



---

# PRÁCTICA 4 - PHISING

---

ADRIÁN ALONSO RIDAO



2º ASIR  
1ª EVALUACIÓN  
CIBERSEGURIDAD

## Contenido

1.	Descarga e Instalación de Gophish.....	2
2.	Descarga e instalación de Ngrok.....	3
3.	Acceder a Gophish.....	4
4.	Campaña de envío de correos .....	6
5.	Lanzamiento de la campaña de phishing .....	14
6.	Conclusiones.....	18
6.1.	Lecciones aprendidas sobre técnicas de ingeniería social. ....	18
6.2.	Medidas de mitigación recomendadas para la organización simulada. ....	19
7.	Aspectos éticos .....	19

# 1. Descarga e Instalación de Gophish.

Para poder obtener Gophish nos dirigimos a <https://github.com/gophish/gophish/releases> Y descargamos la versión para Windows.

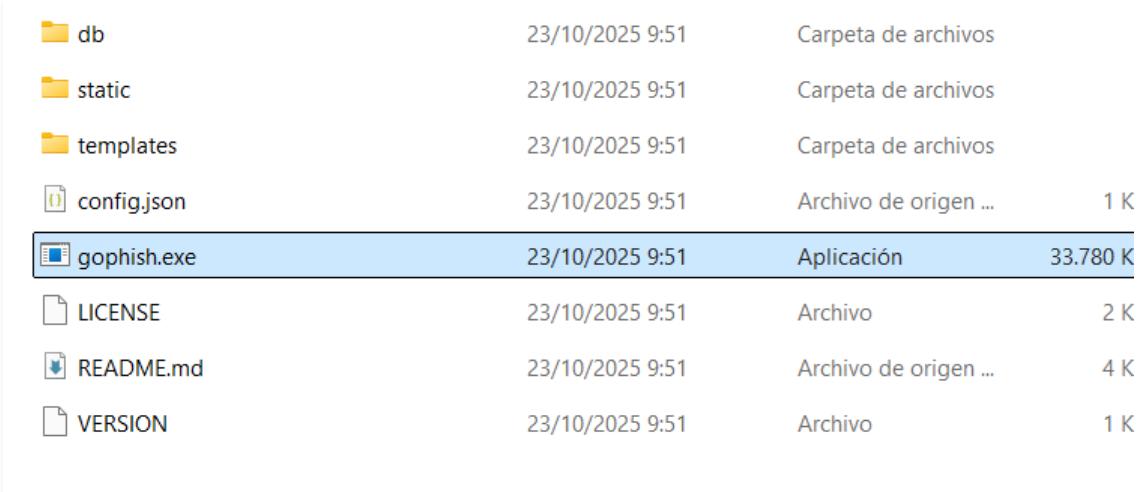


The screenshot shows the 'Assets' section of a GitHub release page. There are six items listed:

Asset	Size	Last Updated
gophish-v0.12.1-linux-32bit.zip	31.4 MB	Sep 14, 2022
gophish-v0.12.1-linux-64bit.zip	31.8 MB	Sep 14, 2022
gophish-v0.12.1-osx-64bit.zip	33.2 MB	Sep 14, 2022
<b>gophish-v0.12.1-windows-64bit.zip</b>	32.1 MB	Sep 14, 2022
Source code (zip)		Sep 14, 2022
Source code (tar.gz)		Sep 14, 2022

Below the table, there are reaction icons and a note: "142 people reacted".

Una vez descargamos nuestra versión para Windows descomprimimos la carpeta y ejecutamos el archivo .exe.



db	23/10/2025 9:51	Carpeta de archivos	
static	23/10/2025 9:51	Carpeta de archivos	
templates	23/10/2025 9:51	Carpeta de archivos	
config.json	23/10/2025 9:51	Archivo de origen ...	
<b>gophish.exe</b>	23/10/2025 9:51	Aplicación	33.780 K
LICENSE	23/10/2025 9:51	Archivo	2 K
README.md	23/10/2025 9:51	Archivo de origen ...	4 K
VERSION	23/10/2025 9:51	Archivo	1 K

