> .

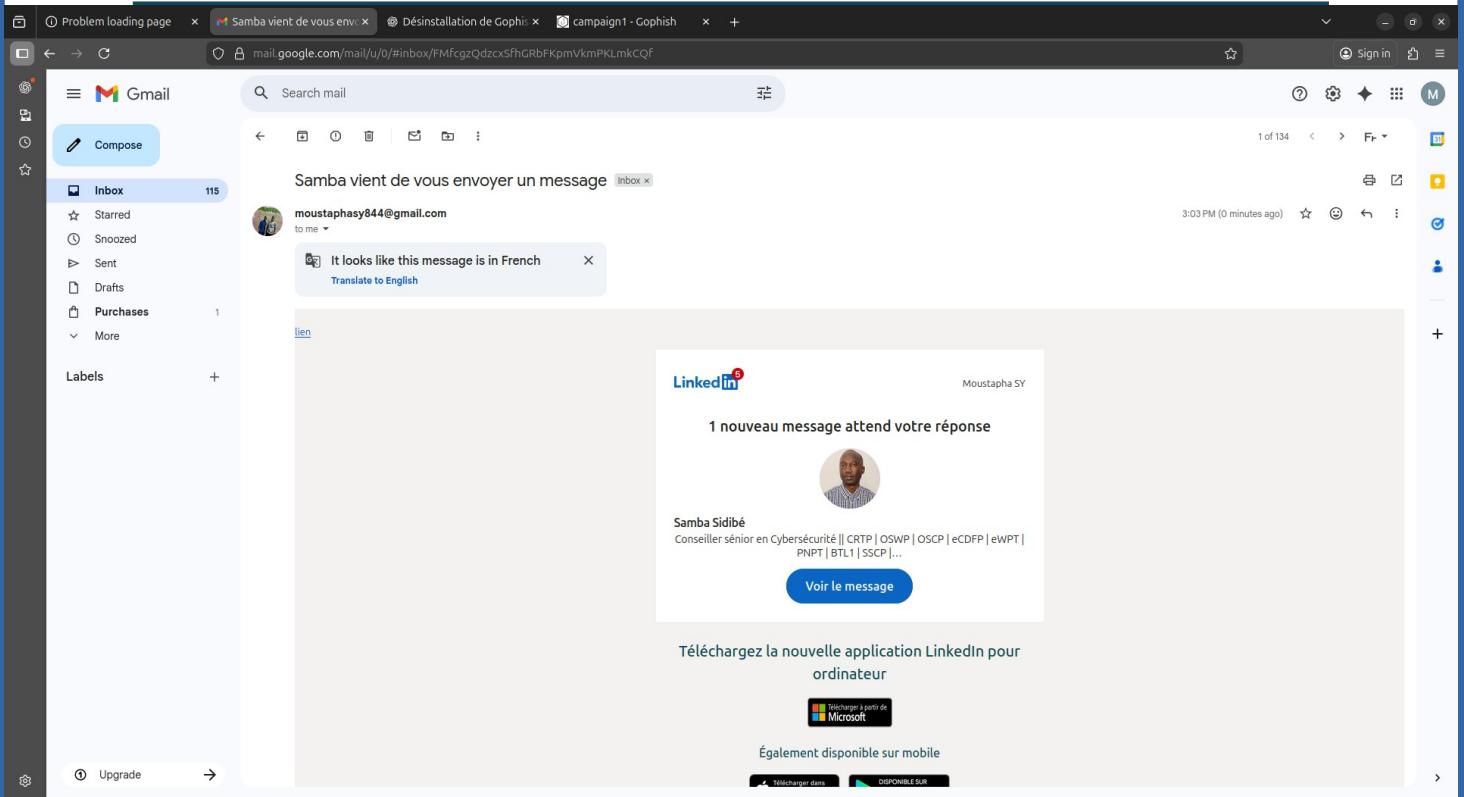


Apres tout ca faite , on peut maintenant créer la campagne , en mettant comme url notre adresse ip (ou nom de domaine si existe)



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

Collecte des clics et réponses des utilisateurs



Samba vient de vous envoyer un message [Inbox](#)

moustaphasy844@gmail.com to me

It looks like this message is in French [Translate to English](#)

lien

LinkedIn Moustapha SY

1 nouveau message attend votre réponse

Samba Sidibé
Conseiller senior en Cybersécurité || CRTP | OSWP | OSCP | eCDFP | eWPT |
PNPT | BT1 | SSCP | ...

