



# KIT DE CONCIENCIACIÓN

Manual de implementación  
de la herramienta Gophish

# ÍNDICE

<b>1. Qué es Gophish</b>	pág. 05
<b>2. Instalación y acceso a Gophish</b>	pág. 06
2.1. Descarga Gophish	pág. 06
2.2. Instalación de Gophish	pág. 07
2.2.1. Instalación en Linux	pág. 07
2.2.2. Instalación en Windows	pág. 09
2.3. Acceso a Gophish	pág. 11
2.4. Cambiar credenciales de acceso	pág. 13
2.5. Registrar nuevos usuarios administradores	pág. 14
<b>3. Campañas de envío de correos</b>	pág. 16
3.1. Perfil de envío	pág. 17
3.2. Página de aterrizaje	pág. 19
3.3. Plantilla de correo	pág. 23
3.4. Grupo de envío de correos	pág. 28
<b>4. Lanzamiento de la campaña de phishing</b>	pág. 29
<b>5. Visualización de la campaña</b>	pág. 33
<b>6. Anexo</b>	pág. 35
6.1. Campaña de phishing: el fraude del CEO	pág. 35
6.1.1. Página de aterrizaje	pág. 35
6.1.2. Plantilla de correo	pág. 37
6.1.3. Lanzamiento de la campaña Fraude del CEO	pág. 40
6.2. Cómo obtener el código fuente de correo electrónico en los distintos gestores de correo	pág. 41

## ÍNDICE DE ILUSTRACIONES

<b>1 - Descargas Gophish</b>	pág. 06
<b>2 - Descarga Gophish</b>	pág. 07
<b>3 - Crear carpeta Gophish</b>	pág. 08
<b>4 - Descomprimir Gophish</b>	pág. 08
<b>5 - Ejecutar Gophish</b>	pág. 08
<b>6 - Resultado de la ejecución</b>	pág. 09
<b>7 - Descomprimir .zip</b>	pág. 09
<b>8 - Ejecutando Gophish en Windows</b>	pág. 10
<b>9 - Archivo config.json</b>	pág. 11
<b>10 - Archivo config.json editado</b>	pág. 12
<b>11 - Cambio de contraseña para el usuario admin</b>	pág. 13
<b>12 - Registro de nuevos usuarios</b>	pág. 14
<b>13 - Nuevo usuario, elección de Role</b>	pág. 15
<b>14 - Nuevo perfil de envío</b>	pág. 17
<b>15 - Perfil de envío</b>	pág. 18
<b>16 - Nueva página de aterrizaje</b>	pág. 19
<b>17 - Importar la página de aterrizaje</b>	pág. 20
<b>18 - Importar la página de LinkedIn</b>	pág. 20
<b>19 - Guardar página de aterrizaje</b>	pág. 21
<b>20 - Capturar datos</b>	pág. 22
<b>21 - Redirección</b>	pág. 22
<b>22 - Nueva plantilla</b>	pág. 23
<b>23 - Correo legítimo de LinkedIn</b>	pág. 24
<b>24 - Importar correo</b>	pág. 25
<b>25 - Diseño de correo</b>	pág. 26
<b>26 - Añadir URL de phishing</b>	pág. 27
<b>27 - Grupo de envío de correos</b>	pág. 28
<b>28 - Nueva campaña</b>	pág. 29
<b>29 - Página de phishing</b>	pág. 30
<b>30 - Edición del archivo hosts</b>	pág. 31

## ÍNDICE DE ILUSTRACIONES

<b>31 - URL del phishing</b>	pág. 32
<b>32 - Resultados de las campañas</b>	pág. 33
<b>33 - Resultados de la campaña phishing LinkedIn</b>	pág. 33
<b>34 - Detalle por usuario</b>	pág. 34
<b>35 - Nueva página de aterrizaje</b>	pág. 35
<b>36 - Página de aterrizaje - concienciación INCIBE</b>	pág. 36
<b>37 - Nueva plantilla - Fraude de CEO</b>	pág. 37
<b>38 - Importando código fuente</b>	pág. 39
<b>39 - Edición del texto del correo</b>	pág. 39
<b>40 - Nueva campaña</b>	pág. 40
<b>41 - Outlook pestaña Archivo</b>	pág. 41
<b>42 - Outlook Guardar como</b>	pág. 41
<b>43 - Hotmail guardar correo para phishing.html</b>	pág. 42
<b>44 - Thunderbird ver código fuente</b>	pág. 43
<b>45 - Copiar código fuente en Thunderbird</b>	pág. 43
<b>46 - Mail para Mac, Fuente sin formato</b>	pág. 44
<b>47 - Outlook acceso al menú</b>	pág. 45
<b>48 - Outlook Ver origen del mensaje</b>	pág. 45
<b>49 - Outlook Copiar</b>	pág. 46
<b>50 - Yahoo Ver mensaje sin formato</b>	pág. 46
<b>51 - Yahoo Copiar</b>	pág. 47

## ÍNDICE DE TABLAS

<b>1 - Variables</b>	pág. 27
----------------------	---------

# 1.

# QUÉ ES GOPHISH

Gophish es un entorno de trabajo que permite la simulación de ataques de **phishing** para poner a prueba los conocimientos en la identificación de correos maliciosos y suplantaciones, en este caso, de la comunidad universitaria.

Se trata de una herramienta que posee un entorno intuitivo y fácil de manejar que explicaremos a lo largo de este documento.

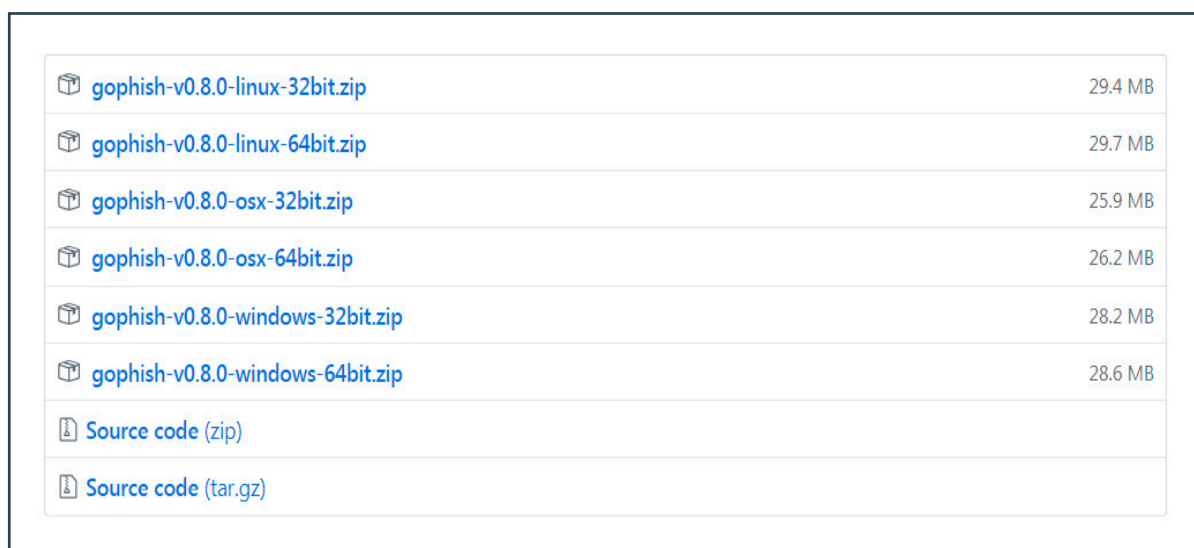
Si estás pensando en poner a prueba las habilidades de tus usuarios en materia de ciberseguridad, no lo pienses más, ¡comencemos a pescar!



A continuación se proponen una serie de instrucciones para instalar y configurar Gophish de manera correcta y generar tus propias campañas de phishing con el objetivo de entrenar a la comunidad universitaria para identificar este tipo de ciberamenazas. Los pasos indicados pueden modificarse en base a las necesidades del sistema operativo o cualquier otra que se pueda considerar por parte del personal de TI o el encargado de los sistemas de la organización.

## 2.1. Descarga de Gophish

Obtener Gophish es tan sencillo como dirigirse al repositorio de Github de la herramienta: <https://github.com/gophish/gophish/releases> y descargar el zip apropiado para tu sistema operativo Linux, Mac OS X o Windows. Puesto que se trata de una aplicación de código abierto, tanto su descarga como su uso son totalmente gratuitos.










 <a href="#">gophish-v0.8.0-linux-32bit.zip</a>	29.4 MB
 <a href="#">gophish-v0.8.0-linux-64bit.zip</a>	29.7 MB
 <a href="#">gophish-v0.8.0-osx-32bit.zip</a>	25.9 MB
 <a href="#">gophish-v0.8.0-osx-64bit.zip</a>	26.2 MB
 <a href="#">gophish-v0.8.0-windows-32bit.zip</a>	28.2 MB
 <a href="#">gophish-v0.8.0-windows-64bit.zip</a>	28.6 MB
 <a href="#">Source code (zip)</a>	
 <a href="#">Source code (tar.gz)</a>	

Ilustración 1. Descargas Gophish

## 2.

INSTALACIÓN Y  
ACCESO A GOPHISH

## 2.2. Descarga de Gophish

## 2.2.1. Instalación en Linux

Para instalar Gophish en Linux tendrás que llevar a cabo las siguientes acciones:

- 1- Acceder a la página oficial: <https://github.com/gophish/gophish/releases>
- 2- Descargar la versión de Gophish para Linux de 32 o de 64 bits dependiendo del sistema operativo donde vayamos a instalarlo. También podemos descargarlo desde la línea de comandos con la instrucción:
  - » `sudo wget https://github.com/gophish/gophish/releases/download/v0.8.0/gophish-v0.8.0-linux-64bit.zip`<sup>1</sup>

```

Archivo Editar Ver Buscar Terminal Ayuda
tecnicolocal@ ~$ sudo wget https://github.com/gophish/gophish/releases/download/v0.8.0/gophish-v0.8.0-linux-64bit.zip
[sudo] contraseña para tecnicolocal:
--2019-10-23 10:02:28-- https://github.com/gophish/gophish/releases/download/v0.8.0/gophish-v0.8.0-linux-64bit.zip
Resolviendo github.com (github.com)... 140.82.118.3
Conectando con github.com (github.com)[140.82.118.3]:443... conectado.
Petición HTTP enviada, esperando respuesta... 302 Found
Ubicación: https://github-production-release-asset-2e65be.s3.amazonaws.com/14508450/6fd87700-bc7a-11e9-8a5c-80e4793a0ad9?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIWNJYAX4CSVEH53A%2F20191023%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20191023T080229Z&X-Amz-Expires=300&X-Amz-Signature=f1a8787c76ee03cd80c7b2d341bfe7f17ce2589a1a53ff2225bf272a64b8b0c&X-Amz-SignedHeaders=host&actor_id=0&response-content-disposition=attachment%3B%20filename%3Dgophish-v0.8.0-linux-64bit.zip&response-content-type=application%2Foctet-stream [siguiente]
--2019-10-23 10:02:29-- https://github-production-release-asset-2e65be.s3.amazonaws.com/14508450/6fd87700-bc7a-11e9-8a5c-80e4793a0ad9?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIWNJYAX4CSVEH53A%2F20191023%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20191023T080229Z&X-Amz-Expires=300&X-Amz-Signature=f1a8787c76ee03cd80c7b2d341bfe7f17ce2589a1a53ff2225bf272a64b8b0c&X-Amz-SignedHeaders=host&actor_id=0&response-content-disposition=attachment%3B%20filename%3Dgophish-v0.8.0-linux-64bit.zip&response-content-type=application%2Foctet-stream
Resolviendo github-production-release-asset-2e65be.s3.amazonaws.com (github-production-release-asset-2e65be.s3.amazonaws.com)... 54.231.82.186
Conectando con github-production-release-asset-2e65be.s3.amazonaws.com (github-production-release-asset-2e65be.s3.amazonaws.com)[54.231.82.186]:443... conectado.
Petición HTTP enviada, esperando respuesta... 200 OK
Longitud: 31158764 (30M) [application/octet-stream]
Guardando como: "gophish-v0.8.0-linux-64bit.zip"

gophish-v0.8.0-linu 100%[=====] 29,71M 14,0MB/s en 2,1s
2019-10-23 10:02:31 (14,0 MB/s) - "gophish-v0.8.0-linux-64bit.zip" guardado [31158764/31158764]

```

Ilustración 2. Descarga Gophish

<sup>1</sup> Ten en cuenta que esta era la versión más actualizada cuando se creó el manual. Recuerda descargar la última versión disponible.

## 2.

## INSTALACIÓN Y ACCESO A GOPHISH

3- Crear una carpeta Gophish en el directorio opt.

» `sudo mkdir /opt/gophish`

```
tecnicolocal@ :/$ sudo mkdir /opt/gophish
tecnicolocal@ :/$
```

**Ilustración 3. Crear carpeta Gophish**

4- Descomprimir en la carpeta creada en el paso anterior.

» `sudo unzip gophish-v0.8.0-linux-64bit.zip -d /opt/gopshish`

```
tecnicolocal@ :~$ sudo unzip gophish-v0.8.0-linux-64bit.zip -d /opt/gopshish/
```

**Ilustración 4. Descomprimir Gophish**

5- Acceder a la carpeta donde hemos descomprimido Gophish.

» `cd /opt/gophish`

6- Ejecutar Gopshish con permisos de administrador.

» `sudo ./gophish`

```
tecnicolocal@ :~/Descargas$ cd /opt/gophish/
tecnicolocal@ :/opt/gophish$ sudo ./gophish
```

**Ilustración 5. Ejecutar Gophish**



## 2.

INSTALACIÓN Y  
ACCESO A GOPHISH

7- La terminal mostrará el siguiente resultado:

```
tecnico@tecnicolocal:~/opt/gophish$ sudo ./gophish
time="2019-05-03T11:44:12+02:00" level=info msg="Background Worker Started Successfully - Waiting for Campaigns"
time="2019-05-03T11:44:12+02:00" level=warning msg="No contact address has been configured."
time="2019-05-03T11:44:12+02:00" level=warning msg="Please consider adding a contact_address entry in your config.json"
goose: no migrations to run. current version: 20180830215615
time="2019-05-03T11:44:12+02:00" level=info msg="Creating new self-signed certificates for administration interface"
time="2019-05-03T11:44:12+02:00" level=info msg="Starting phishing server at http://0.0.0.0:80"
time="2019-05-03T11:44:12+02:00" level=info msg="TLS Certificate Generation Complete"
time="2019-05-03T11:44:12+02:00" level=info msg="Starting admin server at https://127.0.0.1:3333"
```

Ilustración 6. Resultado de la ejecución

Para tener acceso a Gophish, debemos copiar en nuestro navegador la dirección resaltada en la imagen anterior. Así mismo, esta será la dirección IP que tiene asignada el adaptador de red para acceder a este servicio.