Esto abrirá la cmd para proceder con la instalación.

```

OK 20160225173824_0.1.2_capture_credentials.sql
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 20171927213457_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
OK 20190105192341_0.8.0_rbac.sql
OK 20191104103301_0.9.0_create_webhooks.sql
OK 20200116000000_0.9.0_imap.sql
OK 20200619000000_0.11.0_password_policy.sql
OK 20200730000000_0.11.0_imap_ignore_cert_errors.sql
OK 20200914000000_0.11.0_last_login.sql
OK 20201201000000_0.11.0_account_locked.sql
OK 20220321133237_0.4.1_envelope_sender.sql
time="2025-10-23T09:52:55+02:00" level=info msg="Please login with the username admin and the password 10eb3bd9f88aad2c"
time="2025-10-23T09:52:55+02:00" level=info msg="Starting IMAP monitor manager"
time="2025-10-23T09:52:55+02:00" level=info msg="Starting phishing server at http://0.0.0.0:80"
time="2025-10-23T09:52:55+02:00" level=info msg="Creating new self-signed certificates for administration interface"
time="2025-10-23T09:52:55+02:00" level=info msg="Background Worker Started Successfully - Waiting for Campaigns"
time="2025-10-23T09:52:55+02:00" level=info msg="Starting new IMAP monitor for user admin"
time="2025-10-23T09:52:55+02:00" level=info msg="TLS Certificate Generation complete"
time="2025-10-23T09:52:55+02:00" level=info msg="Starting admin server at https://127.0.0.1:3333"
|

```

## 2. Descarga e instalación de Ngrok

Debemos registrarnos en la página web de Ngrok. Al hacer eso iniciaremos la descarga de la Api a través de la tienda de Microsoft.

Una vez instalada en nuestra cmd infresaremos el código **ngrok config add-authtoken 34TPKJcknHaKlnNMumOeOXOvCFU\_5Rj2QTPatwiwj2JZEStLu** para agregar una autenticación al archivo de configuración ngrok.yml

```

C:\Users\Usuario>ngrok config add-authtoken 34TPKJcknHaKlnNMumOeOXOvCFU_5Rj2
QTPatwiwj2JZEStLu
Authtoken saved to configuration file: C:\Users\Usuario\AppData\Local/ngrok/
ngrok.yml

```

Una vez realizada esta operación ponemos el comando **ngrok http 172.16.115.58:8080**, que es nuestra ip de área local. Nos aparecerá esto:

```

Símbolo del sistema - ngrok | × + ⌂
ngrok
(CTRL+C to quit)

◆ Block threats before they reach your services with new WAF actions → https://ngrok.com/r/waf

Session Status          online
Account                 adrianaalonso.rida@gmail.com (Plan: Free)
Version                3.24.0-msix
Region                 Europe (eu)
Latency                33ms
Web Interface          http://127.0.0.1:4040
Forwarding             https://semirhythical-undevastatingly-rosamond.ngrok-free.dev → http://172.16.115.58:8080

Connections            ttl     opn     rt1     rt5     p50     p90
                        3       0      0.00    0.00   10.04   10.08

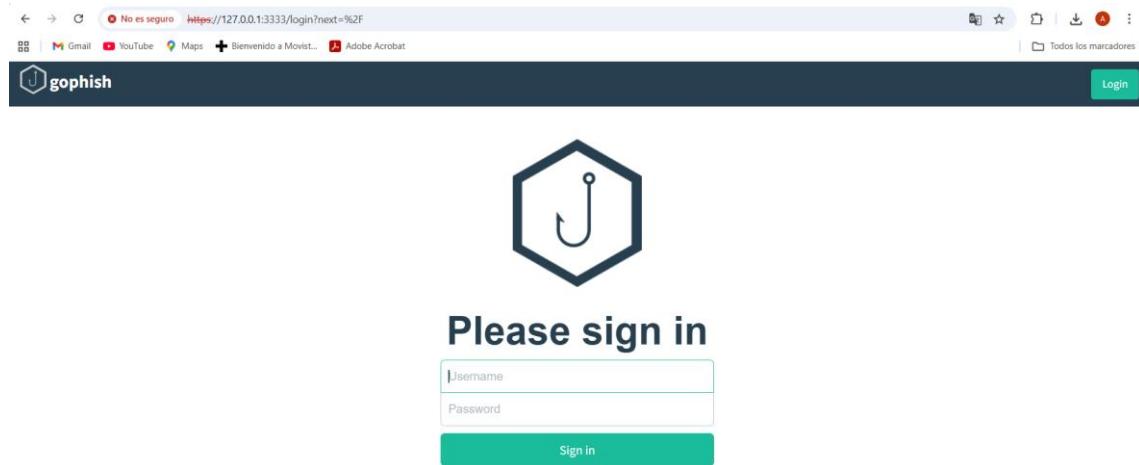
HTTP Requests
-----
10:39:02.877 CEST POST /                         302 Found
10:38:43.318 CEST GET /                          200 OK
10:38:43.121 CEST GET /                          200 OK

