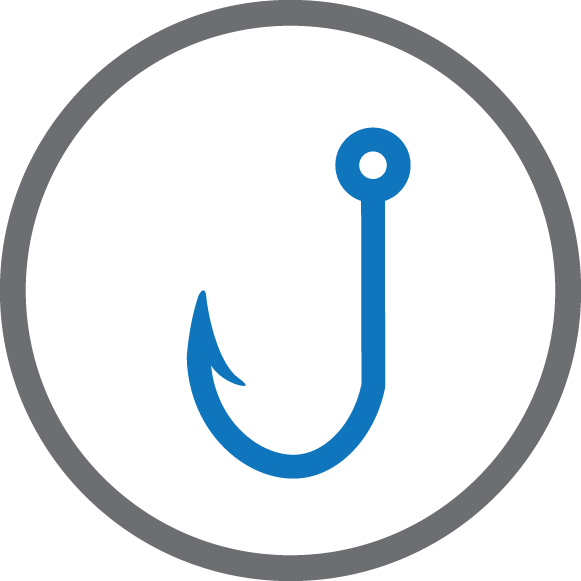
Práctica 1.5

Gophish - Phishing



ÍNDICE

[1.](#_heading=h.30j0zll) INTRODUCCIÓN 2

[2.](#_heading=h.1fob9te) DESARROLLO DE LA PRÁCTICA 2

[2.1](#_heading=h.3znysh7) PRÁCTICA CON PACKET TRACER 2

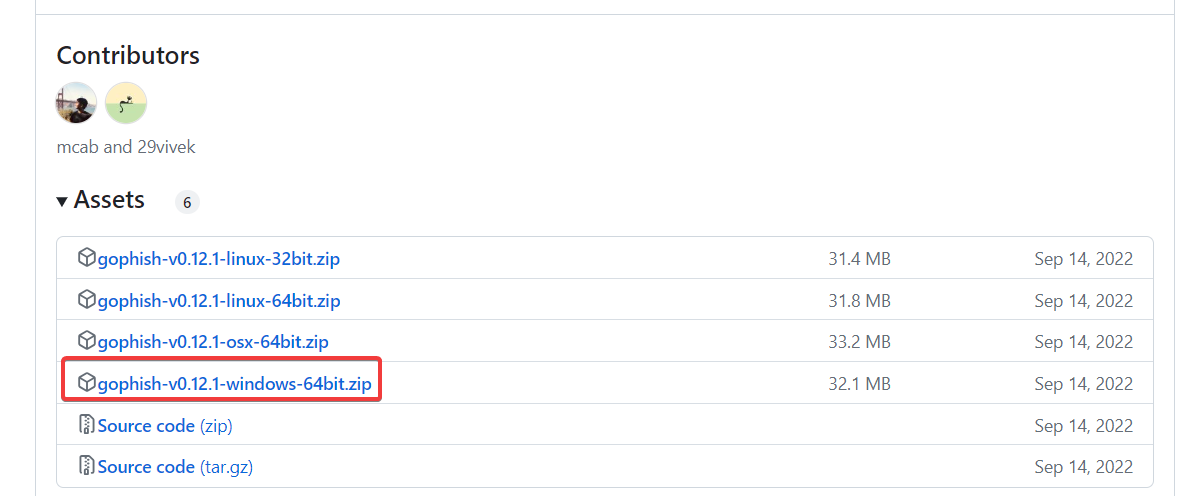
[2.2](#_heading=h.2et92p0) PRÁCTICA PACKET TRACER AVANZADA. 14