## 2.2.2. Instalación en Linux

Para instalar Gophish en Windows tendrás que llevar a cabo las siguientes acciones:

- ▶ Acceder a la página oficial: <https://github.com/gophish/gophish/releases>
- ▶ Descargar la versión de Gophish para Windows de 32 o de 64 bits dependiendo del sistema operativo que tengamos instalado, haciendo clic en el enlace.
- ▶ Acceder a la carpeta donde hayamos guardado el archivo .zip y descomprimirlo en la ubicación que deseemos. Visualizaremos los archivos que se muestran en la siguiente imagen:

Nombre	Fecha de modifica...	Tipo	Tamaño
db	06/09/2018 12:37	Carpeta de archivos	
static	06/09/2018 12:37	Carpeta de archivos	
templates	06/09/2018 12:37	Carpeta de archivos	
config.json	05/09/2018 1:35	Archivo JSON	1 KB
gophish.exe	05/09/2018 1:40	Aplicación	14.505 KB
LICENSE	05/09/2018 1:35	Archivo	2 KB
README.md	05/09/2018 1:35	Archivo MD	4 KB
VERSION	05/09/2018 1:35	Archivo	1 KB

Ilustración 7. Descomprimir .zip

## 2.

INSTALACIÓN Y  
ACCESO A GOPHISH

- ▶ Por último, hacer doble clic en el ejecutable **gophish.exe** y el proceso habrá terminado, obteniendo la siguiente ventana:

```

C:\Users\... \Downloads\gophish-v0.7.0-windows-32bit\gophish.exe
OK 20160227180335_0.1.2_store-smtp-settings.sql
OK 20160317214457_0.2_redirect_url.sql
OK 20160605210903_0.2_campaign_scheduling.sql
OK 20170104220731_0.2_result_statuses.sql
OK 20170219122503_0.2.1_email_headers.sql
OK 20170827141312_0.4_utc_dates.sql
OK 20171027213457_0.4.1_maillogs.sql
OK 20171208201932_0.4.1_next_send_date.sql
OK 20180223101813_0.5.1_user_reporting.sql
OK 20180524203752_0.7.0_result_last_modified.sql
OK 20180527213648_0.7.0_store_email_request.sql
OK 20180830215615_0.7.0_send_by_date.sql
time="2018-09-06T12:44:32+02:00" level=info msg="Starting phishing server at http://0.0.0.0:80"
time="2018-09-06T12:44:32+02:00" level=info msg="Creating new self-signed certificates for administration interface"
time="2018-09-06T12:44:32+02:00" level=info msg="TLS Certificate Generation complete"
time="2018-09-06T12:44:32+02:00" level=info msg="Starting admin server at https://127.0.0.1:3333"
time="2018-09-06T12:45:55+02:00" level=info msg="127.0.0.1 - - [06/Sep/2018:12:45:55 +0200] \"GET / HTTP/2.0\" 302 38 \"\" \"Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/69.0.3497.81 Safari/537.36\"

```

Ilustración 8. Ejecutando Gophish en Windows



Existen tres opciones a la hora de instalar Gophish:

- ▶ Instalar Gophish de manera local. Es la opción que explicamos a lo largo de este manual e implica que los usuarios que reciban el phishing deben abrir el correo cuando estén conectados a la red de área local. De lo contrario la Landing Page que crearemos no será accesible. Consulta el punto 3.2 para más información.
- ▶ Instalar Gophish en un servidor web que pertenezca a la empresa. Deberás contar con personal cualificado que pueda llevar a cabo las tareas de instalación así como la implementación de las medidas de seguridad necesarias.
- ▶ Instalar Gophish en un servidor en la **nube**. Recordare revisar las condiciones de contratación que ofrece cada proveedor, poniendo especial atención en las relativas a ciberseguridad.

## 2.

## INSTALACIÓN Y ACCESO A GOPHISH

### 2.3. Acceso a Gophish

Para acceder a la interfaz web que nos proporciona Gophish, seguiremos estos pasos:

Abrir el navegador y acceder a la URL: <https://127.0.0.1:3333> (para Linux y Windows). Gophish utiliza un certificado autofirmado que debemos aceptar en los navegadores para poder acceder a la herramienta.

- ▶ Introducir las credenciales por defecto de inicio de sesión:
  - » Usuario: admin
  - » Contraseña: gophish

Opcionalmente puedes cambiar estas direcciones por la del servidor que estés utilizando, editando el archivo **config.json** que encontraremos dentro de la carpeta Gophish que hemos descargado y en el que podemos ver la siguiente configuración:



```
config.json
/opt/gophish
Guardar

{
  "admin_server": {
    "listen_url": "127.0.0.1:3333",
    "use_tls": true,
    "cert_path": "gophish_admin.crt",
    "key_path": "gophish_admin.key"
  },
  "phish_server": {
    "listen_url": "127.0.0.1:80",
    "use_tls": false,
    "cert_path": "example.crt",
    "key_path": "example.key"
  },
  "db_name": "sqlite3",
  "db_path": "gophish.db",
  "migrations_prefix": "db/db_",
  "contact_address": ""
}
```

Ilustración 9. Archivo config.json

## 2.

## INSTALACIÓN Y ACCESO A GOPHISH

Sustituimos la dirección 127.0.0.1 por la IP local del servidor que contendrá GoPhish y guardamos los cambios. Recuerda abrir el documento con permisos de administrador.



```
{
  "admin_server": {
    "listen_url": "192.168.13.252:3333",
    "use_tls": true,
    "cert_path": "gophish_admin.crt",
    "key_path": "gophish_admin.key"
  },
  "phish_server": {
    "listen_url": "192.168.13.252:80",
    "use_tls": false,
    "cert_path": "example.crt",
    "key_path": "example.key"
  },
  "db_name": "sqlite3",
  "db_path": "gophish.db",
  "migrations_prefix": "db/db_",
  "contact_address": ""
}
```

Ilustración 10. Archivo config.json editado

A partir de entonces accederemos a Gophish de la siguiente manera: <https://MiDirecciónIp:3333>

## 2.

## INSTALACIÓN Y ACCESO A GOPHISH

### 2.4. Cambiar credenciales de acceso

Para cambiar la contraseña por defecto del usuario **admin**, accedemos a la entrada **Account Settings** del menú principal. Introduce la contraseña **gophish** en el campo **Old Password** y la nueva clave en el campo **New Password**. Para guardar los cambios, hacemos clic en **Save**.

The screenshot shows the Gophish web interface. On the left is a navigation menu with options: Dashboard, Campaigns, Users & Groups, Email Templates, Landing Pages, Sending Profiles, Account Settings (highlighted), User Management (with an 'Admin' badge), User Guide, and API Documentation. The main content area is titled 'Settings' and has two tabs: 'Account Settings' (selected) and 'UI Settings'. Under 'Account Settings', the 'Gophish version' is 0.7.1. The 'API Key' is displayed as a long alphanumeric string with a 'Reset' button. Below this are four input fields: 'Username' (containing 'admin'), 'Old Password' (containing '\*\*\*\*\*'), 'New Password' (empty), and 'Confirm New Password' (empty). A 'Save' button is located at the bottom of the form. Red circles are drawn around the 'Username', 'Old Password', 'New Password', and 'Save' elements.

Ilustración 11. Cambio de contraseña para el usuario admin

## 2.

## INSTALACIÓN Y ACCESO A GOPHISH

### 2.5. Registrar nuevos usuarios administradores

Para registrar nuevos usuarios que puedan administrar Gophish, accedemos a la entrada **User Management** y hacemos clic en el botón **New User**.

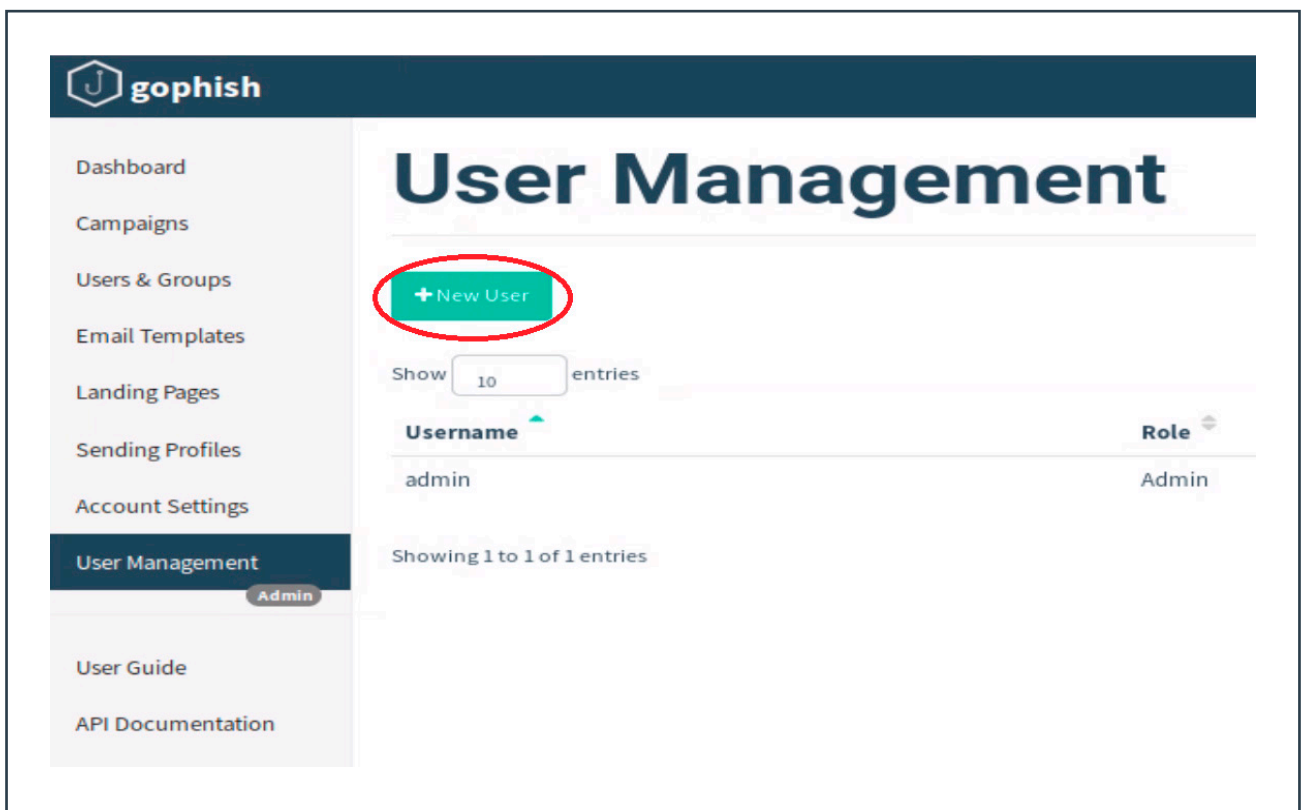
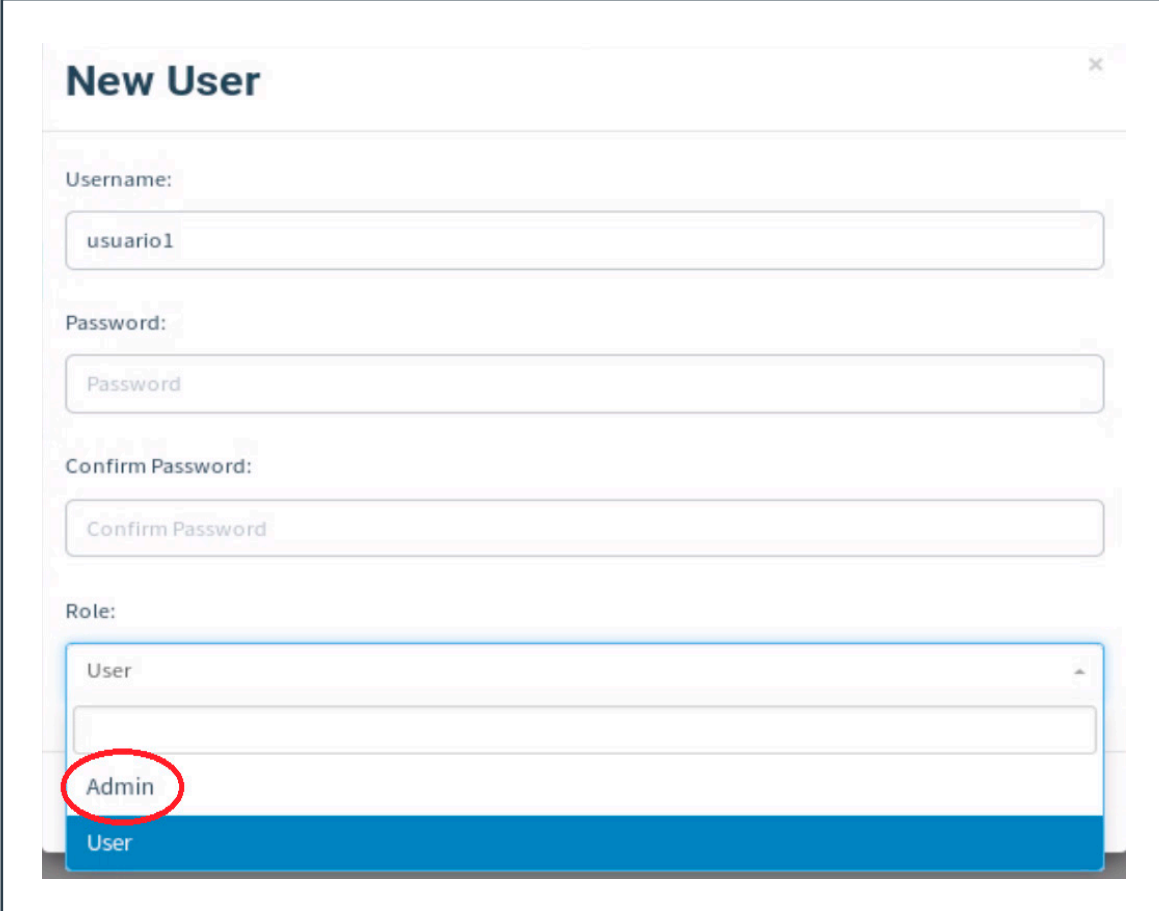


Ilustración 12. Registro de nuevos usuarios

## 2.

## INSTALACIÓN Y ACCESO A GOPHISH

Si queremos que el nuevo usuario tenga permisos de administración elegimos la opción **Admin** del menú desplegable **Role**:



The image shows a 'New User' form with the following fields and options:

- Username:** usuario1
- Password:** Password
- Confirm Password:** Confirm Password
- Role:** A dropdown menu is open, showing 'Admin' (circled in red) and 'User' as options.

Ilustración 13. Nuevo usuario, elección de Role

# 3.

## CAMPAÑAS DE ENVÍO DE CORREOS

Puesto que el objetivo de implementar este sistema será entrenar a nuestros usuarios, hemos de elegir una dirección de correo remitente con la que estén familiarizados o de lo contrario será más complicado que caigan en el engaño.

Entre las alternativas disponibles para llevar a cabo el ataque, podríamos decantarnos por un correo de cambio de contraseña en Gmail/Hotmail/PayPal/Facebook, una solicitud de amistad o consulta de perfil en LinkedIn, acceso a un servicio de la universidad, etc.

También podríamos enviar otro tipo de correos fraudulentos, como **el envío de falsas facturas, el fraude del CEO o el falso soporte técnico.**

En los siguientes puntos se detallan todos los pasos necesarios para la creación y envío de la campaña de phishing.





# 3.

## CAMPAÑAS DE ENVÍO DE CORREOS

### 3.1. Perfil de envío

El primer paso es definir la cuenta desde la que se enviarán los correos maliciosos (perfil de envío). Para ello accedemos a la opción **Sending Profiles** del menú y a continuación hacemos clic en **New Profile**.