```

### 3. Acceder a Gophish

Accedemos a la interfaz web de Gophis poniendo en nuestro navegador la URL:

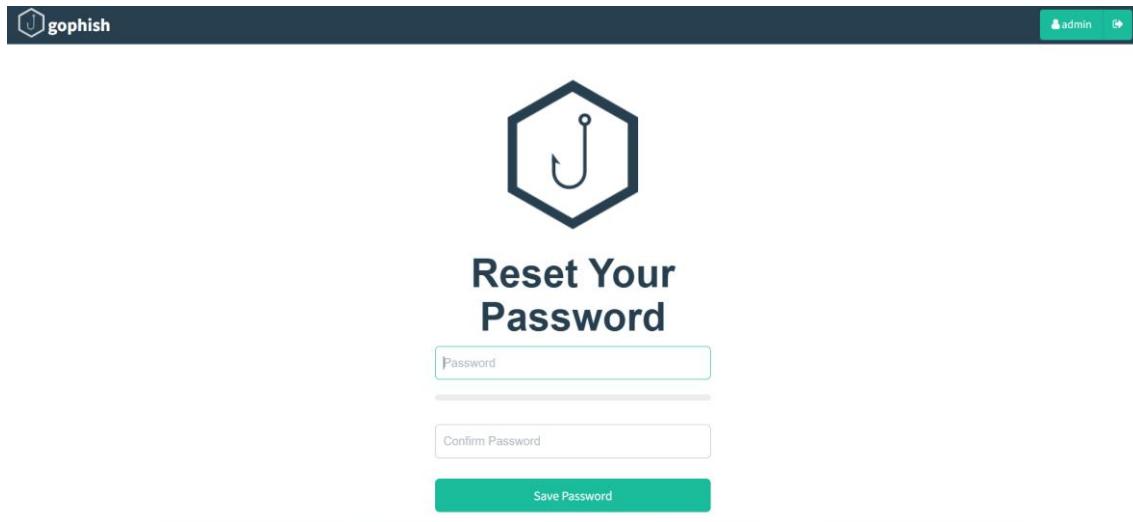
<https://127.0.0.1:3333>.



