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

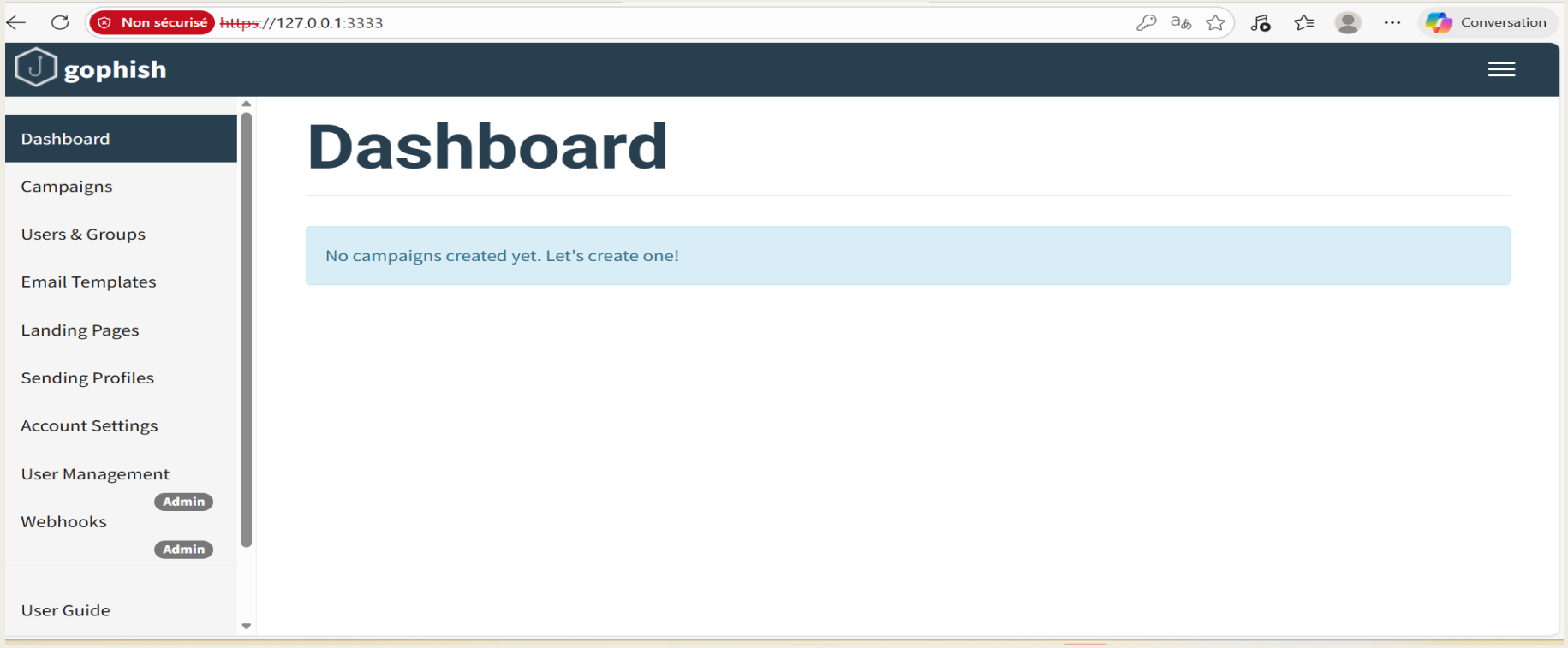
3-Présentation du phishing

- 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