[2.3](#_heading=h.tyjcwt) PRÁCTICA CON MIKROTIK. 16

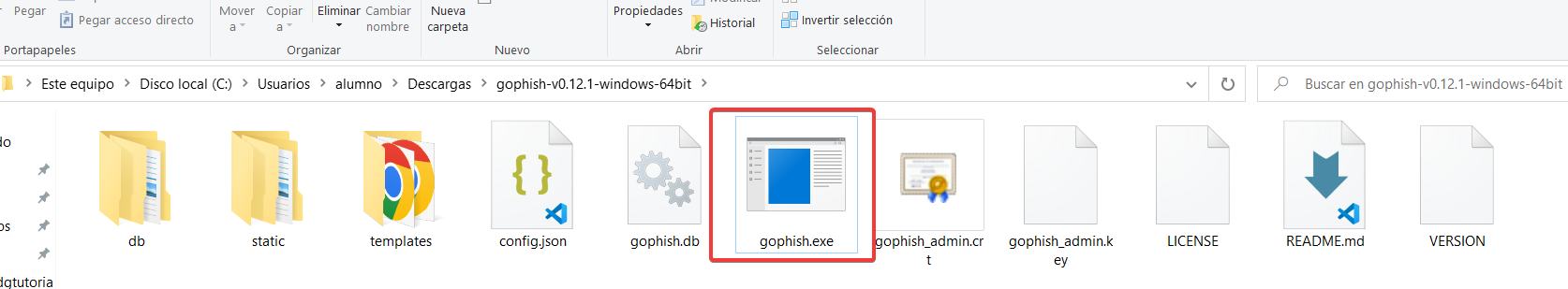
# INSTALACIÓN GOPHISH.

## Instalar la versión 12 de gophish y accede a él con usuario de admin y la clave que aparece en la consola al ejecutarlo por primera vez, luego podrás cambiar la contraseña a una propia.

Para descargar golphish nos iremos al siguiente enlace: <https://github.com/gophish/gophish/releases>, y en la versión 12 buscaremos el apartado Assets, y ahí estará el descargable. En mi caso voy a instalar en Windows.

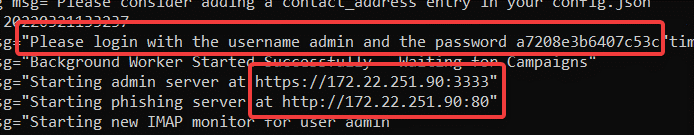


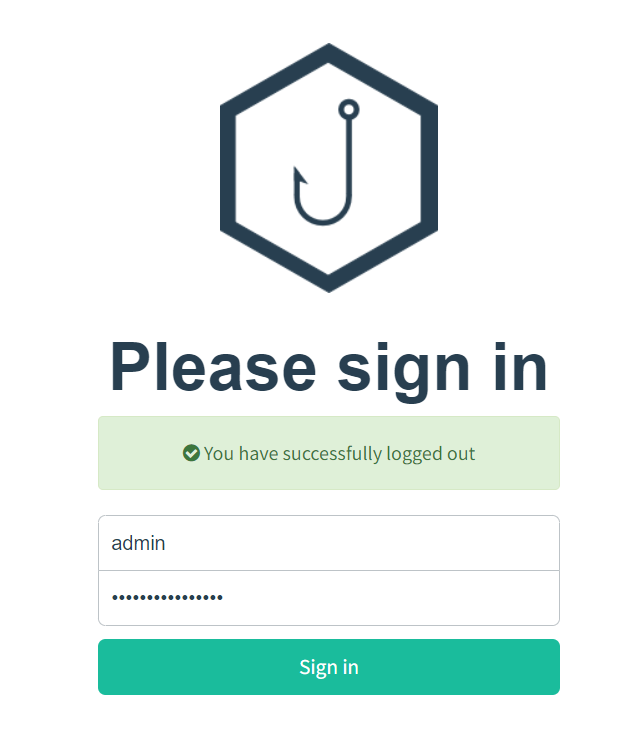
Descomprimiremos el archivo y abriremos la carpeta donde lo hemos extraído, haciendo después clic en golphish.exe.



Una vez abierto el ejecutable se nos abrirá la terminal y nos saldrá una ventana con información relevante tanto para poder iniciar sesión como para acceder a golphish.

Nos dará un usuario y una contraseña y nos dará la url para poder entrar.