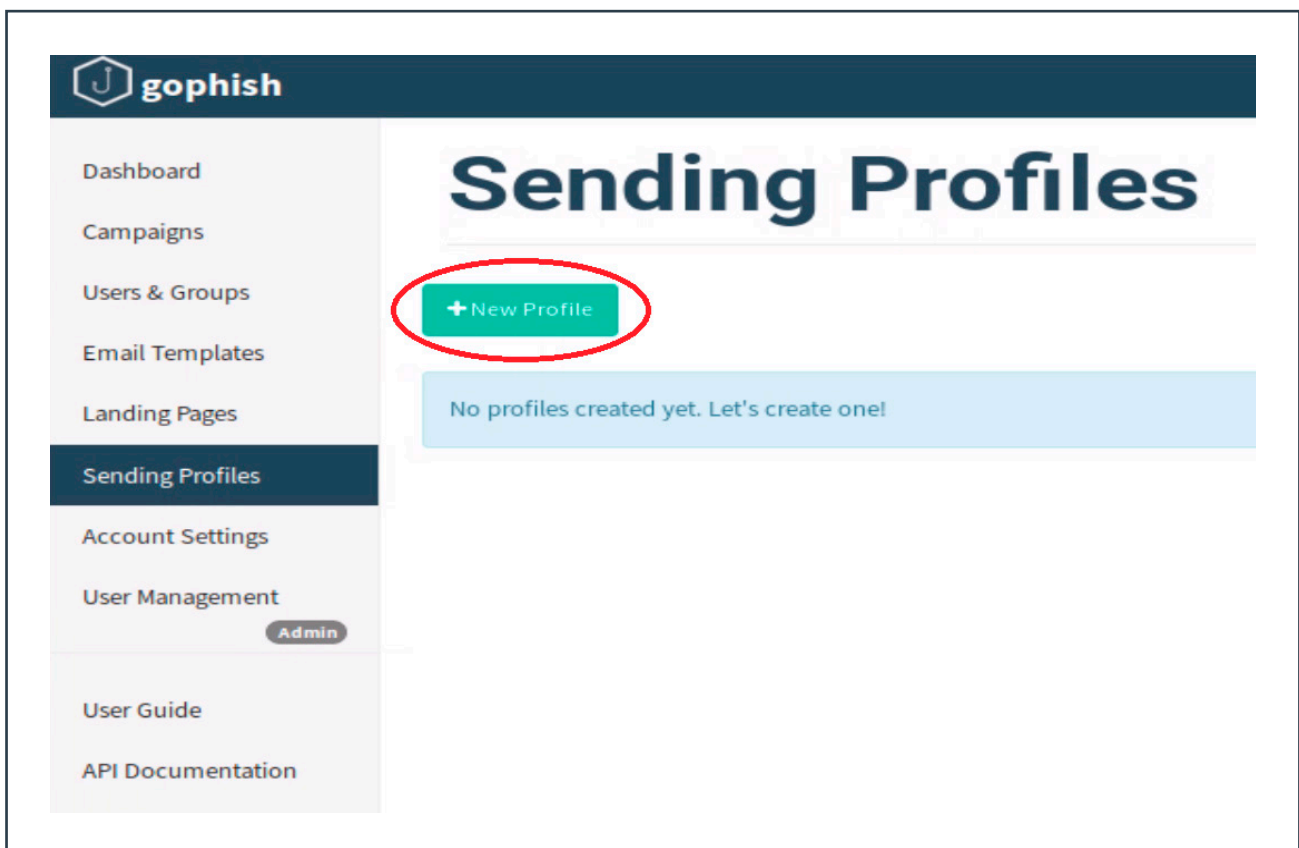


Ilustración 14. Nuevo perfil de envío

Aparecerá una ventana como la que se muestra a continuación en la que completaremos los campos. En este caso hemos elegido una cuenta de correo de Gmail **micuenta@gmail.com** (campo **Username**) y la contraseña (campo **Password**) debe ser con la que accedemos a esa cuenta en dicho proveedor de correo (en este caso Gmail). También podemos usar un servidor de correo propio. Para rellenar el campo Host, tendremos que incluir la información correspondiente de cada proveedor de correo o de nuestro servicio de correo. En el caso de Gmail, podemos dirigirnos a <https://support.google.com/a/answer/176600?hl=es>.

En el campo **From** debemos introducir una cuenta ficticia que esté relacionada con el correo que vamos a enviar ya que será la dirección de remitente que verá el receptor del email de phishing.

# 3.

## CAMPAÑAS DE ENVÍO DE CORREOS

**New Sending Profile**

Name: GMAIL

Interface Type: SMTP

From: micuenta@gmail.com

Host: smtp.gmail.com:587

Username: micuenta@gmail.com

Password: .....

Ignore Certificate Errors ⓘ

Email Headers:

Header	Value
X-Custom-Header	{{.URL}}-gophish

+ Add Custom Header

Show 10 entries Search: [ ]

Showing 0 to 0 of 0 entries Previous Next

Send Test Email

Cancel Save Profile

Ilustración 15. Perfil de envío

Podemos enviar un correo de prueba para comprobar que la configuración introducida funciona correctamente en **Send Test Email**. Si el correo de prueba se envía satisfactoriamente, guardamos el perfil creado.

\* En el caso particular de Gmail, debemos acceder a la configuración de seguridad de la cuenta <https://myaccount.google.com/security> y poner en "SÍ" la opción "Permitir el acceso de aplicaciones poco seguras" para que Gophish pueda utilizar esa cuenta para enviar los correos.

Si utilizas un servidor de correo propio, comprueba que las opciones de seguridad son compatibles con el envío de correos a través de Gophish.

# 3.

## CAMPAÑAS DE ENVÍO DE CORREOS

### 3.2. Página de aterrizaje

El siguiente paso será crear una **landing page** (página de aterrizaje) que será una copia de la web legítima con la que queremos "engañar" a los usuarios. Lo más recomendable es elegir una web con la que la comunidad universitaria esté familiarizada y que el mensaje del correo inste a realizar una acción común: inicio de sesión, cambio de contraseña, etc. Es probable que, si por ejemplo incitamos a la compra de algún producto o a la visualización de algún contenido, muchos usuarios no accedan al enlace al tratarse de un equipo institucional.

En este manual hemos optado por la opción de reproducir el correo que nos envía LinkedIn cuando nuestro perfil tiene una nueva visualización. Al hacer clic en el enlace del correo se abrirá la página de inicio de sesión en LinkedIn: es.linkedin.com

Para copiar la página de aterrizaje en el menú principal accedemos a **Landing Page** y hacemos clic en **New Page**.

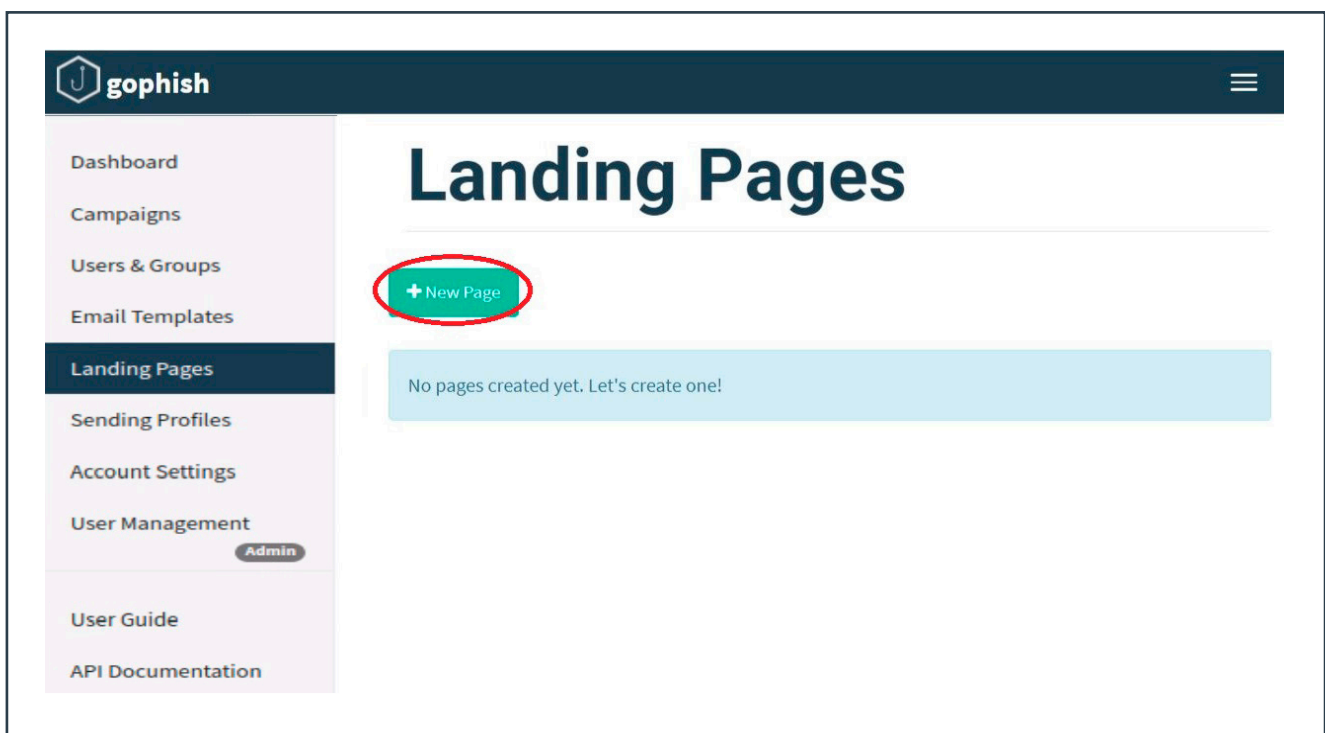


Ilustración 16. Nueva página de aterrizaje

# 3.

## CAMPAÑAS DE ENVÍO DE CORREOS

Al acceder a **New Page** se mostrarán los campos que vemos en la imagen. Lo más sencillo es acceder a la opción **Import Site** y teclear la URL de la web que queremos suplantar. Así se creará una copia que usaremos para los emails de phishing.

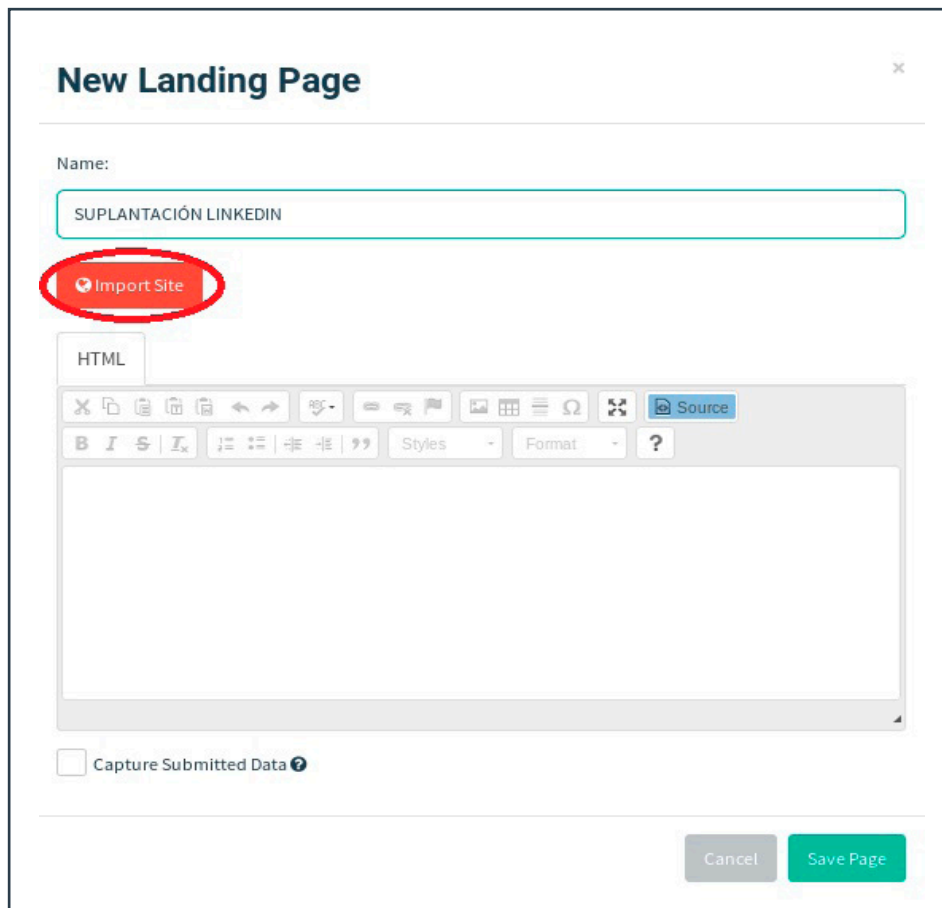


Ilustración 17. Importar página de aterrizaje



Ilustración 18. Importar la página de LinkedIn

# 3.

## CAMPAÑAS DE ENVÍO DE CORREOS

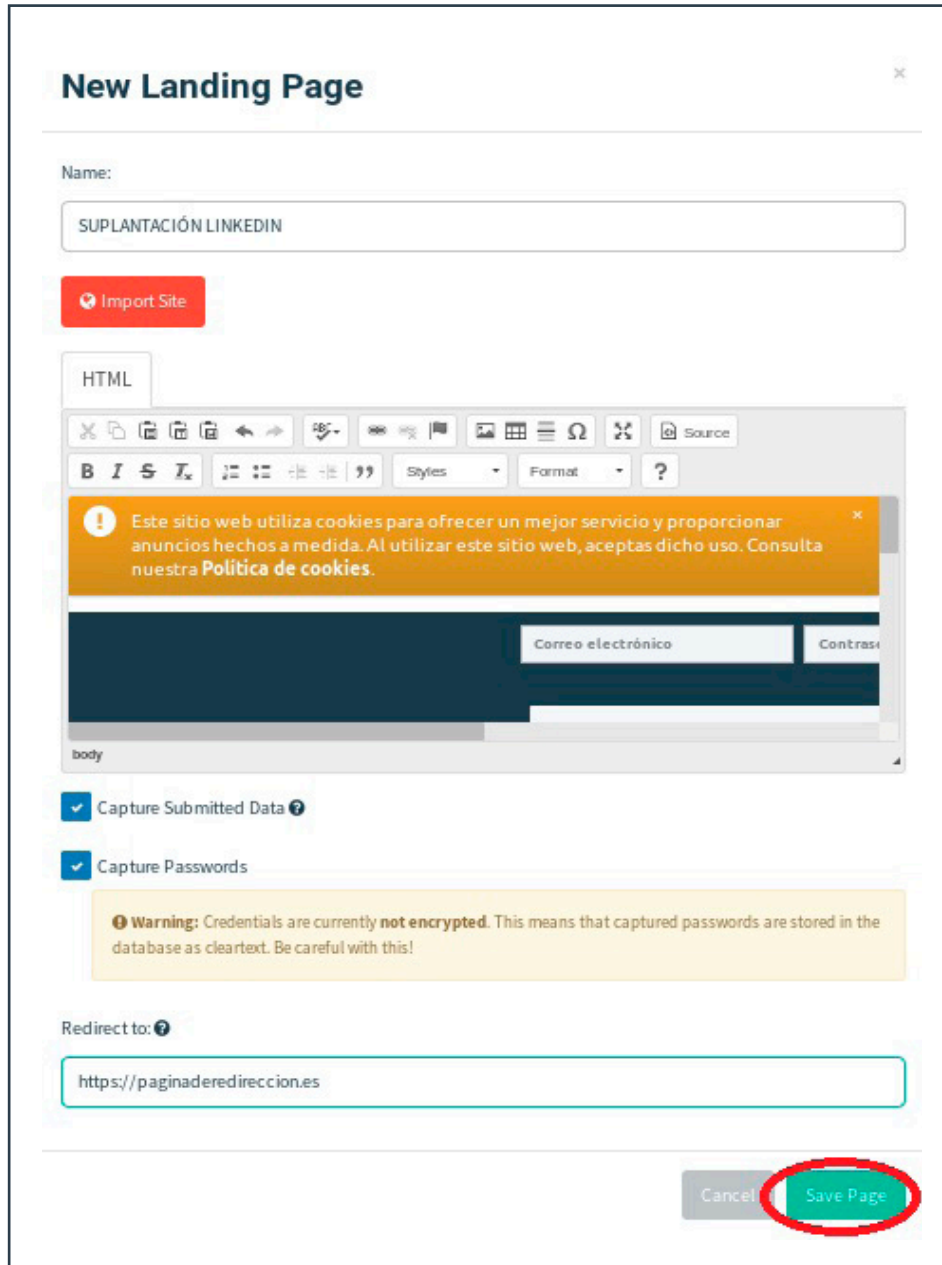


Ilustración 19. Guardar página de aterrizaje

# 3.

## CAMPAÑAS DE ENVÍO DE CORREOS

Para capturar los datos de los usuarios que "pican" en el correo hay que activar la casilla de **Capture Submit Data**.

