



## RAPPORT DE SIMULATION D'UNE ATTAQUE PAR PHISHING

Présentée par ; Aminata Niang et Fatma Ly

# 1. Introduction

- Les cyberattaques deviennent de plus en plus sophistiquées. Parmi elles, le phishing vise principalement à exploiter le facteur humain. Ce projet a pour objectif de simuler une attaque de phishing afin d'évaluer la réactivité et la vigilance des employés dans un environnement contrôlé.

## 2-Contexte et objectifs

- La direction souhaite mesurer la sensibilisation du personnel aux emails frauduleux. Le projet permet de :
  - Identifier les comportements à risque
  - Mesurer le niveau de vigilance
  - Proposer des actions de prévention

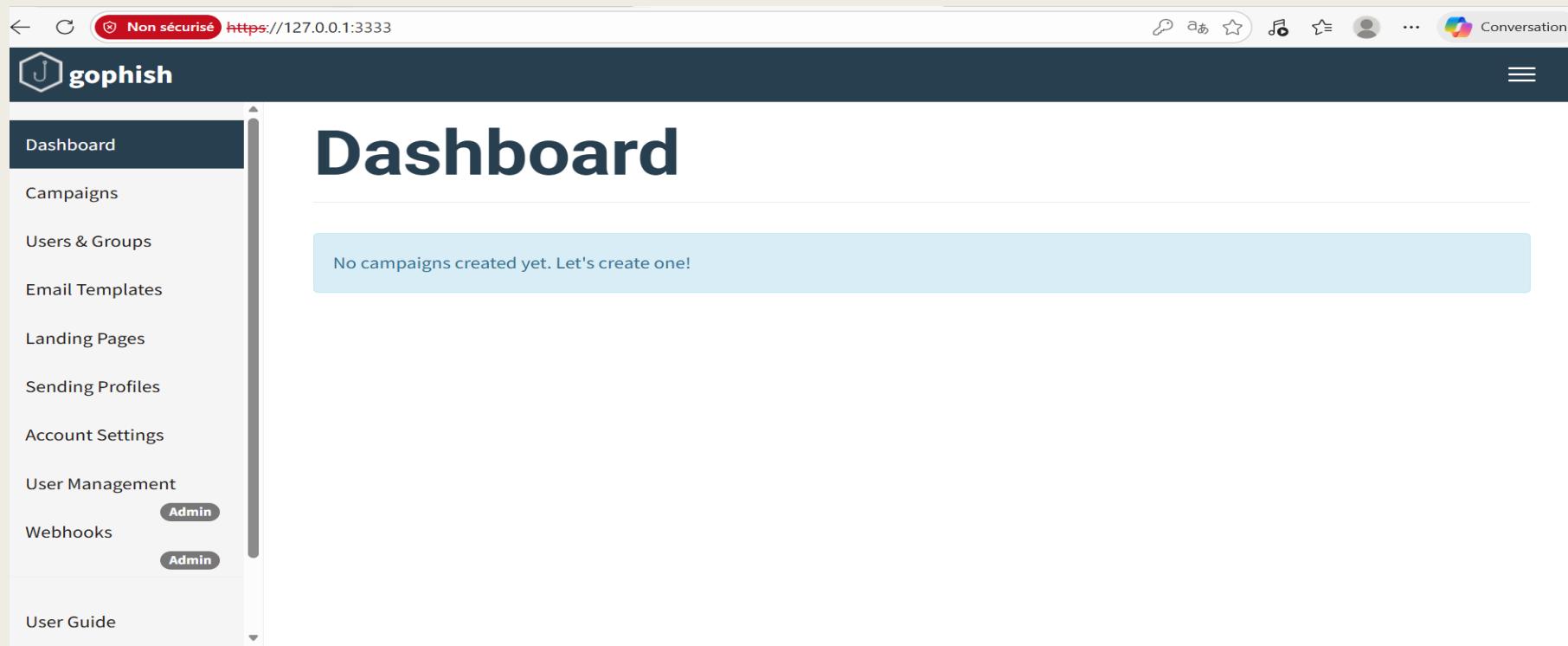
## 3-Présentation du phishing

- Le phishing consiste à envoyer des emails frauduleux ressemblant à des communications légitimes pour tromper la victime et obtenir des informations sensibles. Ces attaques utilisent souvent un sentiment d'urgence et des liens malveillants.

## 4. Méthodologie

- Nous avons utilisé le gophish version Windows pour suivre les instructions afin d'accomplir les étapes de simulation d'attaque phishing.

Apres s'être loggée , l'image ci-dessous nous montre l'interface de gophish



Le Sending Profile permet de configurer le serveur SMTP utilisé par GoPhish pour l'envoi des emails de la campagne de phishing. Cette image nous montre que l'envoi de profil a été fait avec succès.