Para poder acceder pondremos de usuario ‘**admin**’ y la contraseña nos la generara la cmd:

```
time="2025-10-23T09:52:55+02:00" level=info msg="Please login with the username admin and the password 10eb3bd9f88aad2c"  
time="2025-10-23T09:52:55+02:00" level=info msg="Starting IMAP monitor manager"  
time="2025-10-23T09:52:55+02:00" level=info msg="Starting phishing server at http://0.0.0.0:80"  
time="2025-10-23T09:52:55+02:00" level=info msg="Creating new self-signed certificates for administration interface"  
time="2025-10-23T09:52:55+02:00" level=info msg="Background Worker Started Successfully - Waiting for Campaigns"  
time="2025-10-23T09:52:55+02:00" level=info msg="Starting new IMAP monitor for user admin"  
time="2025-10-23T09:52:55+02:00" level=info msg="TLS Certificate Generation complete"  
time="2025-10-23T09:52:55+02:00" level=info msg="Starting admin server at https://127.0.0.1:3333"  
2025/10/23 10:01:41 http: TLS handshake error from 127.0.0.1:52226: remote error: tls: unknown certificate  
2025/10/23 10:01:41 http: TLS handshake error from 127.0.0.1:50007: remote error: tls: unknown certificate  
2025/10/23 10:01:41 http: TLS handshake error from 127.0.0.1:58101: remote error: tls: unknown certificate  
2025/10/23 10:01:41 http: TLS handshake error from 127.0.0.1:50787: remote error: tls: unknown certificate  
time="2025-10-23T10:01:49+02:00" level=info msg="127.0.0.1 - - [23/Oct/2025:10:01:49 +0200] \"GET / HTTP/2.0\" 307 51 \"\\" \"Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/141.0.0.0 Safari/537.36\"\\""  
time="2025-10-23T10:01:49+02:00" level=info msg="127.0.0.1 - - [23/Oct/2025:10:01:49 +0200] \"GET /Login?next=%2F HTTP/2.0\" 200 1038 \"\\" \"Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/141.0.0.0 Safari/537.36\"\\""  
time="2025-10-23T10:01:49+02:00" level=info msg="127.0.0.1 - - [23/Oct/2025:10:01:49 +0200] \"GET /images/logo_inv_small.png HTTP/2.0\" 200 1118 \"https://127.0.0.1:3333/Login?next=%2F\" \"Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/141.0.0.0 Safari/537.36\"\\""  
time="2025-10-23T10:01:49+02:00" level=info msg="127.0.0.1 - - [23/Oct/2025:10:01:49 +0200] \"GET /images/logo_purple.png HTTP/2.0\" 200 4735 \"https://127.0.0.1:3333/Login?next=%2F\" \"Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/141.0.0.0 Safari/537.36\"\\""  
time="2025-10-23T10:01:49+02:00" level=info msg="127.0.0.1 - - [23/Oct/2025:10:01:49 +0200] \"GET /css/dist/gophish.css HTTP/2.0\" 200 52514 \"https://127.0.0.1:3333/Login?next=%2F\" \"Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/141.0.0.0 Safari/537.36\"\\""  
time="2025-10-23T10:01:49+02:00" level=info msg="127.0.0.1 - - [23/Oct/2025:10:01:49 +0200] \"GET /js/dist/vendor.min.js HTTP/2.0\" 200 324943 \"https://127.0.0.1:3333/Login?next=%2F\" \"Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/141.0.0.0 Safari/537.36\"\\""  
time="2025-10-23T10:01:50+02:00" level=info msg="127.0.0.1 - - [23/Oct/2025:10:01:50 +0200] \"GET /images/favicon.ico HTTP/2.0\" 200 1150 \"https://127.0.0.1:3333/Login?next=%2F\" \"Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/141.0.0.0 Safari/537.36\"\\""
```

Una vez puesta la contraseña nos pedirá que la cambiamos.



En el archivo **config.json** cambiamos la ip 127.0.0.1 por la IP local del servidor que contendrá GolPhish y guardamos los cambios.

config.json

```

1  {
2      "admin_server": {
3          "listen_url": "192.168.1.16:3333",
4          "use_tls": true,
5          "cert_path": "gophish_admin.crt",
6          "key_path": "gophish_admin.key",
7          "trusted_origins": []
8      },
9      "phish_server": {
10         "listen_url": "192.168.1.16:80",
11         "use_tls": false,
12         "cert_path": "example.crt",
13         "key_path": "example.key"
14     },
15     "db_name": "sqlite3",
16     "db_path": "gophish.db",
17     "migrations_prefix": "db/db_",
18     "contact_address": "",
19     "logging": {
20         "filename": "",
21         "level": ""
22     }
23 }
24

```

## 4. Campaña de envío de correos

Accedemos a la parte de **Sending Profiles** y clicamos en **New Profile**.

The screenshot shows the Gophish application's main dashboard. On the left, there is a sidebar with various navigation options: Dashboard, Campaigns, Users & Groups, Email Templates, Landing Pages, Sending Profiles (which is currently selected and highlighted in dark blue), Account Settings, User Management, Webhooks, User Guide, and API Documentation. The main content area has a title 'Sending Profiles' and a sub-header 'No profiles created yet. Let's create one!'. Below this, there is a green button labeled '+ New Profile' with a white plus sign. The entire interface has a clean, modern design with a light gray background and dark blue header elements.

Se nos abrirá esta ventana y rellenaremos los datos, una vez hecho esto le daremos a **Send Test Email** para comprobar que la configuración funciona.

Name:

Interface Type:

SMTP From: ?

Host:

Username:

Password:

Ignore Certificate Errors ?

Email Headers:

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

+ Add Custom Header

Show  entries

Search:

Header	Value
No data available in table	

Showing 0 to 0 of 0 entries

## Default Email from Gophish

Recibidos x



adrianalonsoridao@gmail.com

para mí ▾

It works!