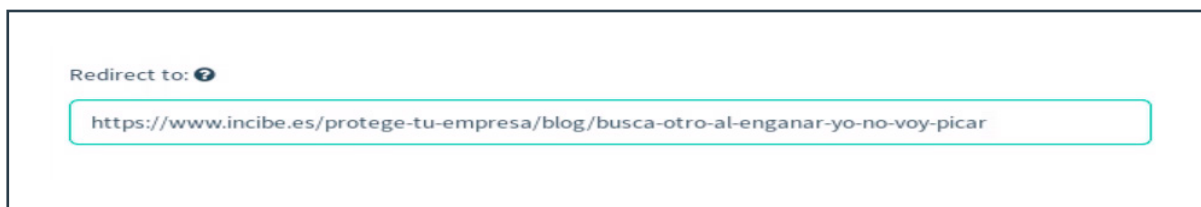


**Ilustración 20. Capturar datos**

También está disponible la opción de capturar las contraseñas de los usuarios (Capture Passwords) que intenten iniciar sesión en la página que hemos clonado y que podremos comprobar en los informes una vez haya sido lanzada la campaña 5.

Aconsejamos no habilitar la opción Capture Passwords si no se ha diseñado un phishing de un servicio institucional, ya que se estaría almacenando la contraseña utilizada por el usuario en un servicio personal y de ámbito privado ajeno a la universidad. Además, como muestra el texto de alerta (**Warning**), si activamos la opción **Capture Passwords** guardaremos en la base de datos de Gophish la contraseña **no cifrada** de la cuenta del usuario en ese servicio por lo que tenemos que ser conscientes de los riesgos de seguridad que esta acción implica.

El campo **Redirect to** nos proporciona la opción de introducir una URL a la que el usuario es dirigido una vez haya introducido y validado sus credenciales. Esta URL puede ser cualquiera que se nos ocurra, incluso una creada por nosotros mismos con algún mensaje para nuestros usuarios o **recomendaciones de ciberseguridad** para no volver a caer en un phishing.



**Ilustración 21. Redirección**

Ya solo queda guardar la configuración de la **Landing Page** o página de aterrizaje en la opción **Save Page**.

# 3.

## CAMPAÑAS DE ENVÍO DE CORREOS

### 3.3. Plantilla de correo

Hemos llegado al punto de configurar el correo que enviaremos a nuestros usuarios. A través de la opción **Email Templates > New Template**, Gophish nos proporciona dos opciones para configurar el modelo de correo electrónico:

- ▶ 1. Podemos importar cualquier correo que hayamos recibido, capturando su código fuente y la opción **Import Email**.
- ▶ 2. Diseñar el correo que queremos enviar añadiendo texto plano (pestaña **Text**) o código HTML (pestaña **HTML**).

Para diseñar la plantilla de correo que enviaremos a nuestros usuarios en este ejemplo, accedemos a la opción **Email Templates** del menú principal y se mostrará una pantalla como la siguiente:

The screenshot shows the 'New Template' interface. At the top, the title 'New Template' is displayed. Below it, the 'Name' field contains 'INVITACIÓN LINKEDIN'. A red button labeled 'Import Email' is highlighted with a red circle. The 'Subject' field is empty. Below the subject field, there are two tabs: 'Text' and 'HTML'. The 'HTML' tab is selected. Below the tabs is a rich text editor with a toolbar. Below the editor, there is a checkbox 'Add Tracking Image' which is checked. There is a red button '+ Add Files'. Below that, there is a 'Show' dropdown set to '10' and a 'Search' field. Below the search field, there is a table header 'Name' and a message 'No data available in table'. At the bottom right, there are 'Cancel' and 'Save Template' buttons, with 'Save Template' circled in red.

Ilustración 22. Nueva plantilla

### 3.

## CAMPAÑAS DE ENVÍO DE CORREOS

Asignamos el nombre "Invitación LinkedIn" o cualquier otro que nos resulte descriptivo. El campo asunto no es necesario rellenarlo ya que si importamos el email también se copiará este campo. Para este ejemplo hemos copiado el código fuente de un correo legítimo de LinkedIn para que compruebes las personas que visitan tu perfil.

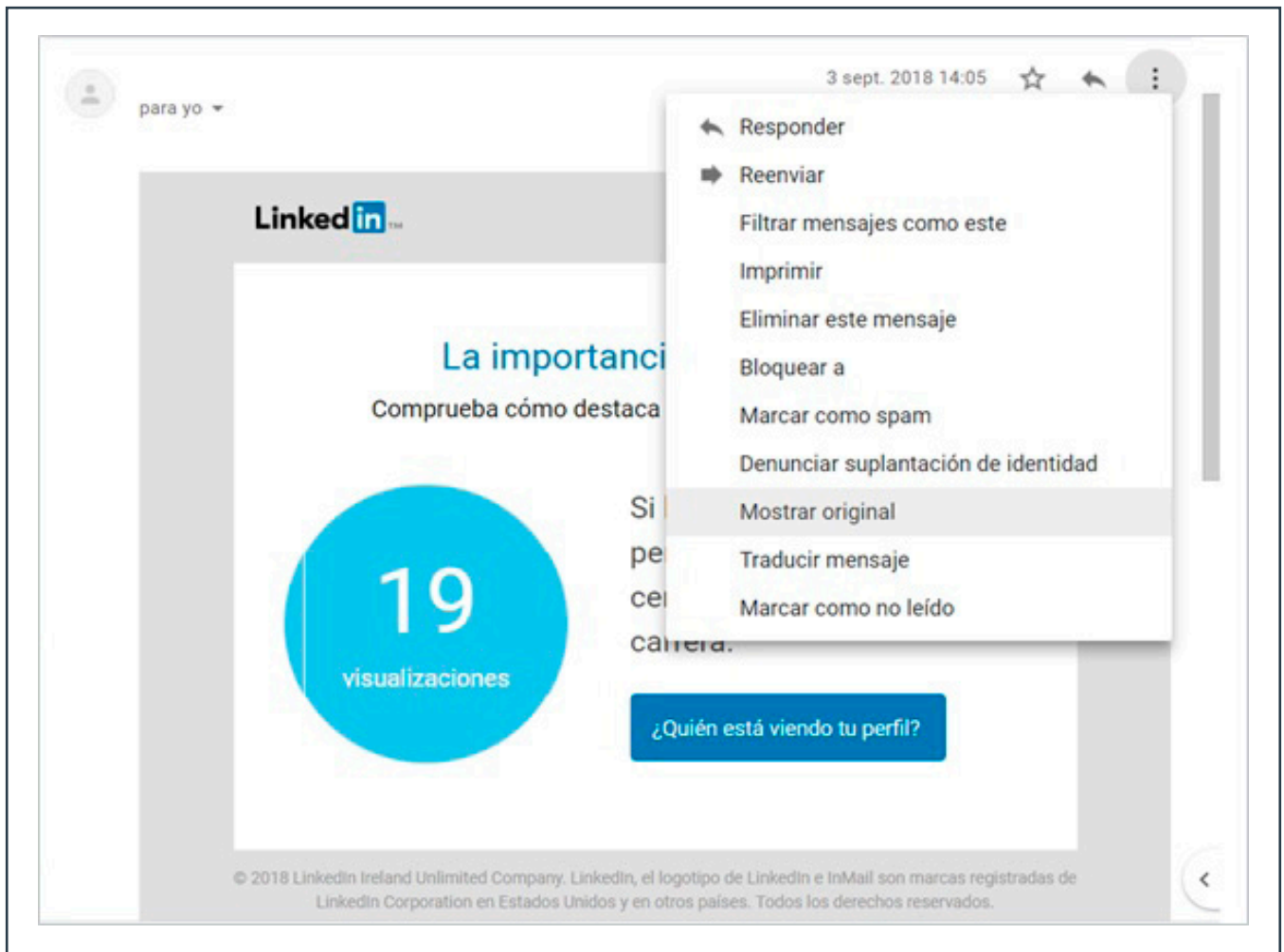


Ilustración 23. Correo legítimo de LinkedIn



# 3.

## CAMPAÑAS DE ENVÍO DE CORREOS

Al hacer clic en **Mostrar original**, aparecerá el código fuente que debemos copiar para después pegar en la ventana **Import Email**. Consulta en el punto 6.2 el procedimiento para los diferentes gestores de correo.

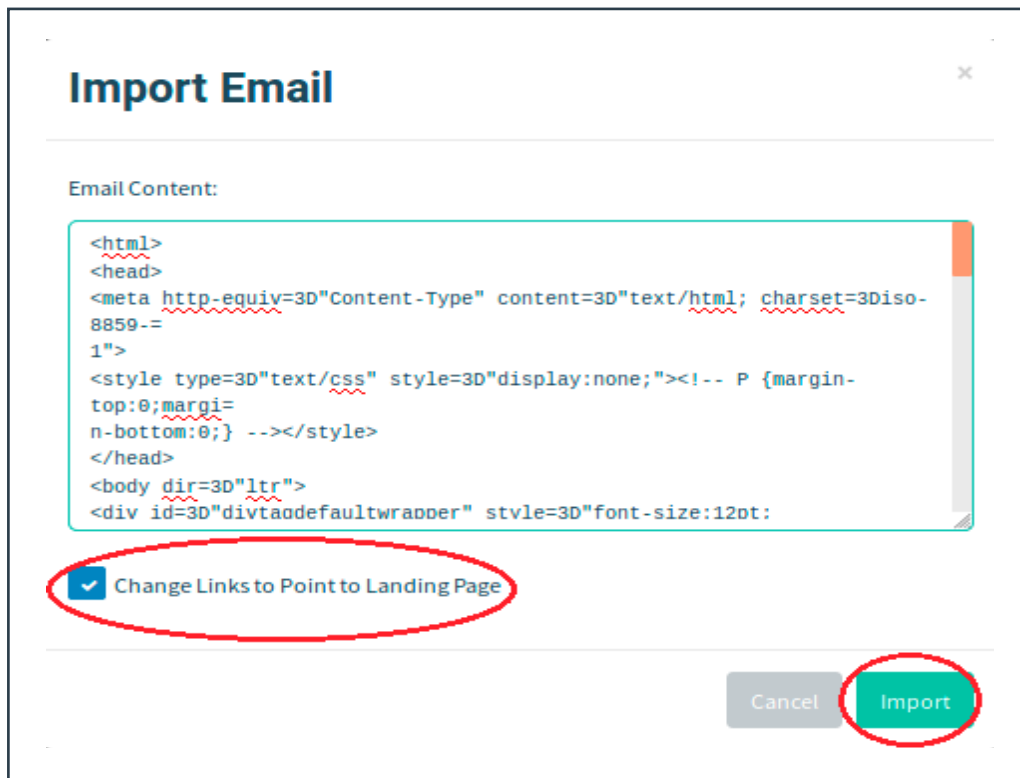


Ilustración 24. Importar correo

Haciendo clic en la opción **Change Links to Point to Landing page**, haremos que los enlaces en el texto del correo que enviemos apunten a la página de aterrizaje que hemos duplicado en el punto 3.2, por lo que el correo y la página de aterrizaje deben hacer referencia al mismo servicio.

Si queremos diseñar nuestro propio modelo de correo en lugar de importar uno que hayamos recibido, podemos obviar la opción de **Import Email** y escribir el texto que queramos, bien en texto plano (pestaña **Text**) o en código HTML (pestaña **HTML**).

En el siguiente ejemplo, accedemos a la pestaña **HTML** y hacemos clic en **Source**. A continuación escribimos un texto para que el usuario cambie su contraseña de usuario a través de un enlace que será el que le dirija a la página de phishing.

# 3.

## CAMPAÑAS DE ENVÍO DE CORREOS

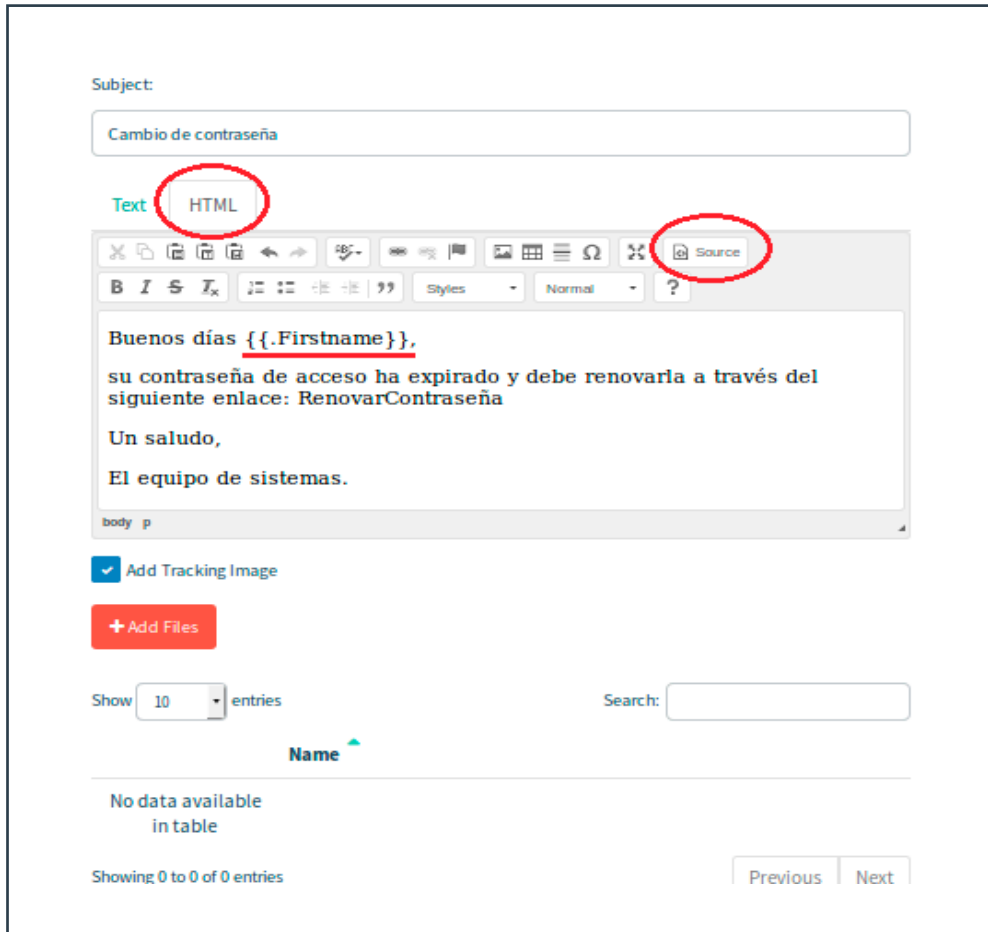


Ilustración 25. Diseño de correo

## 3.

## CAMPAÑAS DE ENVÍO DE CORREOS

Para que la aplicación muestre automáticamente los nombres, así como otros datos de los destinatarios de los correos, debemos utilizar las siguientes variables:

Variable	Descripción
{{.FirstName}}	Nombre del destinatario
{{.LastName}}	Apellido del destinatario
{{.Position}}	Cargo del destinatario
{{.Email}}	Dirección de correo del destinatario
{{.From}}	Dirección del falso remitente
{{.URL}}	La URL de la página utilizada para simular el phishing

Tabla 1. Variables

Para añadir la URL de phishing al correo, seleccionamos la palabra que queremos que sea el enlace, hacemos clic en el símbolo de hipervínculo y rellenamos los campos como se muestra en la siguiente imagen:

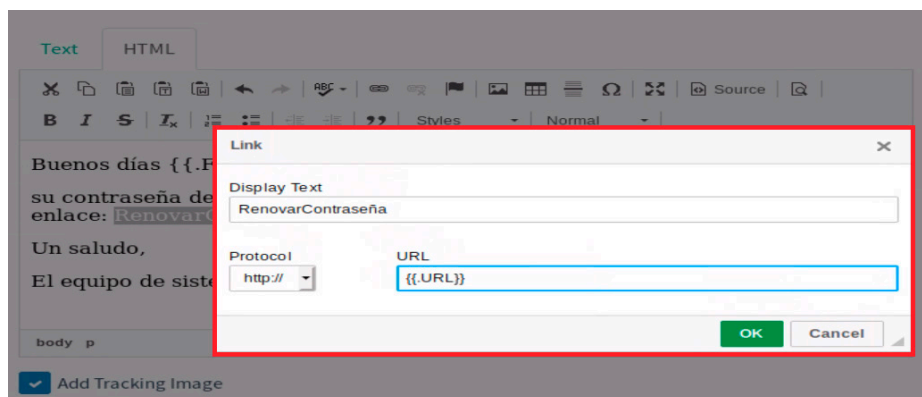


Ilustración 26. Añadir URL de phishing

Guardamos los cambios haciendo clic en **Save Template**.

