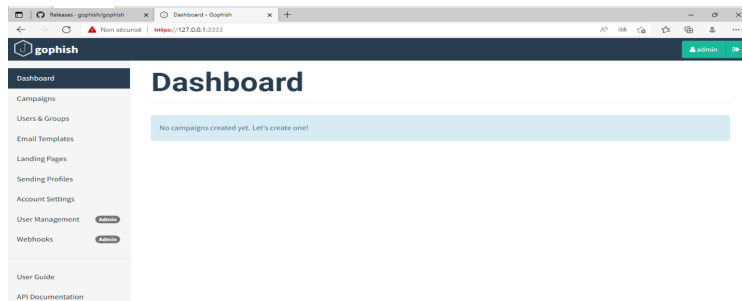


MISSION-1-CHOIX-A

DIAGOURAGA
Ibrahim

TS2SIO



1. Vous créerez un mail destiné à simuler le vols des identifiants et mots de passe windows/ou de la boîte mail des utilisateurs. (soyez malin,votre mail doit être convaincant)

admin
azerty2023

L'entreprise (Moi) envoie un e-mail aux employés, semblant provenir du service informatique.

L'e-mail indique que l'employé doit y inscrire son mot de passe et son adresse mail afin de réenregistrer les comptes dans la base de données.

Le lien dans l'e-mail dirige l'employé vers un faux site Web qui lui demande son adresse e-mail et son mot de passe actuel.

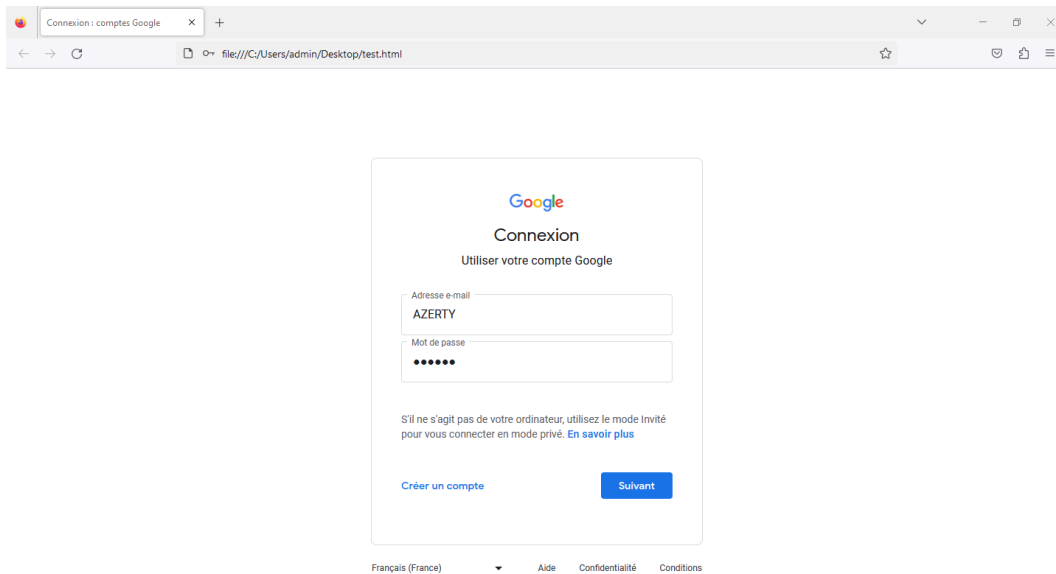
But :

Le but de cet e-mail est d'obtenir l'adresse e-mail et le mot de passe actuel de l'employé.

Idées pour le rendre plus réaliste :