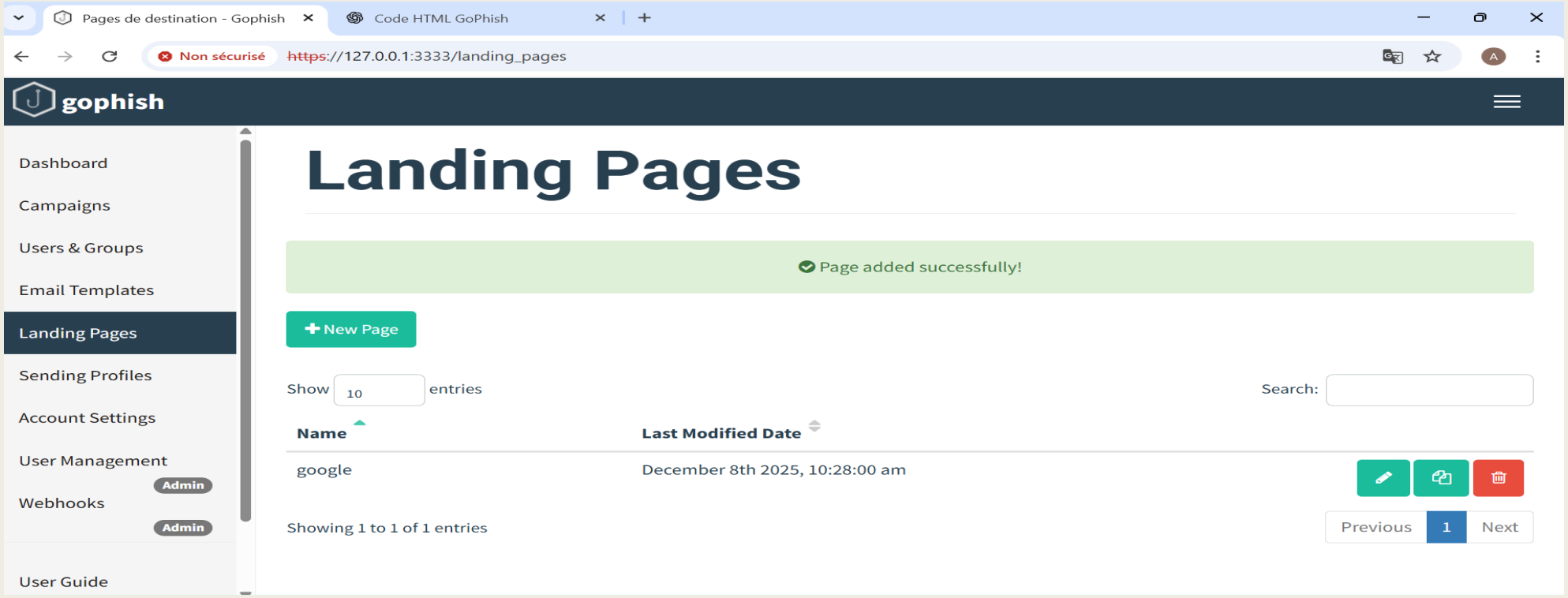
- Nous avons utilisé le gophish version Windows pour suivre les instructions afin d’accomplir les étapes de simulation d’attaque phishing.