# 3.

## CAMPAÑAS DE ENVÍO DE CORREOS

### 3.4. Grupo de envío de correos

Ya hemos diseñado tanto el correo como la página con los que pondremos a prueba a la comunidad universitaria. El siguiente paso es crear una lista con todas las direcciones de correo de los destinatarios del intento de phishing.

Para crear las listas de usuarios para el envío de los correos accedemos a la opción **Users & Groups** del menú principal. Haciendo clic en **New Group** obtenemos la siguiente ventana:

The screenshot shows the 'New Group' interface. At the top, there's a title 'New Group' and a close button. Below that is a 'Name:' label and a text input field containing 'Envío de phishing LinkedIn'. There are two buttons: '+ Bulk Import Users' (circled in red) and 'Download CSV Template'. Below these are four input fields: 'First Name', 'Last Name', 'Email', and 'Position', followed by a red '+ Add' button. There is a 'Show 10 entries' dropdown and a 'Search:' field. Below the search field is a table header with columns: 'First Name', 'Last Name', 'Email', and 'Position'. The table content shows 'No data available in table'. At the bottom, it says 'Showing 0 to 0 of 0 entries' and has 'Previous' and 'Next' buttons. At the very bottom right, there are 'Close' and 'Save changes' buttons, with 'Save changes' circled in red.

Ilustración 27 Grupo de envío de correos

Podemos crear nuestro grupo de usuarios importando un archivo en formato csv (desde la opción **Bulk Import Users**) o añadiendo las direcciones de correo una a una través del botón **Add**. Una vez introducidas todas las direcciones, guardamos haciendo clic en **Save changes**.

# 4.

# LANZAMIENTO DE LA CAMPAÑA DE PHISHING

Para lanzar la campaña de phishing que hemos creado en los puntos anteriores, accedemos a la opción **Campaigns** del menú principal y hacemos clic en **New Campaign**.

**New Campaign**

Name:

Email Template:

Landing Page:

URL:

Launch Date:  Send Emails By (Optional):

Sending Profile:

Groups:

Ilustración 28. Nueva campaña

# 4.

## LANZAMIENTO DE LA CAMPAÑA DE PHISHING

Rellenamos los campos con los datos que hemos utilizado en los apartados anteriores y programamos la hora de envío de los correos de phishing:

- ▶ Name: nombre que queremos asignarle a la campaña. En este caso Campaña phishing LinkedIn.
- ▶ Email template: plantilla de correo que hemos creado. Para este ejemplo será Invitación LinkedIn.
- ▶ Landing Page: página de aterrizaje falsa. Para este ejemplo utilizamos suplantación LinkedIn.
- ▶ URL: <http://127.0.0.1:80> o <https://MiDirecciónIp:80> (Donde están alojadas las páginas de aterrizaje). Esta dirección debe coincidir con la "listen\_url" del archivo config.json.

Cuando el destinatario hace clic en el correo de phishing, la URL que aparece en el navegador será similar a la de este ejemplo:

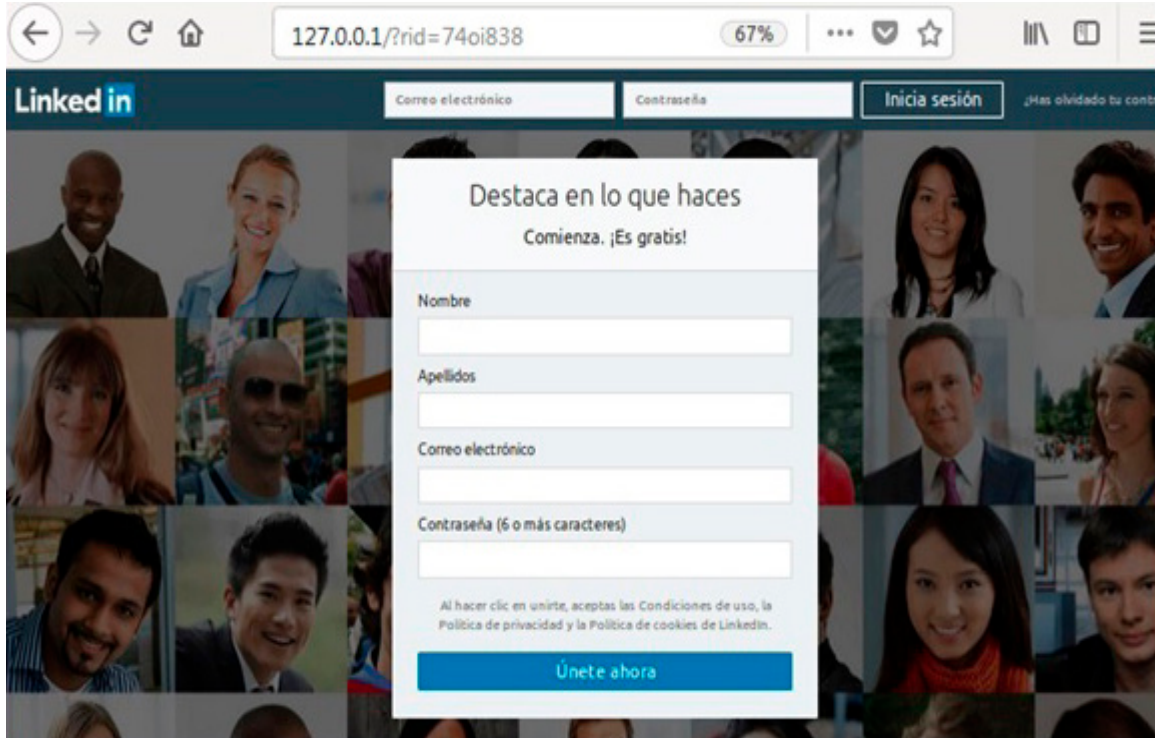


Ilustración 29. Página de phishing

## 4.

LANZAMIENTO  
DE LA CAMPAÑA DE PHISHING

Puesto que a simple vista puede resultar muy sospechosa para el usuario, podemos hacer que aparezca una URL adaptada a la campaña que queremos lanzar. En este caso remplazaremos el 127.0.0.1 por una dirección muy similar a la de inicio de sesión de LinkedIn (es.linkedin.com), como por ejemplo: es.linkedin.com/login-usuario.

Hay que tener en cuenta que cuanto más se parezca a la dirección, más difícil será percatarse del engaño.

El primer paso es cambiar la dirección 127.0.0.1 por nuestra IP como explicamos en el punto 2.4.

Si estás utilizando un sistema Linux, abre el archivo etc/hosts para editarlo. Añade la IP del servidor que has introducido en el archivo config.json y para este phishing en concreto le asignaremos el nombre de es.linkedin.com. Recordad cambiar el nombre según las diferentes campañas lanzadas.

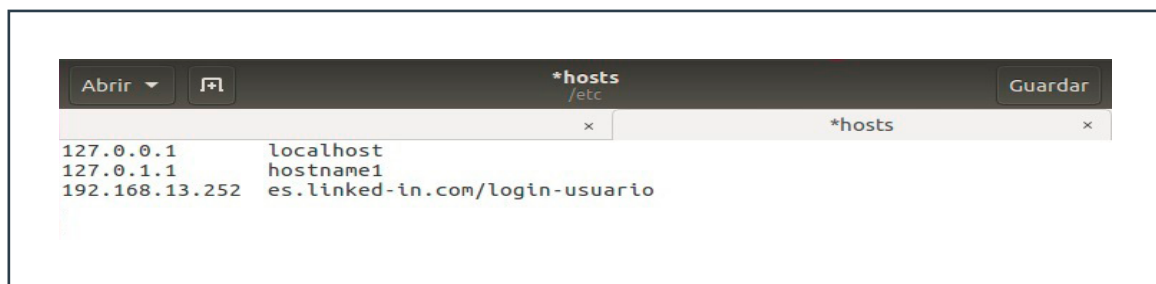


Ilustración 30. Edición del archivo hosts

Para usuarios de Windows el archivo hosts a editar se encuentra en la ruta C:\Windows\System32\Drivers\etc\hosts.

Además es necesario introducirlo también en el campo URL al crear la nueva campaña (**New Campaign**).

► Sustituimos <http://127.0.0.1:80> por [http:// es.linkedin-in.com/login-usuario:80](http://es.linkedin-in.com/login-usuario:80)

Ahora cuando los destinatarios abran el enlace del correo de phishing, visualizarán una dirección similar a la que se muestra en la siguiente imagen:

# 4.

## LANZAMIENTO DE LA CAMPAÑA DE PHISHING

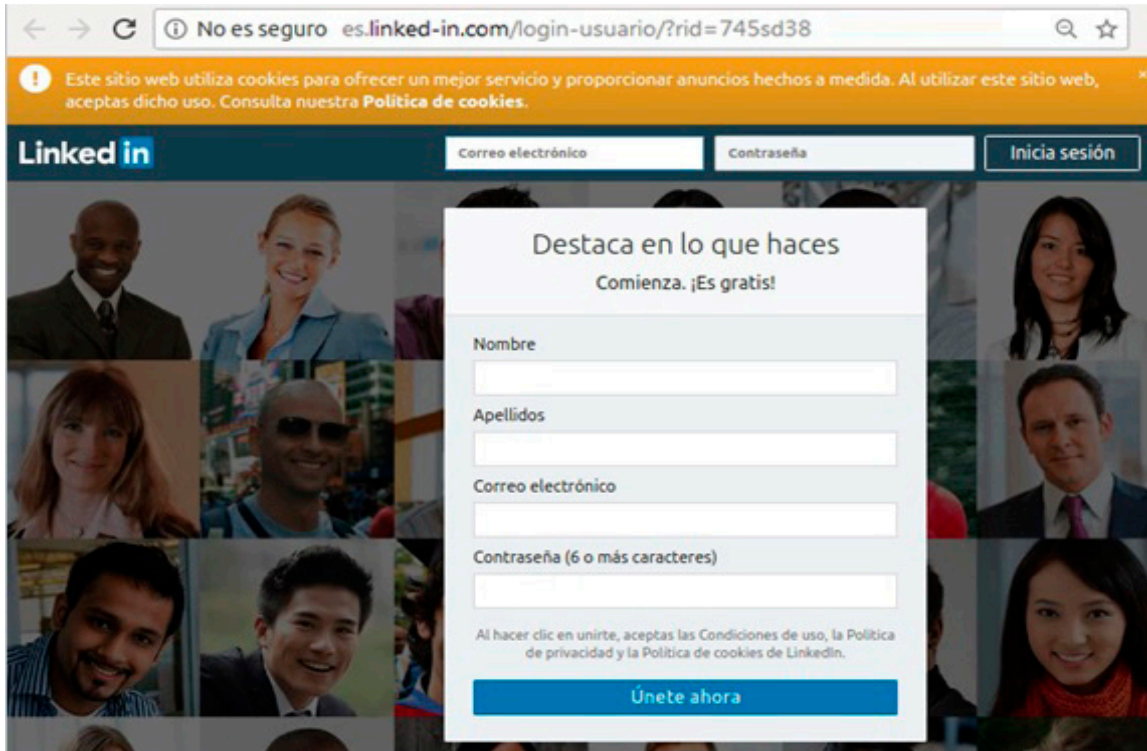


Ilustración 31. URL del phishing

Para terminar el proceso de lanzar campaña, seguimos rellenando los siguientes campos:

- ▶ **Launch Date:** Día y hora en la que se lanzará la campaña (se enviarán automáticamente los correos de phishing).
- ▶ **Send Emails By:** Si rellenamos este campo los correos se enviarán uniformemente entre la fecha que detallemos en el Launch Date y esta fecha.
- ▶ **Sending profile:** el perfil de correo que definimos en el primer paso. En este caso Gmail.
- ▶ **Groups:** se trata del grupo de correos al que enviaremos el correo de phishing. Para este ejemplo, Envío de phishing LinkedIn.

Hacemos clic en **Launch Campaign** para lanzar nuestra campaña.



# 5.

# VISUALIZACIÓN DE LOS RESULTADOS

Accediendo a la opción campañas (**Campaigns**) del menú principal, podemos ver una lista de todas las campañas creadas. Haciendo clic en el botón que representa un gráfico, podemos ver los datos de los usuarios que “han caído en nuestra trampa”.