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

Here are the details:

Who you sent from: [adrianalonsoridao@gmail.com](mailto:adrianalonsoridao@gmail.com)

Who you sent to:

First Name: Adrián

Last Name: Alonso Ridao

Now go send some phish!



Cambie el nombre a ‘Pruebas’ antes de clicar y se quedó creado con ese nombre:

Name	Interface Type	Last Modified Date
Pruebas	SMTP	October 23rd 2025, 5:23:48 pm

Después de crear y comprobar nuestro perfil nos vamos a **Landing Pages** y creamos nuestra copia de la web que queremos usar, en este caso será Facebook:

The screenshot shows the gophish web application interface. On the left, there is a sidebar with the following navigation options: Dashboard, Campaigns, Users & Groups, Email Templates, Landing Pages (which is currently selected and highlighted in dark blue), Sending Profiles, Account Settings, User Management, and Webhooks. Each option has an 'Admin' badge next to it. At the top right, there is a user icon labeled 'admin'. In the main content area, the title 'Landing Pages' is displayed. Below the title is a green button with the text '+ New Page'. Underneath the button, a light blue banner displays the message 'No pages created yet. Let's create one!'. The overall layout is clean and modern.

Se nos abrirá una ventana nueva y clicamos en **Import Site**

This screenshot shows the 'New Landing Page' creation dialog. At the top, the title 'New Landing Page' is displayed. Below it, there is a 'Page name' input field. A red circle highlights the 'Import Site' button, which is located below the input field. The dialog also contains a rich text editor toolbar with various icons for text formatting, tables, and images. A large text area for the page content is present but currently empty. At the bottom of the dialog, there is a checkbox labeled 'Capture Submitted Data' with a question mark icon. Finally, at the very bottom, there are two buttons: 'Cancel' and 'Save Page', with 'Save Page' being the primary action button.

Pegamos la URL de Facebook, activamos las casillas **Capture Submitted Data** y **Capture Password** y damos a **Save Page**.

Name:

Facebook

 Import Site

HTML



B I S | Tx : | ; : | , , | Styles Format

# facebook

Facebook te ayuda a comunicarte y  
compartir con las personas que  
forman parte de tu vida.

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!

Redirect to: 

http://example.com

 Cancel

 Save Page

+ New Page	
Show <input type="text" value="10"/>	entries
Name	Last Modified Date
Facebook October 23rd 2025, 6:18:38 pm	
Showing 1 to 1 of 1 entries	
Search: <input type="text"/>	
  	
Previous <input type="button" value="1"/> Next	

Pasamos a la pestaña **Email Templates**, aquí crearemos el correo que enviaremos a nuestros usuarios.

## Edit Template

Name:

Invitación Facebook

 Import Email

Envelope Sender: 

First Last <test@example.com>

Subject:

Acceso cuenta



### Solo un paso más para confirmar esta dirección de correo electrónico

Hola, Manuel:

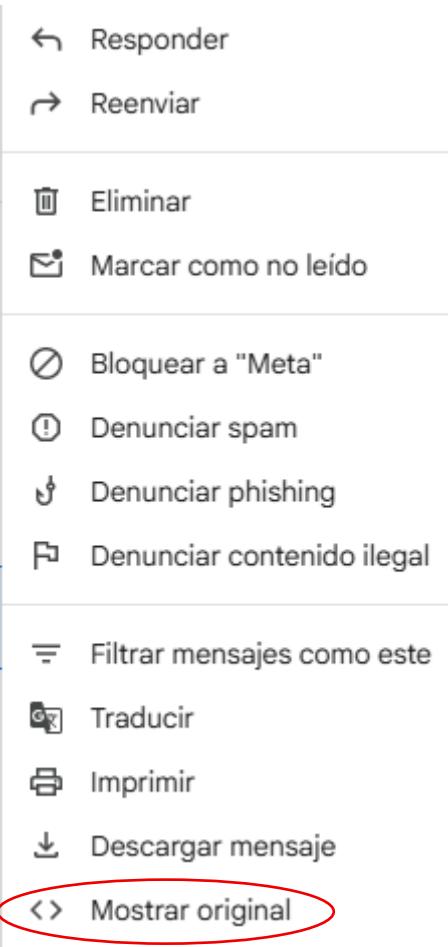
Para poder acceder a su verificación de cuenta acceda con su usuario y contraseña.

```
body table tbody tr td table tbody tr td table tbody tr td p
```

Add Tracking Image

 + Add Files

Copiamos el código fuente de un correo de Facebook pinchando en Mostrar Original.