[Voir le message](#)

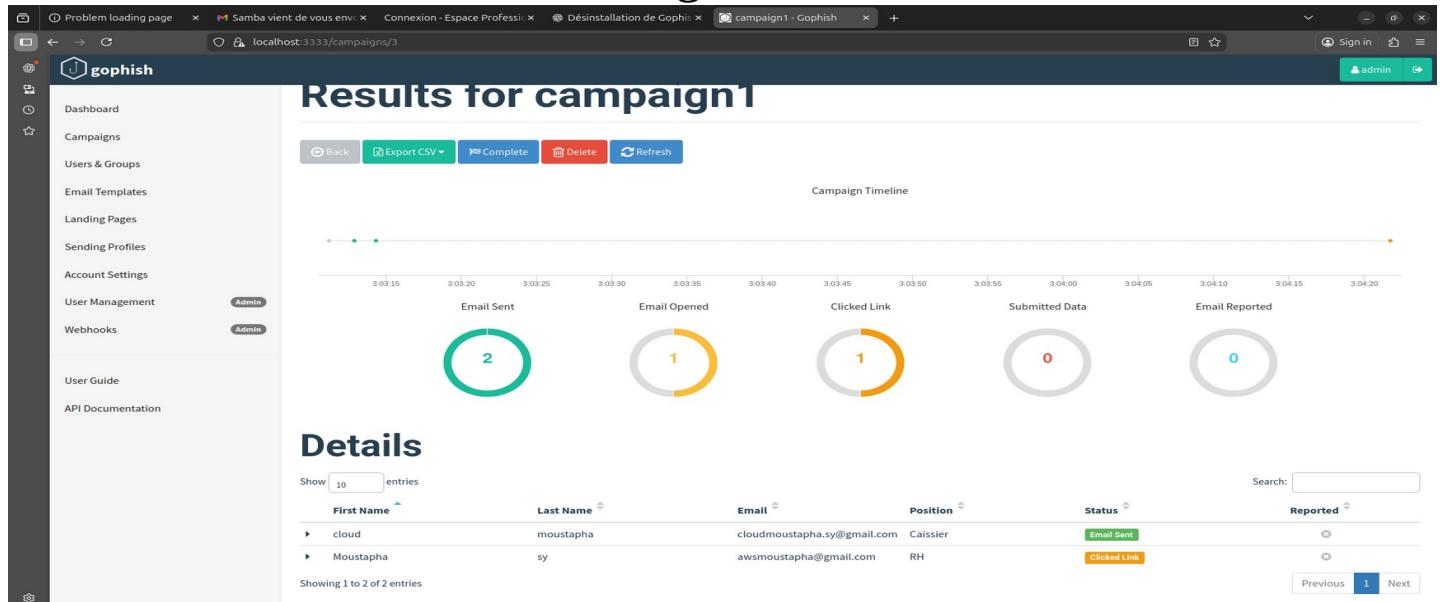
Téléchargez la nouvelle application LinkedIn pour ordinateur

Microsoft

Également disponible sur mobile

[Télécharger dans](#) [DISPONIBLE SUR](#)

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



Results for campaign1

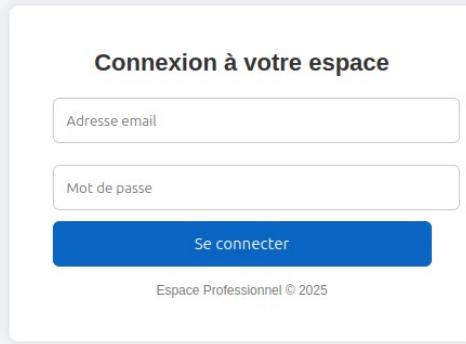
Campaign Timeline

Event	Count
Email Sent	2
Email Opened	1
Clicked Link	1
Submitted Data	0
Email Reported	0

Details

First Name	Last Name	Email	Position	Status
cloud	moustapha	cloudmoustapha.sy@gmail.com	Caisseier	Email Sent
Moustapha	sy	awsmostapha@gmail.com	RH	Clicked Link

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



Une fois cliquer l'utilisateur verra ceci

Results for campaign1

Campaign Timeline

First Name	Last Name	Email	Position	Status	Reported
cloud	moustapha	cloudmoustapha.sy@gmail.com	Caisse	Email Sent	
Moustapha	sy	awsmostapha@gmail.com	RH	Submitted Data	

Showing 1 to 2 of 2 entries

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

The screenshot shows the Gophish web application interface. On the left is a sidebar with navigation links: Dashboard, Campaigns, Users & Groups, Email Templates, Landing Pages, Sending Profiles, Account Settings, User Management (marked as Admin), Webhooks (marked as Admin), User Guide, and API Documentation. The main content area displays a table of users with columns: First Name, Last Name, Email, Position, Status, and Reported. Two entries are shown: 'cloud' (Last Name: moustapha, Email: cloudmoustapha.sy@gmail.com, Position: Caissier, Status: Email Sent) and 'Moustapha' (Last Name: sy, Email: awsmostapha@gmail.com, Position: RH, Status: Submitted Data). Below this is a section titled 'Timeline for Moustapha sy' with the following events:

- Campaign Created (December 6th 2025 3:03:11 pm)
- Email Sent (December 6th 2025 3:03:14 pm)
- Clicked Link (Ubuntu, Firefox (Version: 145.0)) (December 6th 2025 3:04:21 pm)
- Submitted Data (Ubuntu, Firefox (Version: 145.0)) (December 6th 2025 3:06:09 pm)

A green button labeled 'Replay Credentials' is present. At the bottom, there's a table titled 'View Details' with columns 'Parameter' and 'Value(s)' containing 'password' (Value: Teste123!) and 'username' (Value: awsmostapha@gmail.com). Navigation buttons for 'Previous' and 'Next' are at the bottom right.

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 réalisé 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 faites de façons régulières. Enfin, des mesures de techniques anti-phishing devraient 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.