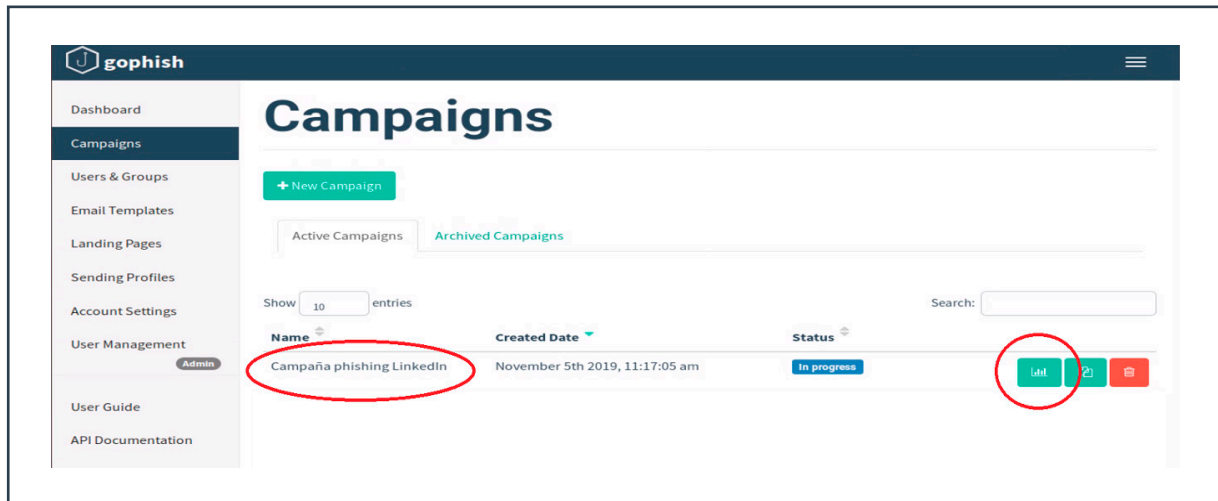


Ilustración 32. Resultados de las campañas

Haciendo clic en el botón de estadísticas, obtenemos algo similar a la siguiente captura de pantalla:

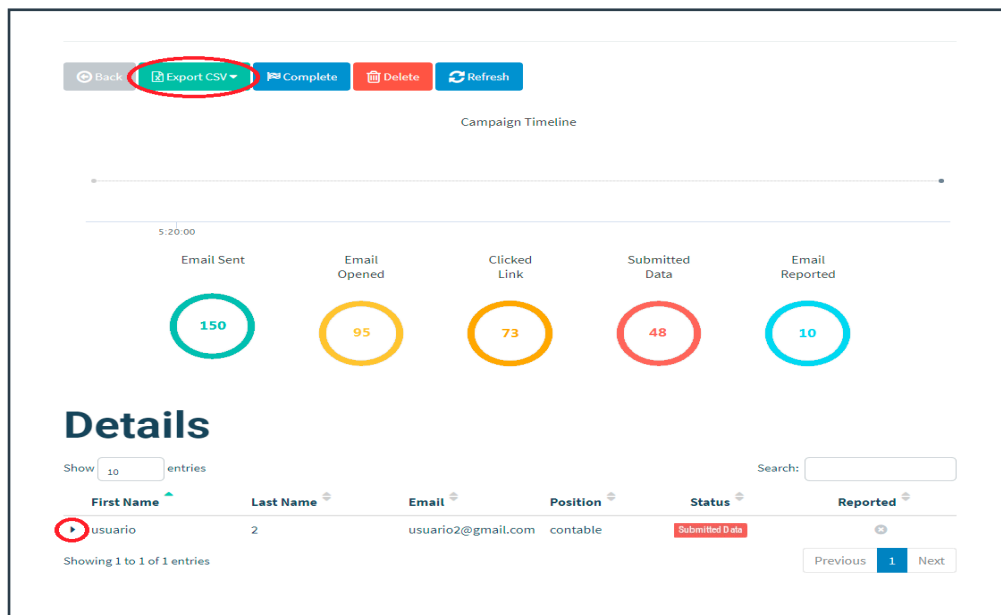


Ilustración 33. Resultados de la campaña phishing LinkedIn

## 5.

VISUALIZACIÓN  
DE LOS RESULTADOS

En la opción **Export CVS** podemos exportar los resultados de la campaña a una hoja de cálculo y así poder guardarlos en nuestros equipos.

Los datos que obtenemos de nuestra campaña de phishing son:

**Timeline for usuario 2**  
Email: usuario2@gmail.com

- Campaign Created** September 4th 2018 10:55:24 am
- Email Sent** September 4th 2018 10:55:25 am
- Clicked Link** September 4th 2018 10:56:46 am
- Submitted Data** September 4th 2018 10:57:12 am
  - Replay Credentials
  - View Details

Parameter	Value(s)
__original_url	https://www.linkedin.com/uas/login-submit
isJsEnabled	false
loginCsrfParam	b94471be-c195-45b3-8dd9-829619f4cc34
session_key	mjkjkhkhk
session_password	hkhhh

- Clicked Link** September 4th 2018 12:47:35 pm

- ▶ **Email sent:** número de correos de phishing que hemos enviado en nuestra campaña.
- ▶ **Email opened:** número de correos abiertos (esto no implica haber "picado"). Simplemente es una muestra de que el correo ha sido leído por su destinatario.
- ▶ **Clicked link:** número de usuarios que han accedido a la **Landing Page** que hemos diseñado haciendo clic en el enlace que se envió en el correo electrónico.
- ▶ **Submitted data:** número de usuarios que han introducido sus credenciales para acceder al servicio que hemos plagiado a través de la **Landing Page**.
- ▶ **Email Reported:** se trata del número de usuarios que han identificado el correo como fraudulento y lo han reportado como tal a través de su gestor de correo electrónico. Actualmente esta opción se encuentra en vías de desarrollo.

**Ilustración 34. Detalle por usuario**

En la parte de **Details** podemos ver detalladamente los usuarios que han picado en el phishing. Al hacer clic en la flecha situada a la izquierda del nombre del usuario que ha abierto el correo, se desplegará una lista con los detalles de la campaña para ese usuario, como se muestra en la imagen.

En el **Timeline** se puede ver el usuario y la contraseña introducidos por el usuario (siempre y cuando hayamos habilitado la opción de **Capture Submit Data y Capture Password**).

Ahora, ya sabes todo lo que necesario para lanzar una campaña de phishing con Gophish. ¿A qué esperas? Pon a prueba a la comunidad universitaria, entrénala y haz que tu universidad sea más segura.

# 6.

# ANEXO

## 6.1. Campaña de phishing: El fraude del RECTOR

A continuación se detalla un ejemplo de cómo lanzar una campaña de phishing llamada "El fraude del RECTOR". Puedes consultar todos los detalles sobre este phishing en: [Historias reales: el fraude del CEO](#)

Al igual que hicimos en la campaña de LinkedIn 4, y asumiendo que hemos creado nuestro perfil de envío como indicamos en el punto 3.1, añadimos la **Landing Page** a la que se accederá cuando el usuario haga clic en el enlace enviado en el correo.

En este caso será una página que le advierta directamente de su error y de que, de haber sido real, habría caído en la trampa de los ciberdelincuentes. Además, en esta página encontrará información sobre este tipo de fraudes y cómo aprender a reconocerlos.

### 6.1.1. Página de aterrizaje

Como explicamos anteriormente, al hacer clic en la opción **Landing Page** del menú principal y posteriormente en el botón **New Page**, se abrirá una ventana que completaremos con los siguientes datos:

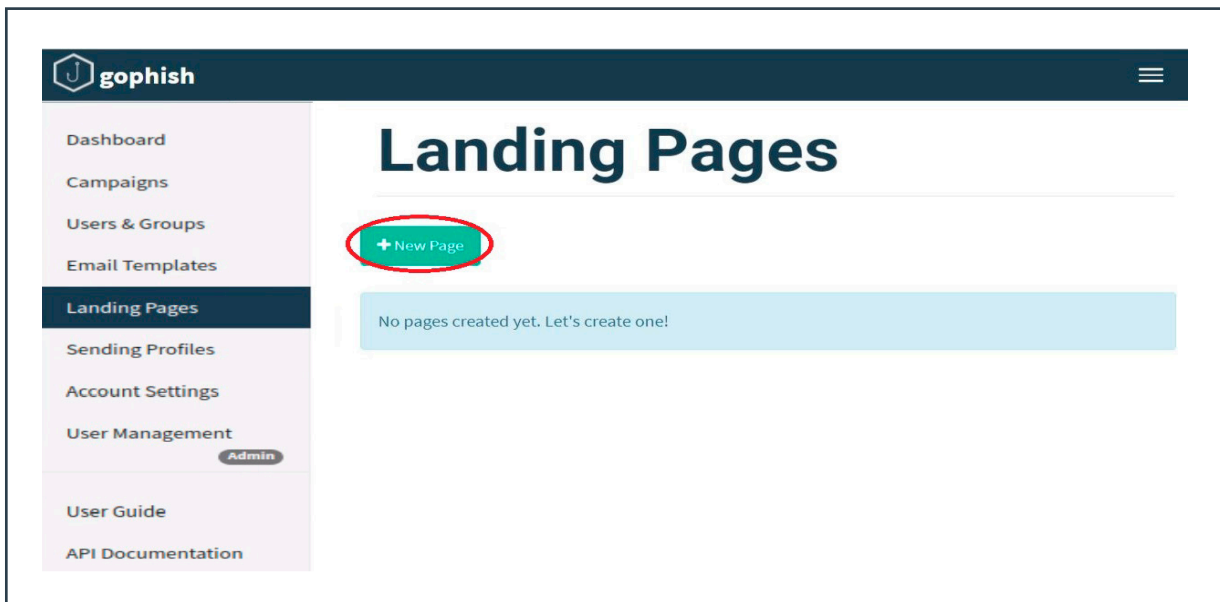
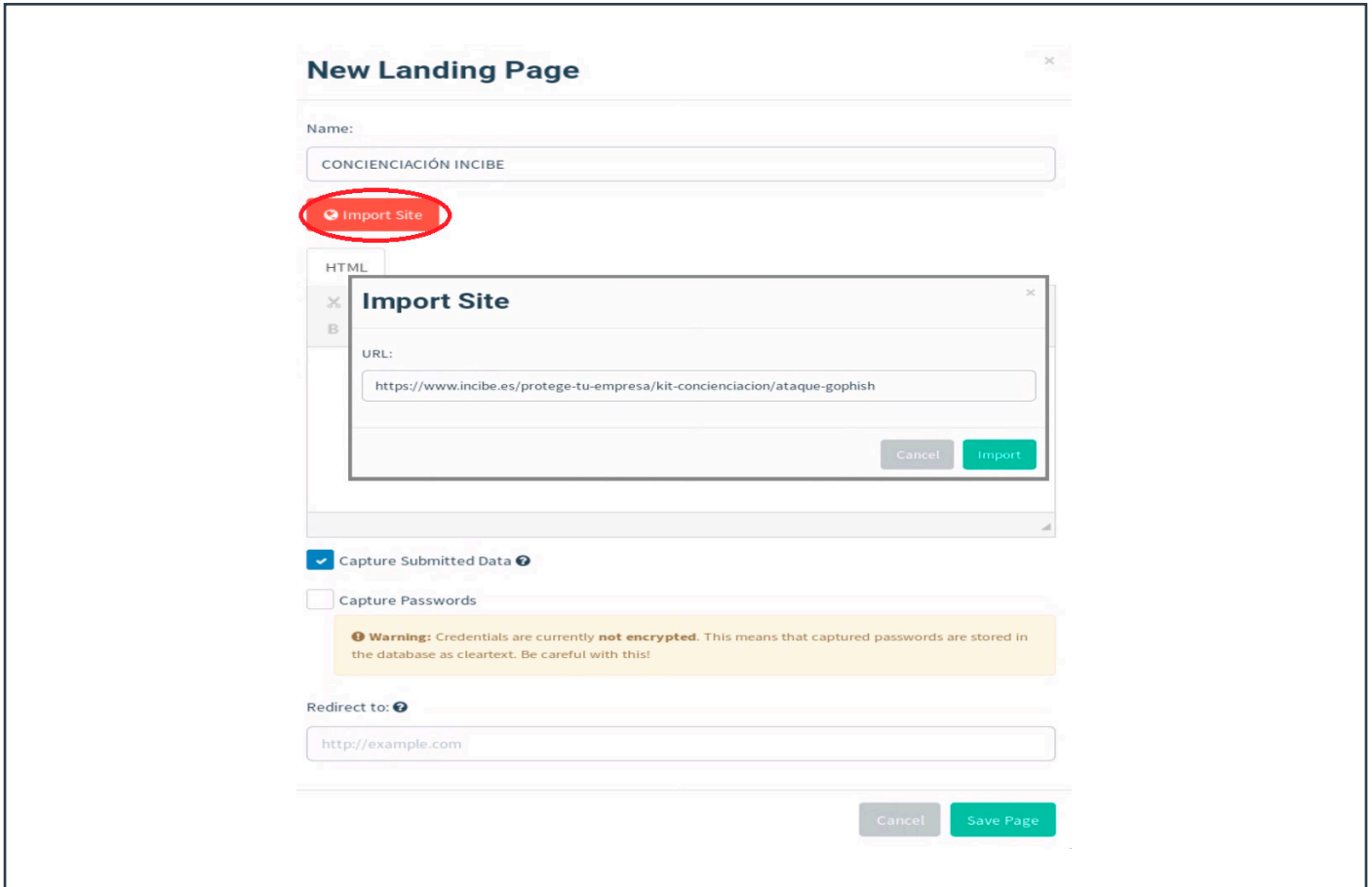


Ilustración 35. Nueva página de aterrizaje

# 6.

## ANEXO



**Ilustración 36. Página de aterrizaje - concienciación INCIBE**

Elegimos un nombre descriptivo de la página. En este caso "CONCIENCIACIÓN INCIBE". Hacemos clic en **Import Site** y en la nueva ventana introducimos la URL de la página a copiar. En este ejemplo utilizamos una página especialmente diseñada para concienciar al usuario sobre este tipo de ataques, para que aprenda a identificarlos y a cómo reaccionar si ha sido víctima de uno de ellos.

La dirección de la página de concienciación es la siguiente: <https://www.incibe.es/protege-tu-empresa/kit-concienciacion/ataque-gophish>

Activamos la opción **Captured Submitted Data**. En esta ocasión no es necesario introducir una página para la redirección, ya que queremos que el usuario se quede en la página de concienciación.

Guardamos todos los cambios realizados haciendo clic en **Save Page**.

# 6.

## ANEXO

### 6.1.2. Plantilla de correo

Para crear esta plantilla proporcionamos, a modo de ejemplo, el código de un correo tipo del fraude del RECTOR. Accedemos a la configuración de la plantilla a través de la opción del menú principal **Email Templates > New Template** e importamos el código haciendo clic en el botón **Import Email**.

The screenshot shows the 'New Template' configuration window. At the top, the title is 'New Template'. Below it, there is a 'Name:' field containing 'FRAUDE DEL CEO'. A red circle highlights the 'Import Email' button. Below the name field is a 'Subject:' field. Underneath is a rich text editor with 'Text' and 'HTML' tabs. The editor has a toolbar with various icons and a 'Source' button. Below the editor, there is a checked checkbox for 'Add Tracking Image' and a red '+ Add Files' button. At the bottom, there is a 'Show 10 entries' dropdown, a 'Search:' field, and a table with the header 'Name'. The table is empty, with the message 'No data available in table' and 'Showing 0 to 0 of 0 entries'. A 'Previous' and 'Next' button are also present. At the very bottom, there are 'Cancel' and 'Save Template' buttons, with the 'Save Template' button circled in green.