## Import Email

Email Content:

```
=3D""><td height=3D"10" style=3D"line-height:10px;">&nbsp;</td></tr></td><=tr></td><td width=3D"15" style=3D"display:block;width:15px;">&nbsp;=&nbsp;&nbsp;</td></tr><tr style=3D""><td height=3D"20" style=3D"line-height=20px;" colspan=3D"3">&nbsp;</td></tr></table><span style=3D""><img src=3D"https://www.facebook.com/email_open_log_pic.php?mid=3D641d5ad392accG63bf00bdG641d5f6cf2d9eG142" style=3D"border:0;width:1px;height:1px;" /></span></td></tr></table></body></html>

--b1_2f40180faf0fdbba62451e566d066d2aa--
```

Change Links to Point to Landing Page

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.

The screenshot shows a rich-text editor interface with two tabs at the top: "Text" (selected) and "HTML". Below the tabs is a toolbar with various icons for text formatting, tables, and images. The main content area contains the following text:

**Solo un paso más para confirmar esta dirección de correo electrónico**

Hola, Manuel:

Hemos recibido tu solicitud para añadir esta dirección de correo electrónico a tu cuenta.

Below the text, the HTML source code is visible:

```
body table tbody tr td table tbody tr td table tbody tr td p
```

At the bottom left, there is a checked checkbox labeled "Add Tracking Image".

Seleccionamos una palabra del mensaje y creamos un hipervínculo que nos lleve a nuestra página de Facebook falsa, rellenamos con esta información para ello:

A modal dialog box titled "Link" is open over the email editor. It contains the following fields:

- Display Text:** "aqui"
- Protocol:** "http://"
- URL:** "{{.URL}}

At the bottom right of the dialog are "OK" and "Cancel" buttons. In the background, the email editor shows a placeholder text: "Para continuar, ingrese su usuario y contraseña [aqui](#)".

The screenshot shows a table with one row of data. The columns are 'Name' and 'Modified Date'. The 'Name' column contains 'Invitación Facebook' and the 'Modified Date' column contains 'October 23rd 2025, 6:40:31 pm'. At the top right, there are three small icons: a pencil, a magnifying glass, and a trash can. Below the table, it says 'Showing 1 to 1 of 1 entries' and has navigation buttons for 'Previous', '1', and 'Next'.

Ahora procedemos a enviar nuestro falso correo a los destinatarios que queramos. Vamos a la pestaña **User & Groups** y añadimos un nuevo grupo.

En este caso solo será un usuario así que pondremos su correo electrónico:

The screenshot shows a form for creating a new group. The title is 'New Group'. The 'Name' field contains 'Facebook grupo'. Below the name, there are four input fields: 'First Name', 'Last Name', 'Email', and 'Position'. To the right of these fields is a red button with a plus sign and the text '+Add'. Above the input fields are two buttons: a red one labeled '+ Bulk Import Users' and a grey one labeled 'Download CSV Template'. At the bottom, there are search and pagination controls: 'Show 10 entries', 'Search:', 'Showing 1 to 1 of 1 entries', 'Previous', '1', and 'Next'. At the very bottom are two buttons: 'Close' and a green 'Save changes' button.

## 5. Lanzamiento de la campaña de phishing

Para lanzar nuestra campaña nos vamos a la pestaña **Campaigns** y creamos una nueva campaña.

Seleccionamos nuestro grupo de Facebook creado anteriormente y ponemos en **URL** la url que nos generó anteriormente Ngrok.

```
Simbolo del sistema - ngrok | X + v - □ ×
ngrok
♦ Block threats before they reach your services with new WAF actions → https://ngrok.com/r/waf
Session Status      online
Account            adrianalonsoridao@gmail.com (Plan: Free)
Version             3.24.0-msix
Region              Europe (eu)
Latency             33ms
Web Interface      http://127.0.0.1:4040
Forwarding          https://semirhythrical-undevastatingly-rosamond.ngrok-free.dev → http://172.16.115.58:808
Connections         ttl     opn      rt1      rt5      p50      p90
                    3       0       0.00    0.00    10.04   10.08
HTTP Requests
-----
10:39:02.877 CEST POST /           302 Found
10:38:43.318 CEST GET /          200 OK
10:38:43.121 CEST GET /          200 OK
```