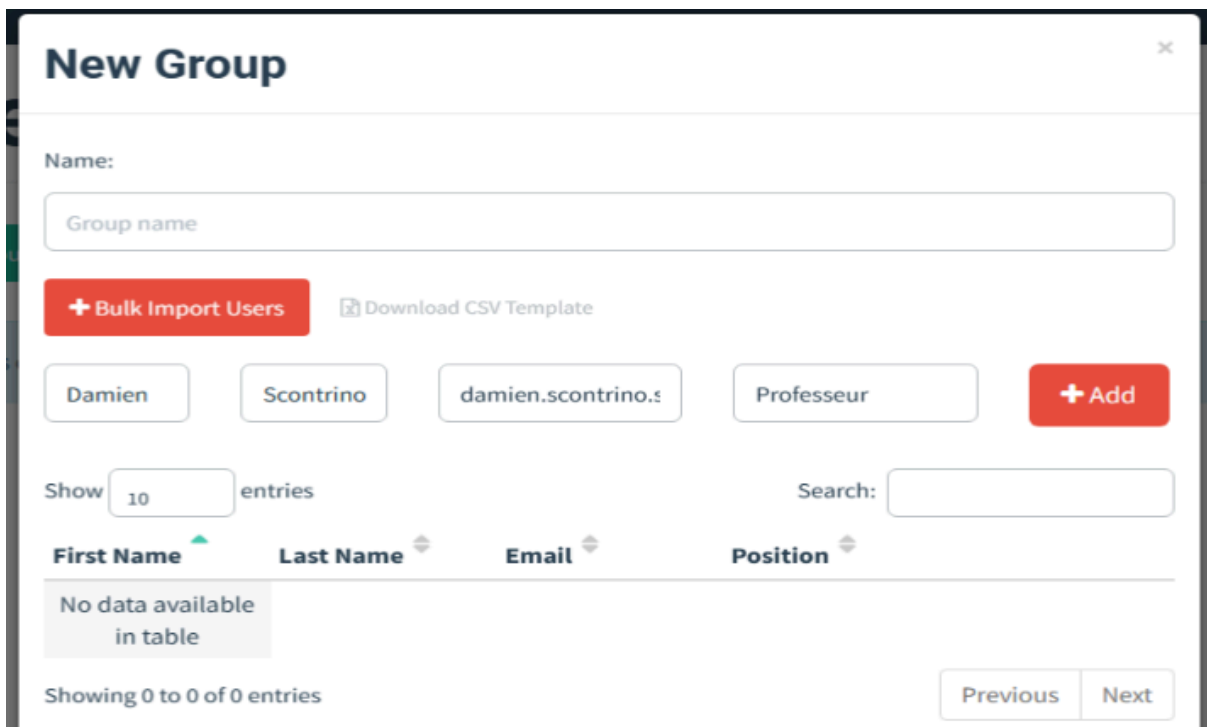
- L'e-mail devrait être envoyé à partir d'une adresse e-mail légitime du service informatique.
- L'e-mail devrait inclure un lien vers un faux site Web de connexion de l'entreprise qui ressemble exactement au site Web réel.
- L'e-mail devrait inclure une urgence, comme un avis de violation de données, pour inciter l'employé à agir rapidement.

Pour créer cette page, j'ai dû aller dans le code source . (ctrl-u)
après modifications.



The screenshot shows a web browser window with the title "Connexion : comptes Google". The address bar shows the file path "file:///C:/Users/admin/Desktop/test.html". The main content is a Google login form with the Google logo at the top, followed by the heading "Connexion" and the subtext "Utiliser votre compte Google". There are two input fields: "Adresse e-mail" containing "AZERTY" and "Mot de passe" with masked characters. Below the fields is a link "En savoir plus" and two buttons: "Créer un compte" and "Suivant". At the bottom, there are links for "Français (France)", "Aide", "Confidentialité", and "Conditions".

Création des utilisateurs (victime)



The screenshot shows a "New Group" interface. At the top is a header "New Group" with a close button. Below is a "Name:" label and a text input field containing "Group name". There are two buttons: a red "+ Bulk Import Users" and a "Download CSV Template" button with a download icon. Below these are four input fields: "Damien", "Scontrino", "damien.scontrino.s", and "Professeur", followed by a red "+ Add" button. There is a "Show" dropdown set to "10" and a "Search:" input field. Below the search field is a table header with columns: "First Name", "Last Name", "Email", and "Position". The table body contains a message "No data available in table". At the bottom, it says "Showing 0 to 0 of 0 entries" and has "Previous" and "Next" buttons.

Afin de pouvoir capturer les informations et le mot de passe.

☒ Capture Submitted Data ?
☒ Capture Passwords

Warning: Credentials are currently **not encrypted**. This means that captured passwords are stored in the database as cleartext. Be careful with this!

Création du profil (qui envoi le mail)

Edit Sending Profile

Name:

ibrahim

Interface Type:

SMTP

SMTP From: ?

ibrahim[REDACTED].sio@gmail.com

Host:

smtp.gmail.com:465

Username:

ibrahim[REDACTED].sio@gmail.com

Password:

☒ Ignore Certificate Errors ?

(Création de mot de passe pour application).

Pour que Gophish puisse se connecter à mon adresse mail (attaquant)

Send Test Email


Send Test Email to:

Ibrahim

ibrahim.sio@gmail

Position

Cancel

 Send

Je peux enfin envoyer des mail de phishing.

This is an email letting you know that your gophish configuration was successful.

Here are the details:

Who you sent from: ibrahim.sio@gmail.c

Who you sent to:

First Name: Ibrahim

Last Name:

Now go send some phish!

MAIL TYPE:

Objet : Réenregistrement des comptes Gmail - Cleanergy

Bonjour,

Nous vous informons que nous procédons à une mise à jour de notre base de données. Dans le cadre de cette mise à jour, nous vous demandons de réenregistrer vos informations de connexion.

Pour ce faire, veuillez cliquer sur le lien ci-dessous et saisir vos informations d'identification.

[Lien vers le faux site Web]

Ce processus est nécessaire pour garantir la sécurité de vos informations.

Merci pour votre compréhension.

L'équipe informatique de Cleanergy

Création de la page.