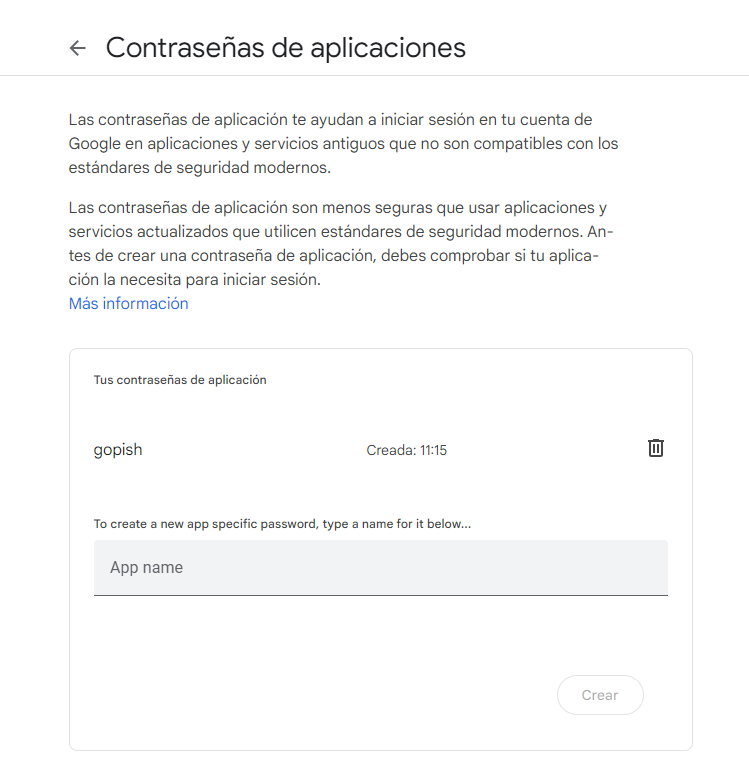


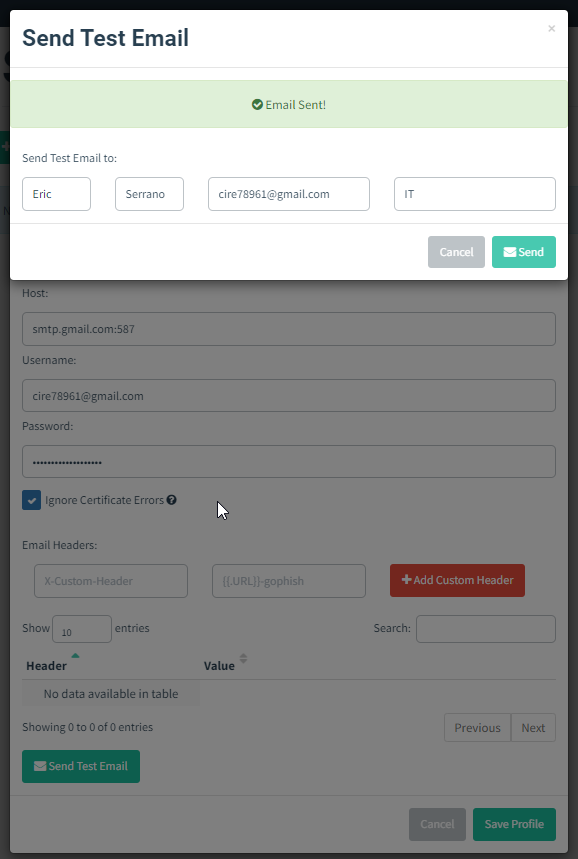


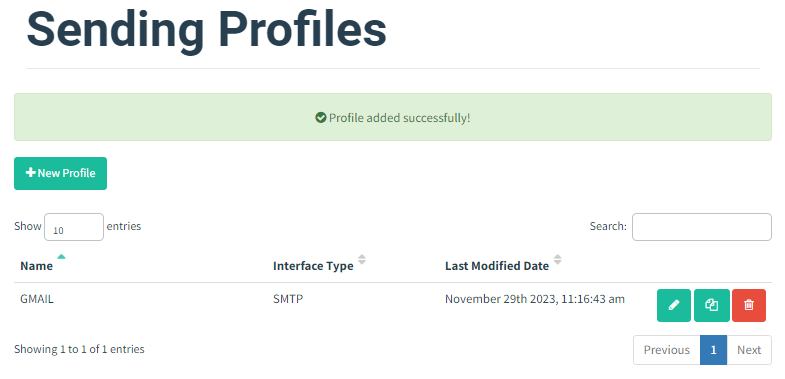
# CREAR UN PERFIL DE ENVÍO.