# New Campaign

X

Name:

Campaña Invitación Facebook

Email Template:

Invitación Facebook

Landing Page:

Facebook

URL: 

<https://semirhythmical-undevastatingly-rosamond.ngrok-free.dev>

Launch Date

Send Emails By (Optional) 

October 24th 2025, 10:43 am

Sending Profile:

Pruebas

 Send Test Email

Groups:

\* Facebook grupo |

Facebook grupo

 Close

 Launch Campaign

Una vez enviado el correo, nuestro compañero podrá ver el correo electrónico de esta manera:



**Solo un paso más para confirmar esta dirección de correo electrónico**

Hola, Adrián:

Hemos recibido tu solicitud para añadir esta dirección de correo electrónico a tu cuenta.

Para continuar inicia sesión en facebook [aquí](#).

**¿No has pedido esto?**

Si recibes este correo electrónico, pero no has intentado confirmar tu dirección de correo electrónico, es posible que alguien esté intentando hackear tu cuenta. Mientras no compartas este código con nadie, no es necesario que tomes ninguna otra medida. Si quieres que tu cuenta sea más segura, ve a [Security Checkup](#).

Gracias,  
Seguridad de Meta

¿No sabes si este correo electrónico es realmente nuestro? Visita el Servicio de ayuda para confirmarlo: [www.facebook.com/help/check-email](http://www.facebook.com/help/check-email)

from  
 Meta

© Facebook, Meta Platforms Ireland Limited, Merrion Road, Dublin 4, D04 X2K5, Ireland

Nuestros resultados de la campaña se quedarán reflejados en gophish:

The dashboard shows the following metrics:

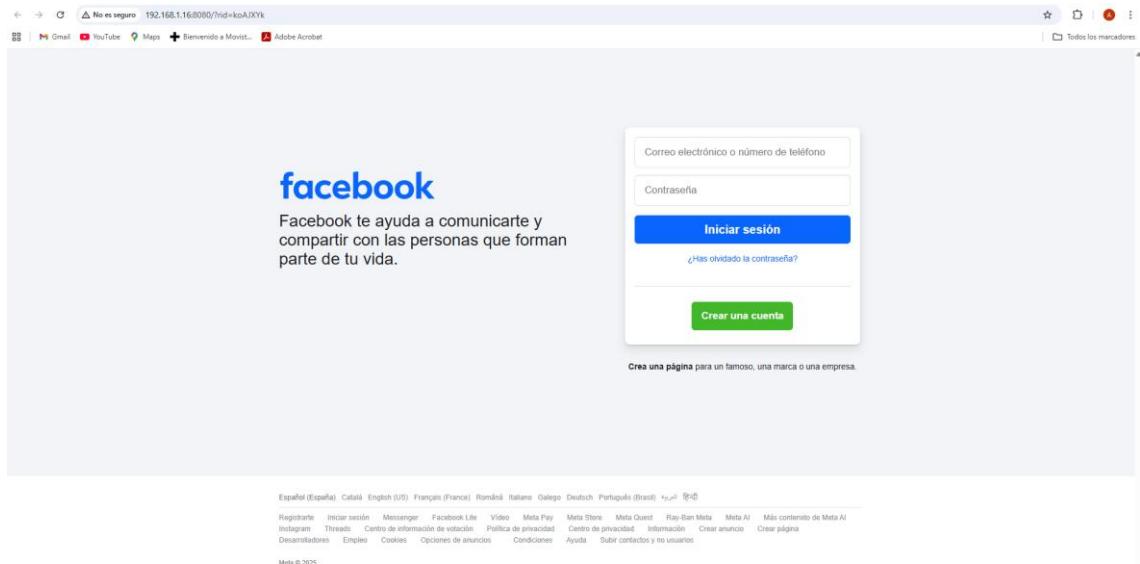
- Email Sent: 2
- Email Opened: 2
- Clicked Link: 2
- Submitted Data: 1
- Email Reported: 0

**Details**

First Name	Last Name	Email	Position	Status	Reported
Adrián	Alonso Ridaó	adrianalonsoridao@gmail.com		Clicked Link	
Manuel		mzdelcerro@gmail.com		Submitted Data	