Ilustración 37. Nueva plantilla - Fraude del CEO

# 6.

## ANEXO

Copia y pega el código fuente del correo ejemplo del fraude del RECTOR:

```
MIME-Version: 1.0
Date: Tue, 29 Oct 2019 12:13:30 +0100
Message-ID: <CAA-6bagSdnmOz0VEC=C8xHx4gBFptRMK8Tq1J-b9ihS2yV26zQ@mail.gmail.com>
Subject: Colaboracion
From: Protege Tu Empresa <protegetuempresa5@gmail.com>
To: Protege Tu Empresa <protegetuempresa5@gmail.com>
Content-Type: multipart/alternative; boundary="000000000000d2e16505960ab4fb"

--000000000000d2e16505960ab4fb
Content-Type: text/plain; charset="UTF-8"
Content-Transfer-Encoding: quoted-printable

Buenos d=C3=ADas,

necesito tu ayuda para una operaci=C3=B3n confidencial.
=C2=BFPuedo contar con tu discreci=C3=B3n?
Descarga estos documentos donde se explica todo en detalle:
Documentacion.rar

Un cordial saludo,

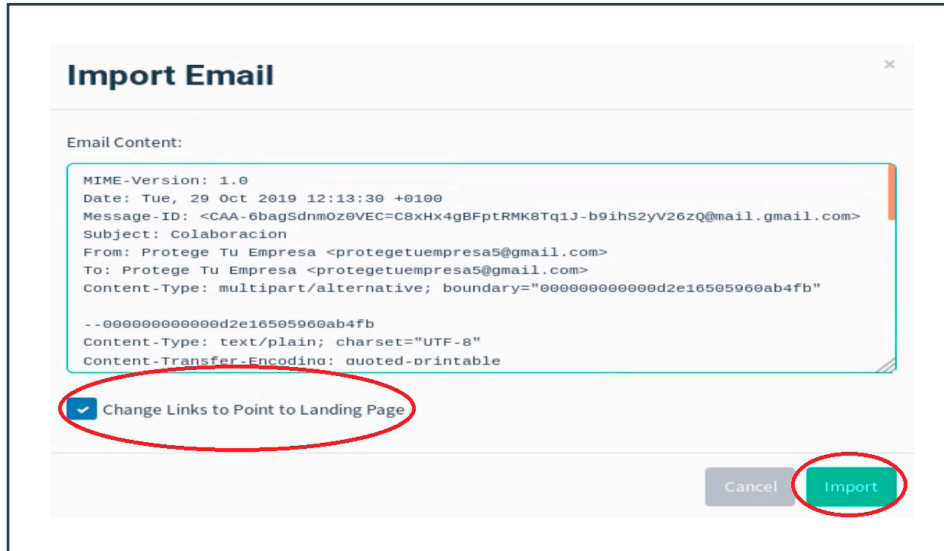
--000000000000d2e16505960ab4fb
Content-Type: text/html; charset="UTF-8"
Content-Transfer-Encoding: quoted-printable

<div dir=3D"ltr">Buenos d=C3=ADas,</div><br></div><div>necesito tu ayuda par=
a una operaci=C3=B3n confidencial.</div><div>=C2=BFPuedo contar con tu disc=
reci=C3=B3n?</div><div>Descarga estos documentos donde se explica todo en d=
etalle: <a href=3D"http://Documentacion.rar">Documentacion.rar</a></div><di=
v><br></div><div>Un cordial saludo,</div></div>

--000000000000d2e16505960ab4fb--
```

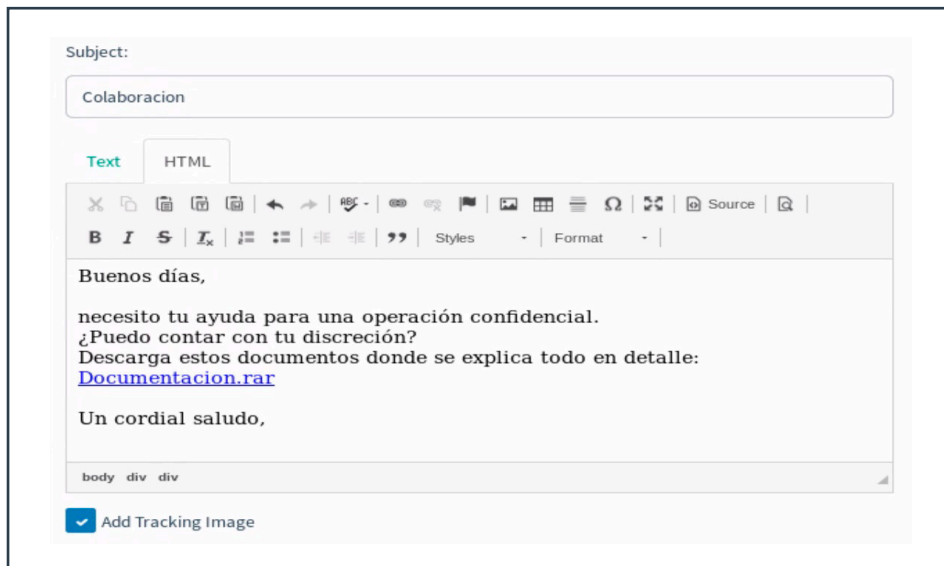
# 6.

## ANEXO



**Ilustración 38. Importando código fuente**

Es importante habilitar la opción **Change Links to Point to Landing Page**, así el enlace del correo apuntará a la página de concienciación de INCIBE y además aparecerá contabilizado en los informes. Además podemos adaptar este mensaje a nuestras necesidades, una vez importado, cambiando el texto que aparece en la **pestaña HTML**.



**Ilustración 39. Edición del texto del correo**

Finalizamos el diseño de la plantilla haciendo clic en el botón **Save Template**, como se muestra en la imagen "Nueva plantilla - Fraude del RECTOR"

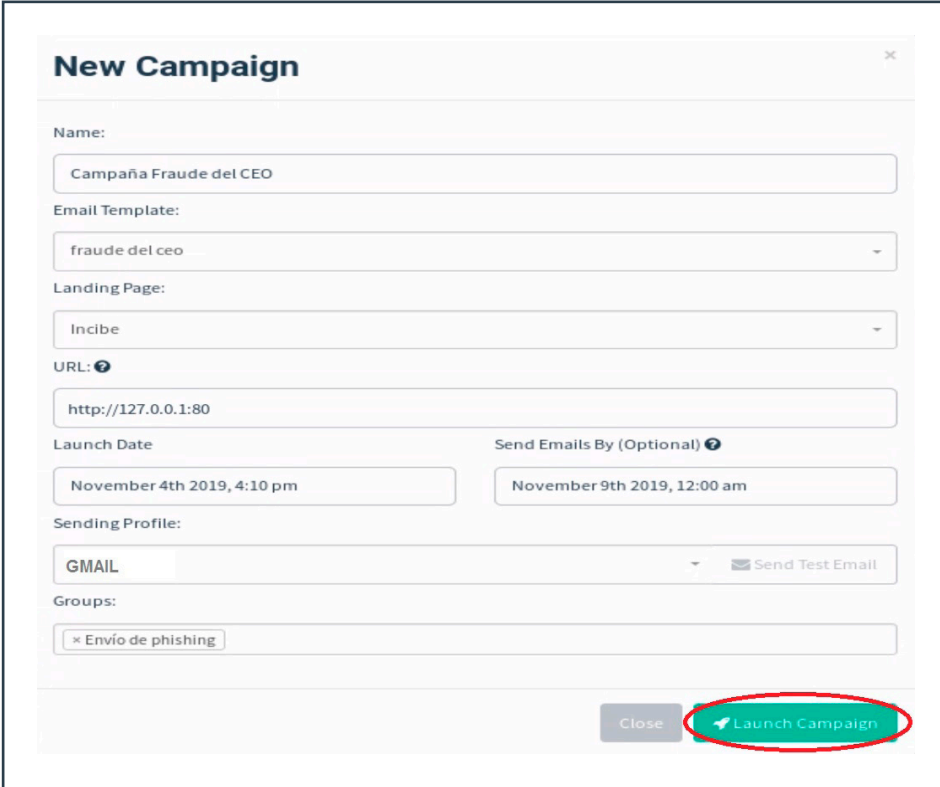
# 6.

## ANEXO

### 6.1.3. Lanzamiento de la campaña Fraude del RECTOR

Para crear la nueva campaña, accede a través de la opción **Campaign > New Campaign** y rellena los campos como se muestra en la siguiente imagen. Vuelve al punto 4 si necesitas recordar el detalle de cada campo.

Elige la fecha de lanzamiento **Launch Date** en la que quieras lanzar la campaña y configura el campo **Send Emails By** si prefieres que los correos no se envíen todos a la vez sino entre las fechas indicadas.



The screenshot shows the 'New Campaign' form with the following details:

- Name:** Campaña Fraude del CEO
- Email Template:** fraude del ceo
- Landing Page:** Incibe
- URL:** http://127.0.0.1:80
- Launch Date:** November 4th 2019, 4:10 pm
- Send Emails By (Optional):** November 9th 2019, 12:00 am
- Sending Profile:** GMAIL (with a 'Send Test Email' button)
- Groups:** Envío de phishing

The 'Launch Campaign' button is circled in red.

Ilustración 40. Nueva campaña

Para finalizar la programación de la campaña, hacemos clic en **Launch Campaign**.

Consulta el punto 5 para recordar cómo se interpretan los resultados de la campaña lanzada y saber cuántos usuarios han caído en la trampa.

En el siguiente apartado explicamos cómo obtener el código fuente en los gestores de correo más utilizados para crear las plantillas en Gophish.



# 6.

## ANEXO

### 6.2. Cómo obtener el código fuente de un correo electrónico en los distintos gestores de correo

#### OUTLOOK

1. Accedemos al correo del que queremos obtener el código fuente.
2. En la parte superior izquierda del menú seleccionamos la opción **Archivo**.

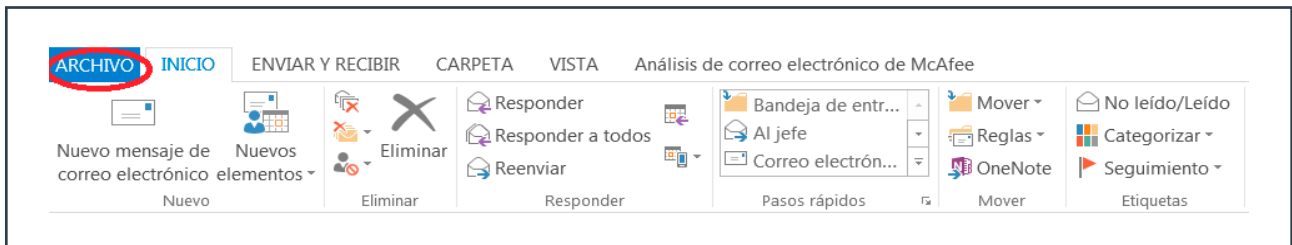


Ilustración 41. Outlook pestaña Archivo

3. En la lista desplegable que se muestra elegimos la opción **Guardar como**.

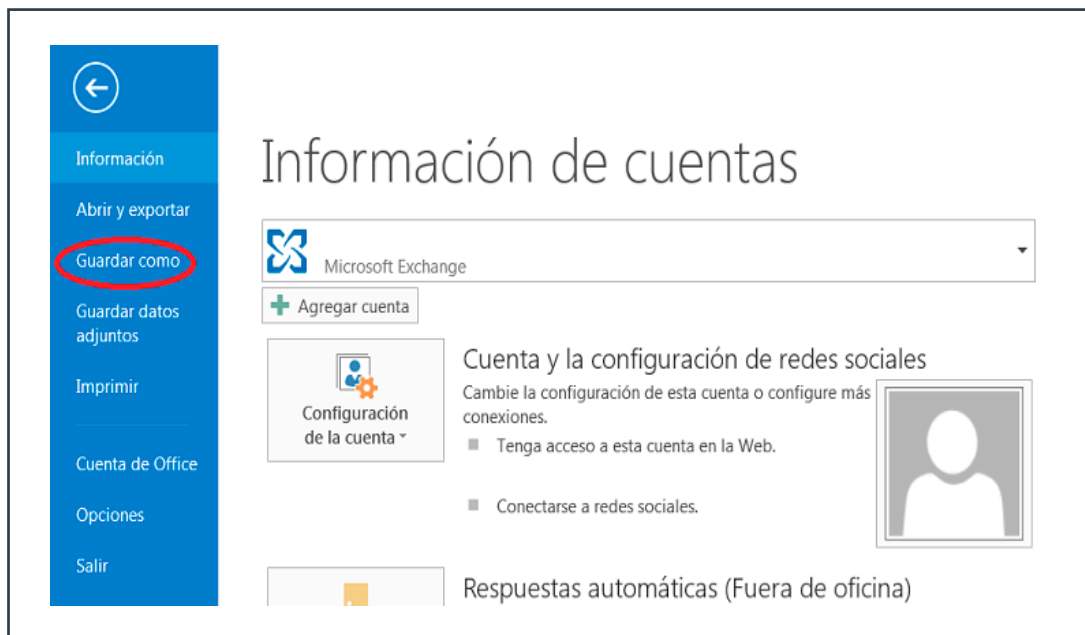
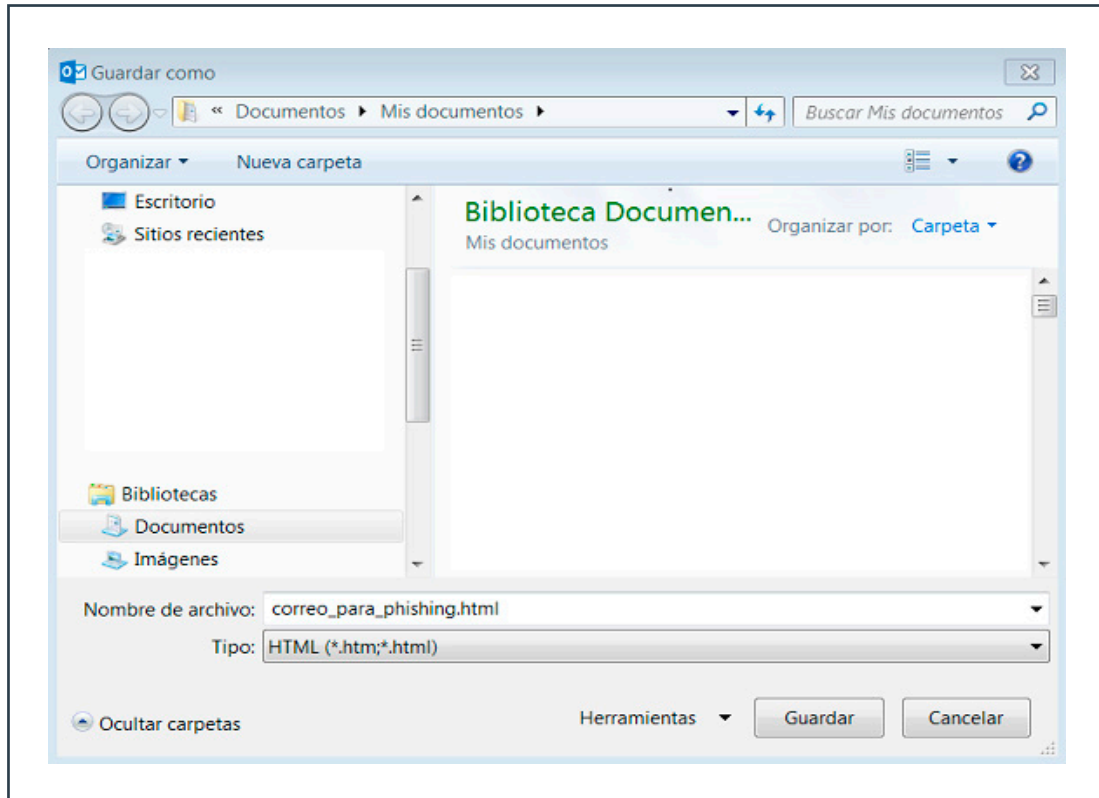


Ilustración 42. Outlook Guardar como

# 6.

## ANEXO

4. Guardamos el mensaje en nuestro equipo con el nombre que elijamos y el **Tipo HTML**, por ejemplo: correo\_para\_phishing.html



**Ilustración 43. Hotmail guardar correo para phishing.html**

5. El código fuente del correo está en el archivo que hemos creado. Cópialo en la plantilla de Gophish, como se explica en el punto 3.3.

# 6.

## ANEXO

### THUNDERBIRD

1. Accedemos al correo del que queremos obtener el código fuente.
2. En el menú superior derecho elegimos la opción **Más** y dentro del desplegable **>Ver código fuente**.