## Es posible que con las cuentas de gmail debáis activar el inicio de sesión en aplicaciones no seguras o activar la verificación en 2 pasos y crear una contraseña de aplicación específica para gophish. Otra opción es una cuenta con otro proveedor de emails que permita el acceso a aplicaciones poco seguras, pero ya casi todos lo controlan.

Primero vamos a crear una contraseña de aplicación para el campo password.

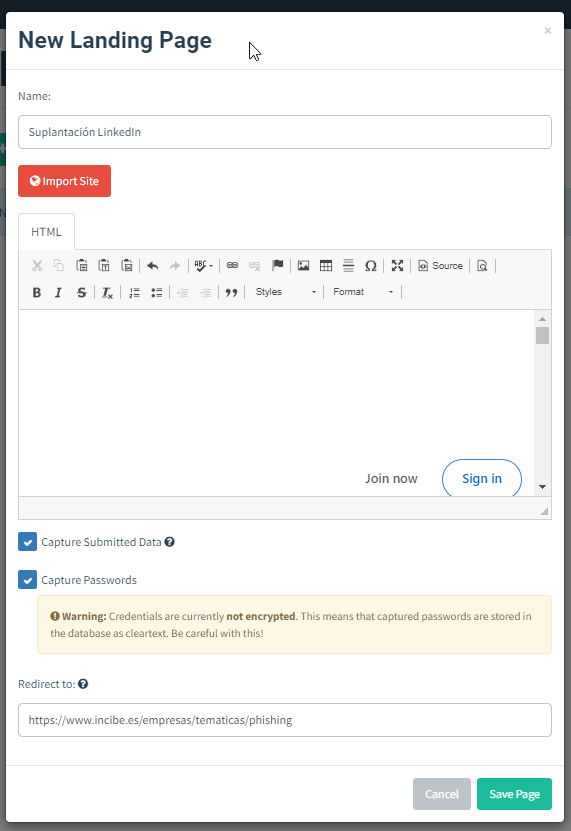






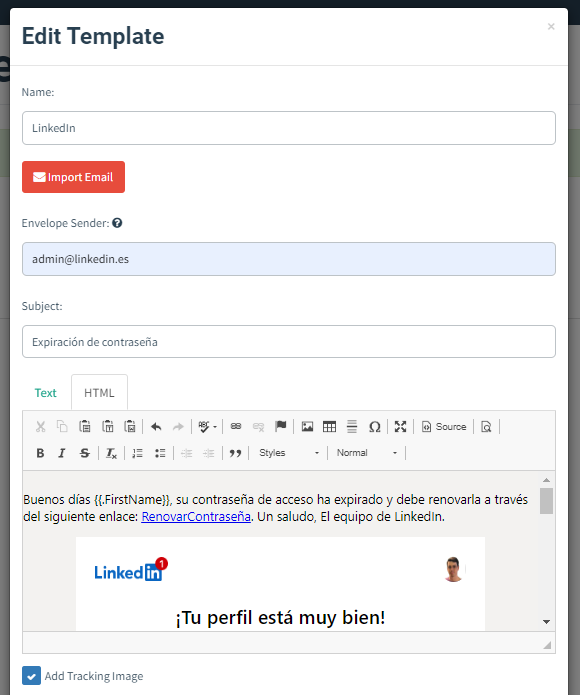
# LANDING PAGE

## Crea una landing page.



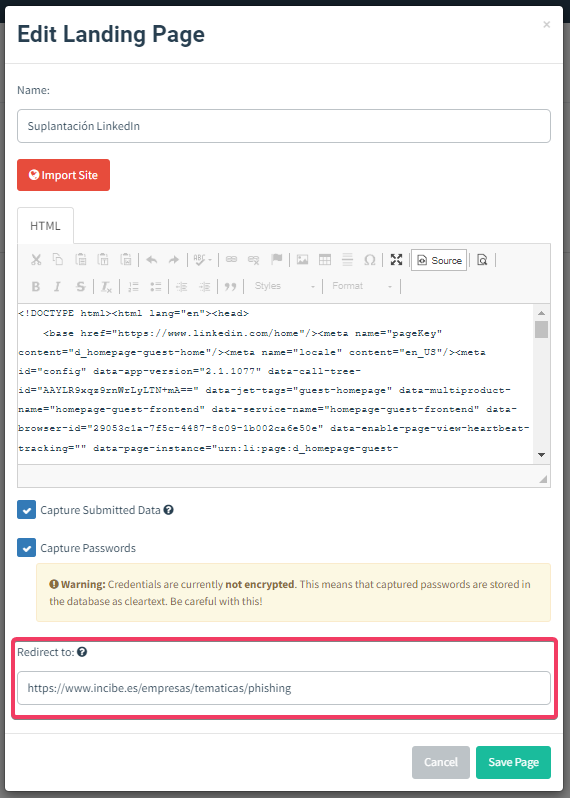