Showing 1 to 2 of 2 entries

Al clicar en cualquier enlace del correo electrónico saldrá esta ventana:



Si exportamos el archivo CSV de los Eventos nos saldrá un archivo con los eventos realizados en nuestra campaña, como podemos ver se puede ver perfectamente el nombre de usuario pero la contraseña viene encriptada:

The interface includes buttons for Back, Export CSV, Completed!, Delete, and Refresh. A modal window titled "Results" shows two items: "Raw Events".

```

afari/537.36"""}"
,""email"":[""mzdelcerro@gmail.com""],""encpass"":[""next"""],""email"":[""hola"""],""encpass"":[""#PWD_BRO

```

Que la contraseña salga encriptada depende de la página web que usamos, he hecho un segundo intento con GLS y se ve perfectamente la contraseña.

```
eturnUrl=%2F""], ""password"": [""123455678""], ""rid"": [""FemGwEM""
```

## 6. Conclusiones

### 6.1. Lecciones aprendidas sobre técnicas de ingeniería social.

Durante la realización de la práctica se ha podido comprobar que las técnicas de ingeniería social continúan siendo uno de los vectores de ataque más eficaces dentro del ámbito de la ciberseguridad. El éxito de una campaña de phishing no depende exclusivamente de la complejidad técnica, sino de la capacidad del atacante para generar confianza y urgencia en la víctima.

El uso de herramientas como Gophish ha permitido simular campañas realistas, observando cómo el diseño visual, la elección del remitente y la redacción del mensaje influyen de manera directa en la tasa de interacción de los usuarios. Asimismo, la utilización de Ngrok ha facilitado la exposición controlada de servidores locales, demostrando que con recursos limitados es posible recrear un escenario de phishing funcional.

Entre las lecciones más relevantes se destacan:

- **La importancia de la apariencia de legitimidad** (logos, dominios y lenguaje corporativo) para inducir confianza en el destinatario.
- **La vulnerabilidad del factor humano**, que sigue siendo el eslabón más débil de la cadena de seguridad.
- La necesidad de **educar y sensibilizar** a los usuarios frente a correos o enlaces sospechosos, dado que las medidas técnicas por sí solas no resultan suficientes.
- **El riesgo asociado a la exposición de servicios locales** mediante túneles o plataformas externas, lo que pone de manifiesto la relevancia de aplicar políticas de control de acceso y registro de actividad.

## 6.2. Medidas de mitigación recomendadas para la organización simulada.

A partir del análisis realizado, se proponen las siguientes estrategias de mitigación orientadas a una organización hipotética:

1. **Formación continua en ciberseguridad:** Implementar programas periódicos de capacitación sobre reconocimiento de intentos de phishing, verificación de URLs y protocolos de reporte de incidentes.
2. **Autenticación multifactor (MFA):** Incorporar este mecanismo para mitigar el impacto de posibles compromisos de credenciales.
3. **Políticas de seguridad del correo electrónico:** Configurar correctamente los registros SPF, DKIM y DMARC, y utilizar filtros antiphishing y antimalware en los servidores de correo.
4. **Gestión segura de contraseñas:** Promover el uso de gestores de contraseñas y la creación de claves robustas, evitando su reutilización entre diferentes servicios.
5. **Monitorización y respuesta ante incidentes:** Establecer procedimientos de detección temprana y protocolos de respuesta que incluyan la suspensión de cuentas comprometidas y la notificación oportuna a los usuarios.
6. **Evaluaciones periódicas de seguridad:** Realizar simulaciones controladas de phishing y auditorías internas que permitan medir el nivel de resiliencia de la organización frente a este tipo de ataques.

## 7. Aspectos éticos

La práctica se desarrolló exclusivamente en un entorno controlado, con fines académicos y de aprendizaje, sin afectar a sistemas, datos o usuarios reales. Todas las simulaciones se realizaron sobre cuentas y servidores de prueba, con autorización implícita dentro del marco educativo del ejercicio.

Se hace constar de forma expresa que no se ha llevado a cabo ninguna actividad ilícita, ni se han vulnerado sistemas externos o políticas de privacidad ajenas. Los datos recopilados durante la práctica se utilizaron únicamente con fines demostrativos y fueron eliminados al finalizar el ejercicio.