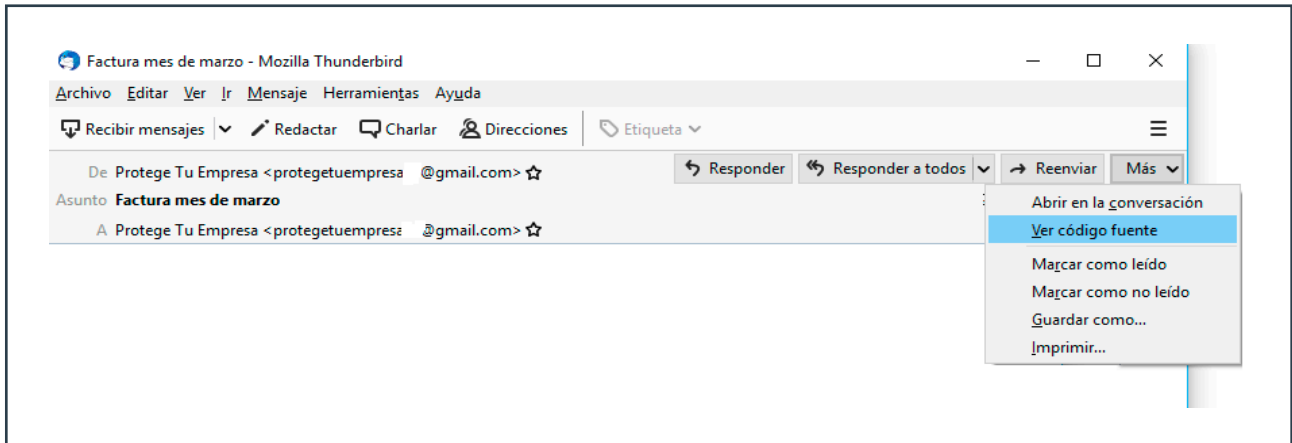


Ilustración 44. Thunderbird ver código fuente

3. A continuación se abrirá una nueva ventana con el código fuente del correo en cuestión.

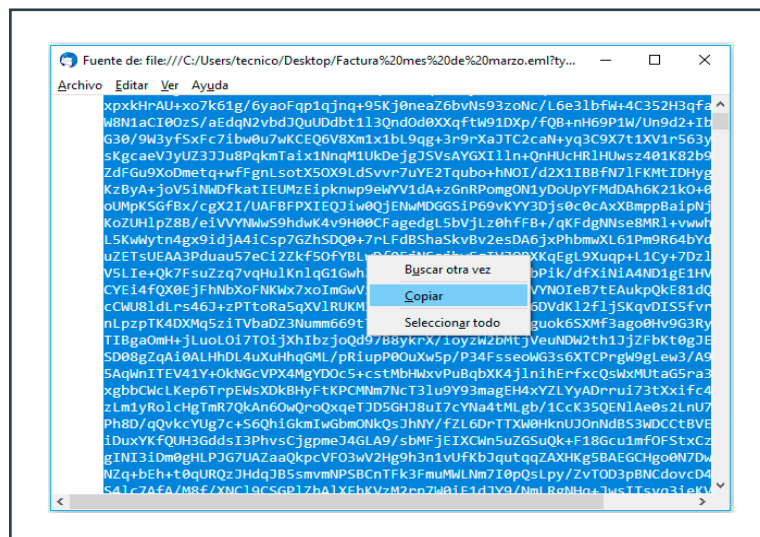


Ilustración 45. Copiar código fuente en Thunderbird

4. Cópialo en la plantilla de Gophish, como se explica en el punto 3.3.

# 6.

## ANEXO

### MAIL PARA MAC

1. Accedemos al correo del que queremos obtener el código fuente.
2. Ve a **Visualización > Mensaje > Fuente sin formato**.

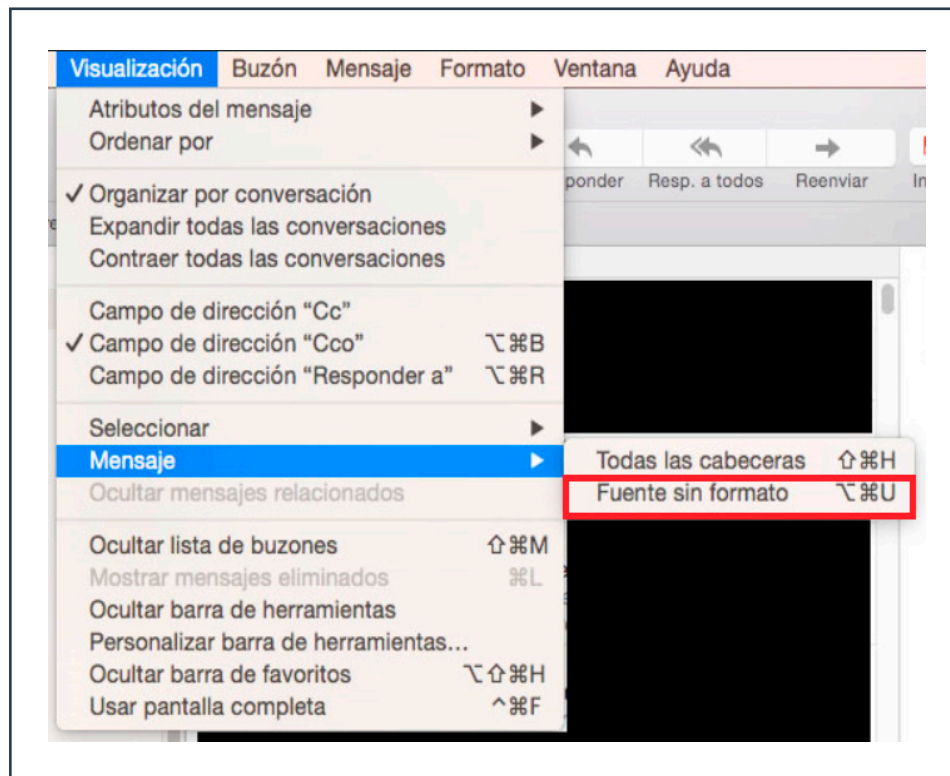


Ilustración 46. Mail para Mac, Fuente sin formato

3. A continuación, se mostrará el código fuente del correo.
4. Cópialo en la plantilla de Gophish, como se explica en el punto 3.3.

# 6.

## ANEXO

### OUTLOOK

1. Accedemos al correo del que queremos obtener el código fuente.
2. Desplegamos la lista situada en la parte superior derecha del correo haciendo clic en la flecha, tal y como muestra la imagen a continuación.

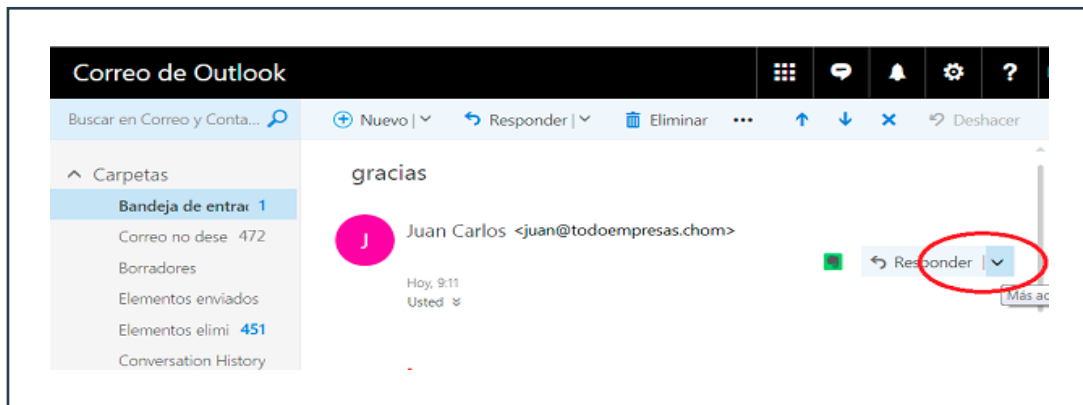


Ilustración 47. Outlook acceso al menú

3. De la lista que obtenemos seleccionamos la opción Ver origen del mensaje.

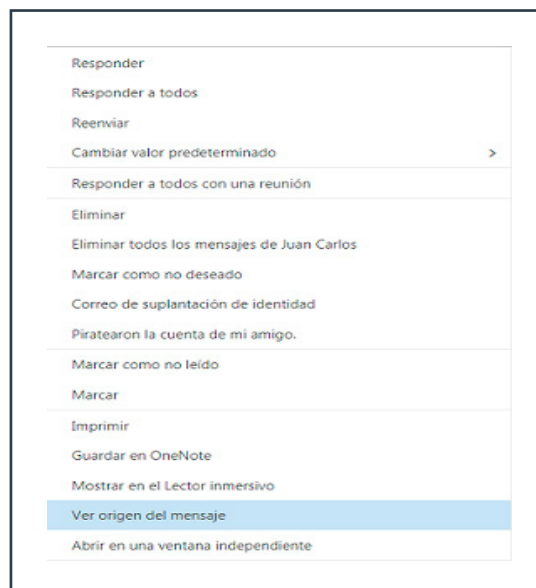


Ilustración 48. Outlook Ver origen del mensaje

# 6.

## ANEXO

4. Selecciona el texto, cópialo y pégalo en la plantilla de Gophish, como se explica en el punto 3.3.

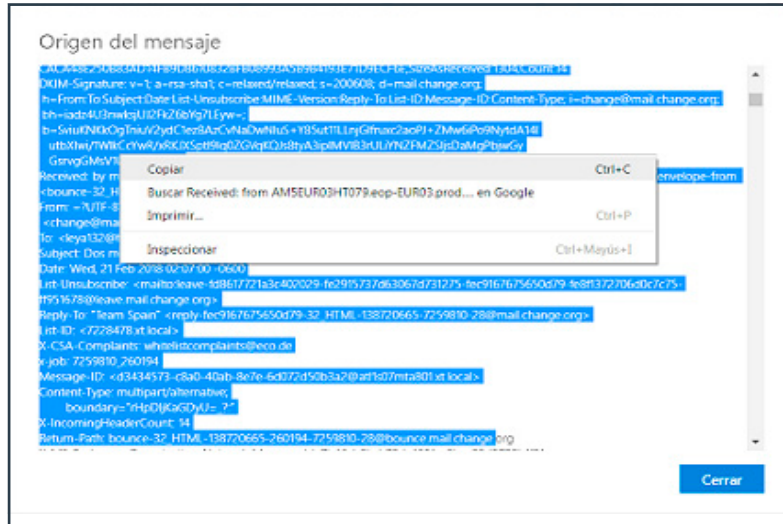


Ilustración 49. Outlook Copiar

### YAHOO

1. Accedemos al correo del que queremos obtener el código fuente.
2. Desplegamos la lista situada en la parte superior derecha del correo haciendo clic en la línea de puntos. De la lista desplegada elegimos la opción **Ver mensaje sin formato**.

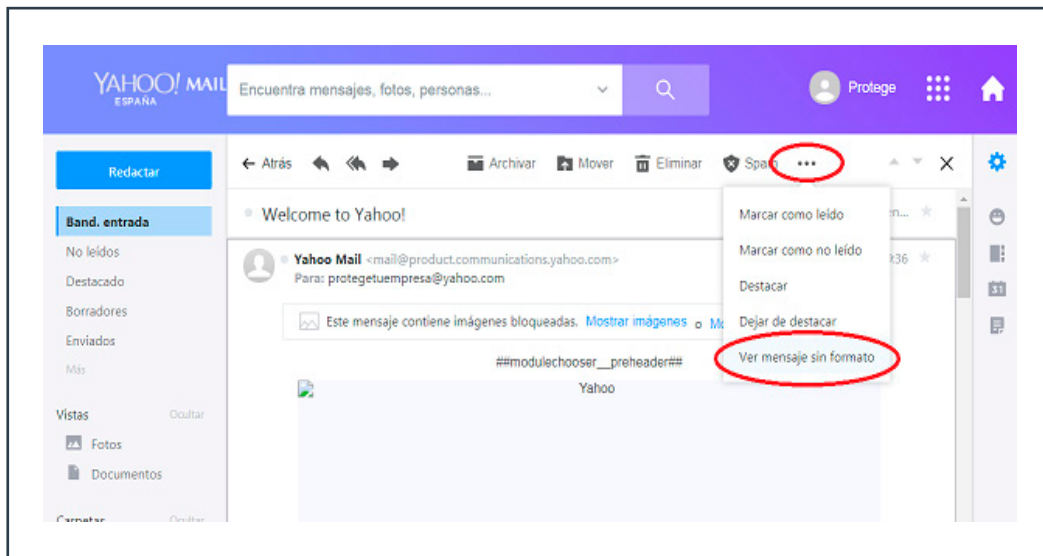


Ilustración 50. Yahoo Ver mensaje sin formato

# 6.

## ANEXO

3. Se abrirá una nueva pestaña en el navegador como se muestra en la imagen siguiente. Selecciona todo el texto, haz clic con el botón derecho y elige la opción **Copiar**. Pega el texto seleccionado en la plantilla de Gophish, como se explica en el punto 3.3.

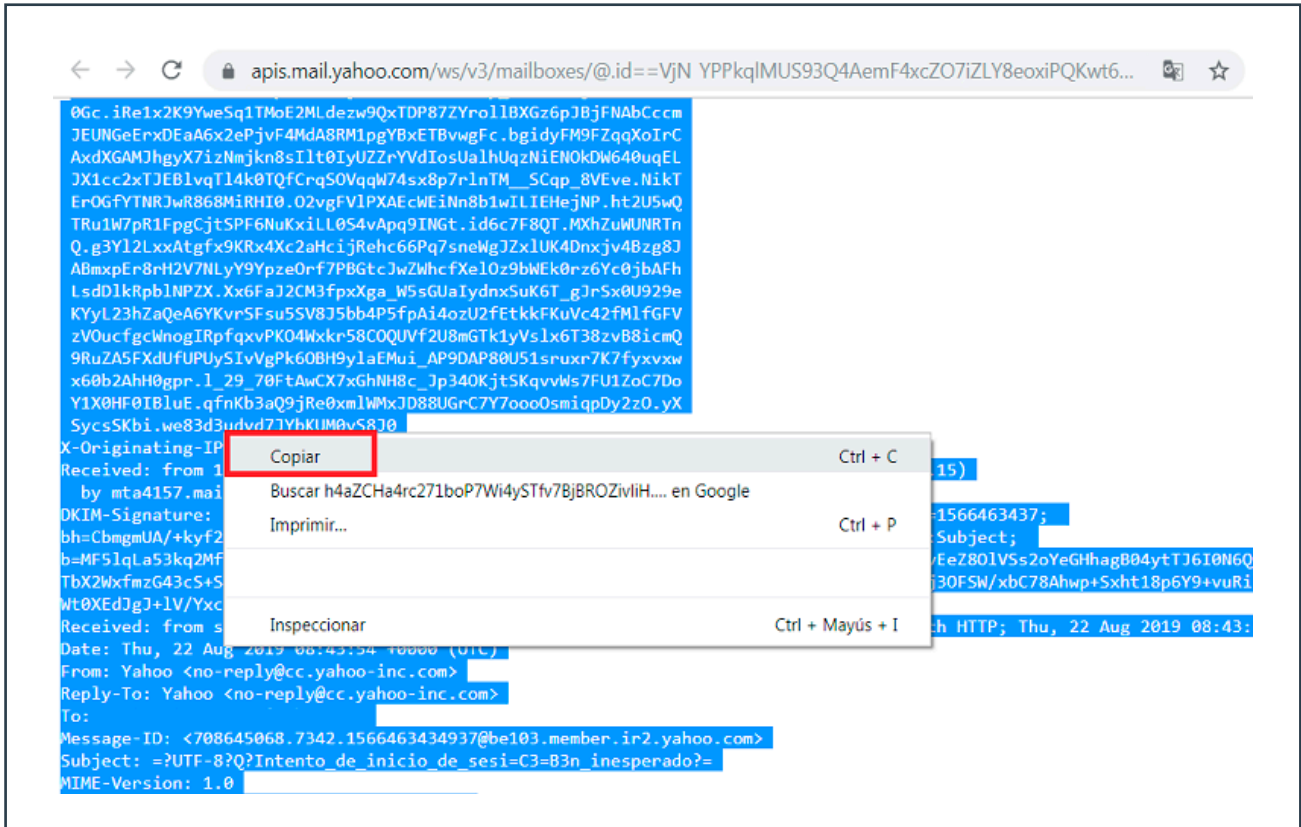


Ilustración 51. Yahoo Copiar