The screenshot shows the Gophish web application interface. The title bar reads "Envoi de profils - Gophish" and the address bar shows "https://127.0.0.1:3333/sending\_profiles". The main header "gophish" has a logo icon. The left sidebar menu is visible with items like "Tableau de bord", "Campagnes", "Utilisateurs et groupes", "Modèles d'e-mails", "Pages de destination", "Envoyer de profils" (which is selected and highlighted in dark blue), "Paramètres du compte", "Gestion des utilisateurs" (with "Administrateur" role), "Webhooks" (with "Administrateur" role), and "Guide de l'utilisateur". The main content area has a large heading "Envoi de profils". A green success message box contains the text "Profil ajouté avec succès !". Below it is a teal button labeled "+Nouveau profil". The table lists one entry: "amina" (Nom), "SMTP" (Type d'interface), and "8 décembre 2025, 10h03min08s" (Date de dernière modification). The table has columns for "Nom", "Type d'interface", and "Date de dernière modification". At the bottom of the table are edit, copy, and delete icons. Navigation buttons "Précédent", "1", and "Suivant" are also present. The bottom of the screen shows a Windows taskbar with various icons and system status information.

La landing page est la page web utilisée pour simuler le site ciblé et mesurer le comportement des utilisateurs après le clic sur le lien de phishing . L'image ci-dessous nous montre que le landing pages ou page de destination a été bien créée .

The screenshot shows the Gophish web application interface. The left sidebar has a dark theme with white text and icons. The 'Landing Pages' option is highlighted in blue, indicating it is the active section. The main content area has a light background. At the top, there is a green success message: 'Page added successfully!'. Below this, there is a table with one entry:

Name	Last Modified Date	Action Buttons
google	December 8th 2025, 10:28:00 am	

Below the table, it says 'Showing 1 to 1 of 1 entries'. There are navigation buttons at the bottom right: 'Previous' (disabled), '1', and 'Next'.

Les Email Template permettent de simuler des messages de phishing réalistes en intégrant un lien unique de suivi généré par GoPhish. L'image ci-dessous nous montre que l'email a été bien créé avec succès .

The screenshot shows the GoPhish web application interface. The left sidebar has a dark theme with white text and includes links for Dashboard, Campaigns, Users & Groups, Email Templates (which is the active tab), Landing Pages, Sending Profiles, Account Settings, User Management (with an Admin badge), Webhooks (with an Admin badge), and User Guide. The main content area has a light background. At the top, there are tabs for 'Modèles d'e-mails - Gophish' and 'Code HTML GoPhish', and a browser header showing 'Non sécurisé https://127.0.0.1:3333/templates'. A success message 'Template added successfully!' is displayed in a green bar. Below it is a table with one entry:

Name	Modified Date	Action Buttons
google	December 8th 2025, 10:47:09 am	

Below the table, it says 'Showing 1 to 1 of 1 entries'. There are also navigation buttons for 'Previous', a page number '1', and 'Next'.

Les utilisateurs représentent les destinataires des emails, tandis que les groupes permettent de structurer et cibler les campagnes de phishing. L'image ci-dessous nous permet de voir que la page a été bien créée .

The screenshot shows the GoPhish web application interface. The title bar indicates the window is titled "Utilisateurs et groupes - Gophish" and the address bar shows "https://127.0.0.1:3333/groups". The main header features the "gophish" logo. On the left, a sidebar menu includes "Tableau de bord", "Campagnes", "Utilisateurs et groupes" (which is selected and highlighted in blue), "Modèles d'e-mails", "Pages de destination", "Envoi de profils", "Paramètres du compte", "Gestion des utilisateurs" (with an "Administrateur" badge), "Webhooks" (with an "Administrateur" badge), and "Guide de l'utilisateur". The main content area has a large title "Utilisateurs et groupes". A green success message box displays "Groupe ajouté avec succès !". Below it is a button labeled "+Nouveau groupe". The table lists one user group: "Google" with "1" member, last modified on "8 décembre 2025, 10h52". The table has columns for "Nom", "Nombre de membres", and "Date de modification". At the bottom, there are navigation links for "Précédent", "1", and "Suivant".

La campagne permet de simuler une attaque de phishing complète en combinant l'envoi d'emails, l'interaction utilisateur et l'analyse des résultats.  
L'image ci-dessous nous montre les résultats qu'on a pu observer.



## 5. Résultats et Interprétation.

- L'analyse montre que certains employés sont encore vulnérables. Le taux de clics révèle les points faibles et permet de cibler les actions de sensibilisation. Ces résultats servent à renforcer la politique de sécurité et à améliorer la réactivité du personnel.

# 6. Plan de sensibilisation

- Pour réduire les risques, il est proposé :
  - Des formations régulières
  - Des campagnes de phishing simulées périodiques
  - Des guides et rappels de sécurité
  - Un processus clair de signalement

# Conclusion

- Cette simulation a démontré l'importance du facteur humain dans la cybersécurité. La mise en place d'actions régulières de sensibilisation est essentielle pour réduire les risques et protéger l'entreprise contre les attaques de phishing.