# CREAR UNA PLANTILLA DE CORREO.

## Recuerda meter en la plantilla algunos de los campos de personalización {{.FirstName}}{{.LastName}} {{.Position}} {{.Email}} {{.From}} para hacerlo más creíble y personalizado para cada receptor.



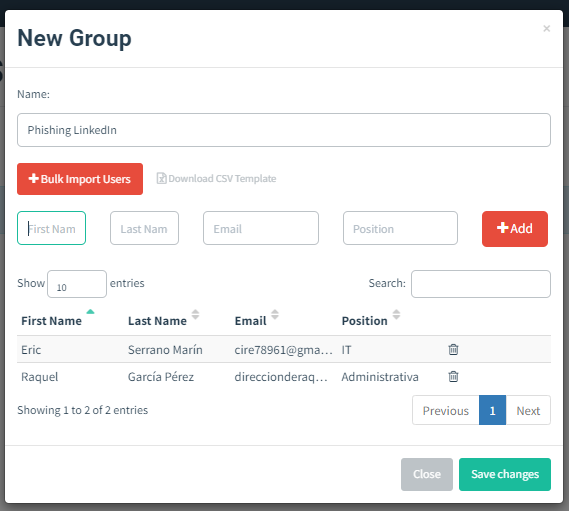
# URL DE DESTINO

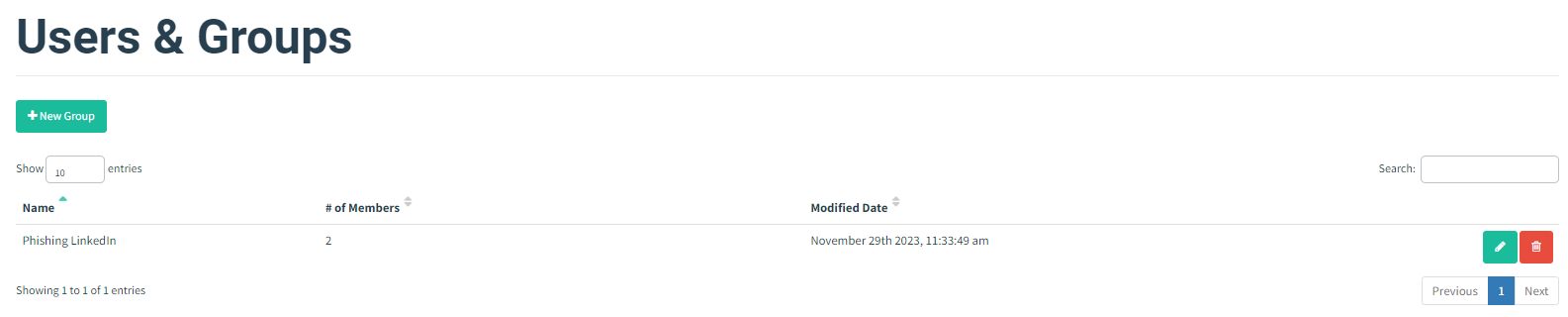
## Configura una URL de destino que sirva de aviso a formación al usuario sobre el phishing.



# CREAR UN GRUPO

## Crear un grupo de envío de correos. Alguno de los correos que sea uno al que tengas acceso para que veas cómo funciona la "trampa"





# Campaña Phishing.

## Lanza una campaña de Phishing.