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

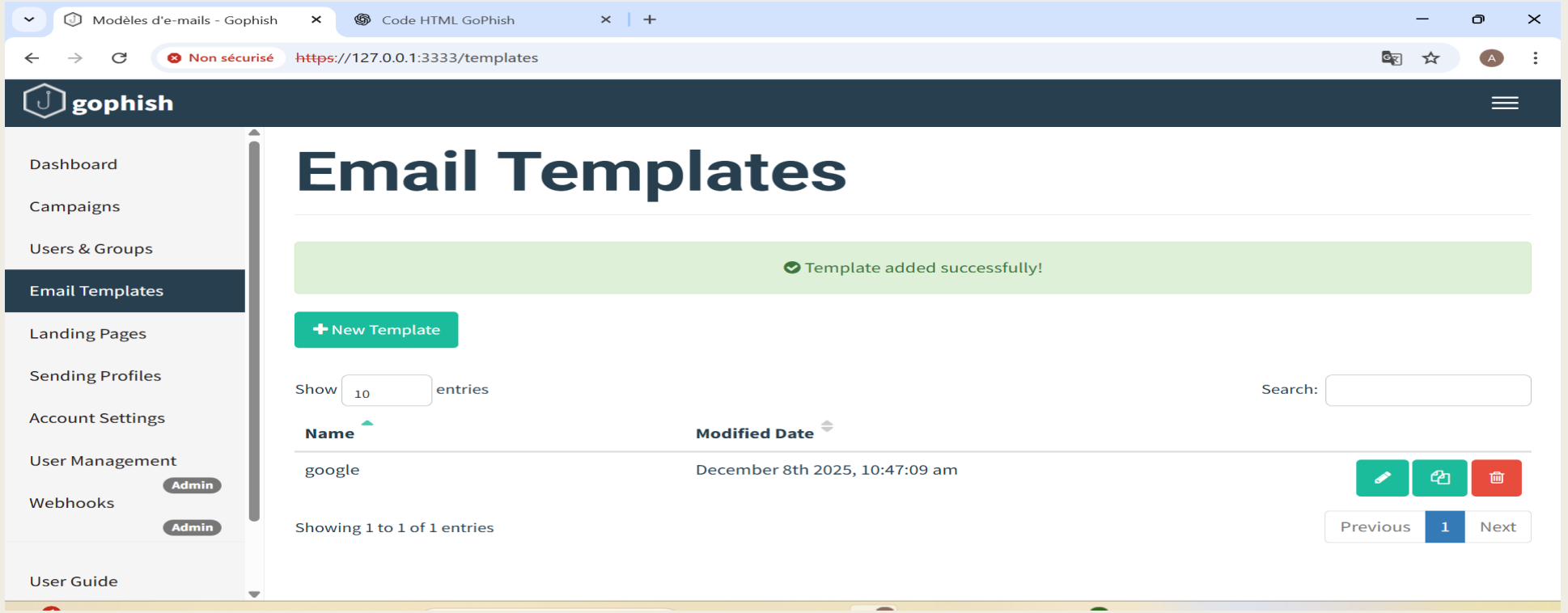


Le Sending Profile permet de configurer le serveur SMTP utilisé par GoPhish pour l'envoi des emails de la campagne de phishing. Cette image nous montre que l'envoi de profil a été faite avec succès.

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 crée .

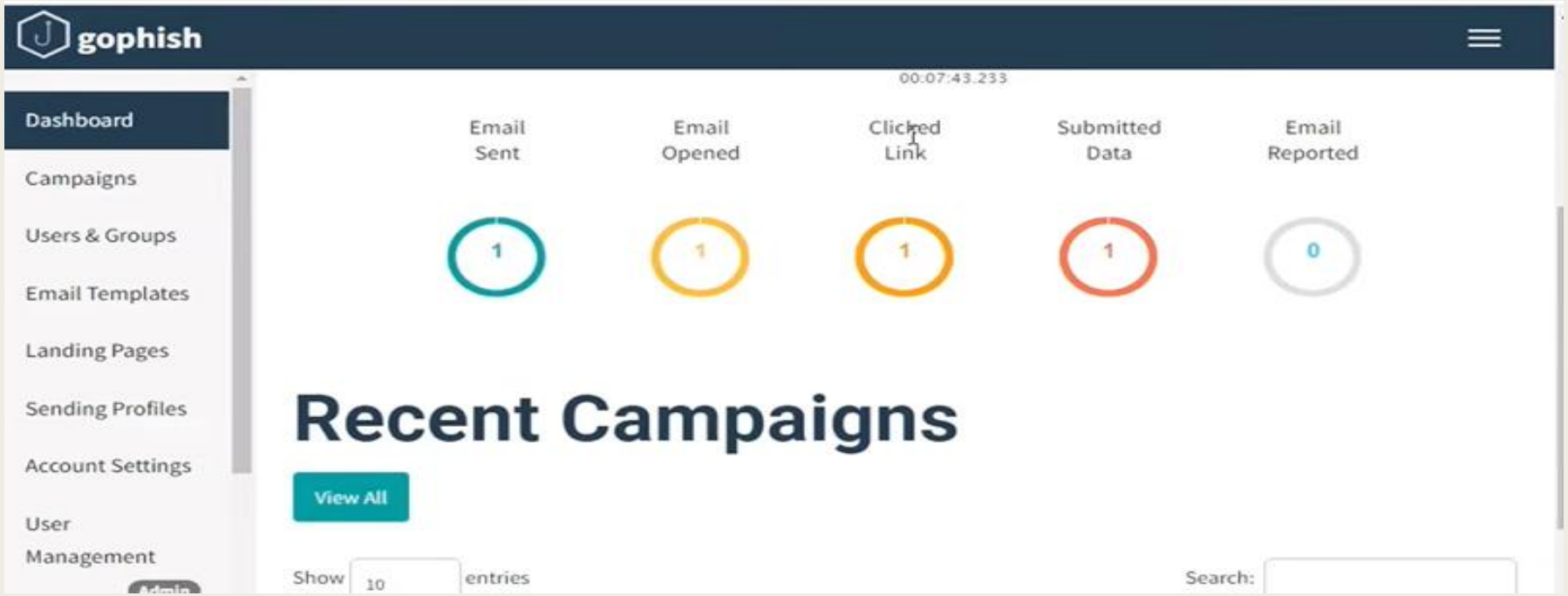


Les Email Template permettent de simuler des messages de phishing réalistes en intégrant un lien unique de suivi généré par GoPhish. L'image ci-dessous nous montre que l'email a été bien crée avec succès .



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 crée .

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.