The screenshot shows an email creation interface. At the top, there is a 'Name:' field with a 'Template name' input. Below it is a red 'Import Email' button. The 'Envelope Sender:' field shows 'First Last <test@example.com>'. The 'Subject:' field is partially visible. A 'Text' toolbar is on the left. A 'Link' dialog box is open in the center, with 'Display Text' set to '[Cliquez ici]', 'Protocol' set to 'http://', and 'URL' set to '{{URL}}'. The dialog has 'OK' and 'Cancel' buttons. The email body contains the following text: 'Nous vous informons que nous procédons à une mise à jour de notre base de données. Dans le cadre de cette mise à jour, nous vous demandons de réenregistrer vos informations de connexion. Pour ce faire, veuillez cliquer sur le lien ci-dessous et saisir vos informations d'identification. [Lien vers le faux site Web]'. At the bottom, there is a checkbox for 'Add Tracking Image' and a red 'Add Files' button.

Résultat du mail

Objet : Réenregistrement des comptes Gmail - Cleanergy

Bonjour,

Nous vous informons que nous procédons à une mise à jour de notre base de données. Dans le cadre de cette mise à jour, nous vous demandons de réenregistrer vos informations de connexion.

Pour ce faire, veuillez cliquer sur le lien ci-dessous et saisir vos informations d'identification.

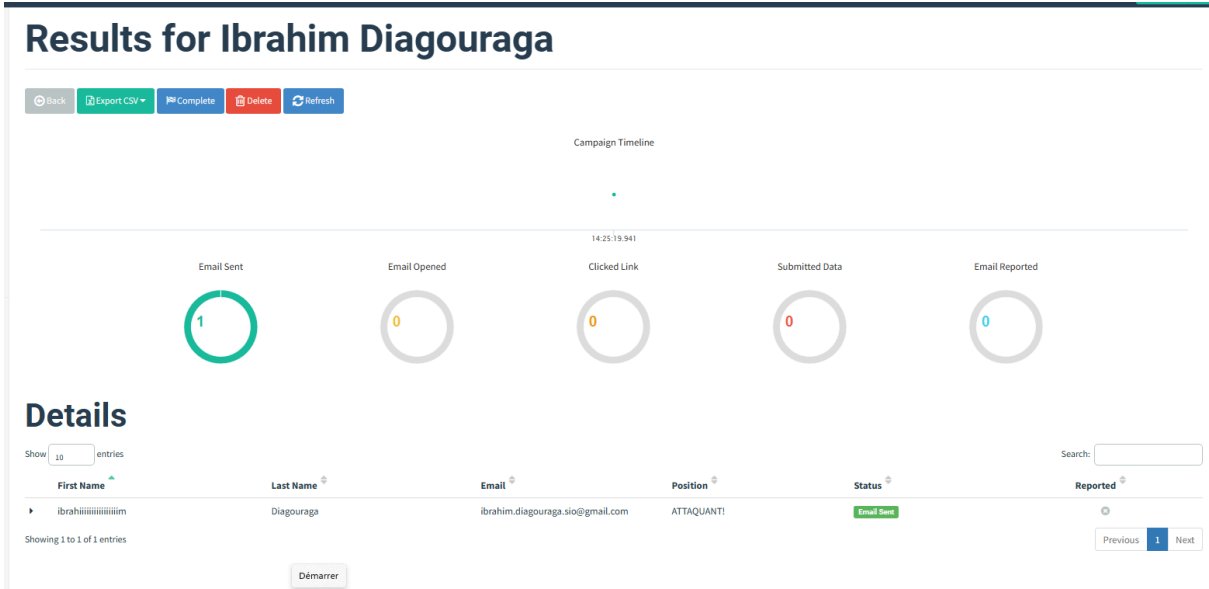
[\[Cliquez ici\]](#)

Ce processus est nécessaire pour garantir la sécurité de vos informations.

Merci pour votre compréhension.

L'équipe informatique de Cleanergy

Résultat du test.



Mission en stage

But : Le but de cet e-mail est d'obtenir l'adresse e-mail et le mot de passe actuel des enseignants.

Idée réaliste : Nous avons besoin des informations de connexion de tous les enseignants du lycée pour mettre à jour notre base de données et garantir une communication efficace.

En se faisant passer pour M.Kacimi (Professeur et Responsable informatique dans le lycée)

Adresse mail utilisé : kacimi.pc@gmail.com

(Véritable adresse : kacimi.p.c@gmail.com)

MAIL TYPE :

Objet : Recensement des adresses e-mail des professeurs

Cher enseignant(e),

Afin de mettre à jour notre base de données et d'assurer une communication efficace au sein de notre établissement, nous réalisons actuellement un recensement des adresses e-mail des professeurs du lycée Christophe Colomb.

Pour ce faire, veuillez cliquer sur le lien ci-dessous et saisir vos informations d'identification.

[Lien vers le faux site Web] (ma page d'authentification Gmail)

Votre coopération dans cette démarche est essentielle pour garantir la précision de nos informations et pour faciliter la communication au sein de notre communauté éducative.

Nous vous remercions par avance pour votre réponse rapide.

Cordialement,

Brahim Kacimi
Lycée Christophe Colomb

