

Laboratorio 01

Plataforma para
ataques de
ingeniería social

Ing. Alex Araya Rojas, MT

CISSP, CISM

Agosto 2022

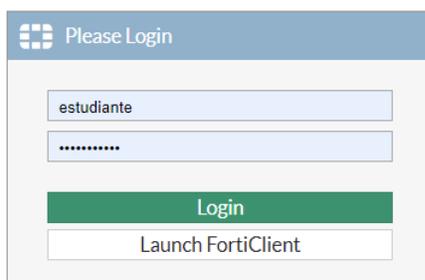
Lab 01

Plataforma para ataques de ingeniería social

Procedimiento

Preparación

01. Esta herramienta es compatible tanto para Windows, Linux como MacOS, puede ejecutar el laboratorio en cualquiera de esas plataformas.
02. Se ha preparado una máquina en el laboratorio para cada estudiante, para el ejercicio, utilizaremos una virtual con Ubuntu instalado, a la cual usted accederá vía RDP.
03. Ingrese al sitio web <https://vpn.araya.vip:10443> las credenciales para su acceso son “estudiante” con la contraseña “ CIFTen2022! “ Esta es una VPN vía SSL por lo que **no** debe instalar ningún cliente en su equipo ya que el acceso será vía un navegador de internet a los equipos asignados, solo ingrese las credenciales y presione el botón Login.

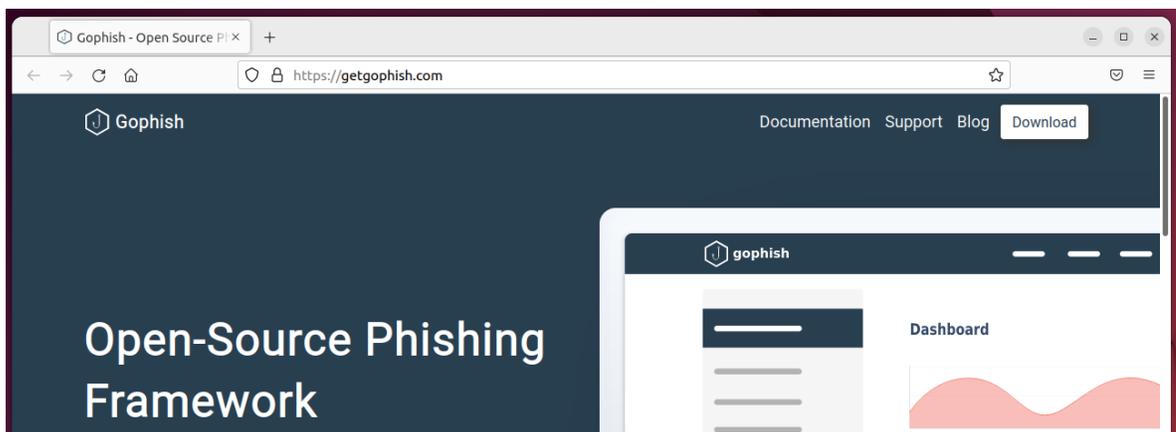


04. Una vez que haya ingresado, verá varios íconos con un número de estudiante, ingrese al que le fue proporcionado para el laboratorio.



05. Valide el acceso a su equipo, no debe continuar hasta que tenga visión acceso a su equipo.

06. Es necesario que este equipo sea visible desde la Internet, por ejemplo, puede utilizar una máquina virtual en Azure o en su red empresarial y publicar el servicio en una DMZ. Nosotros lo instalaremos en una máquina virtual local y utilizaremos direcciones de la LAN para efectos del laboratorio.
07. Ahora es el turno de la herramienta GoPhish, que habilitará el framework para poder hacer nuestros ataques de phishing, puede descargarlo de este url: <https://getgophish.com/> la última versión liberada al realizar esta guía era la v0.12.0, nosotros utilizaremos la versión para Linux que más adelante instalaremos. Si abre el Firefox en su equipo Ubuntu deberá llevarlo directo a ese sitio web.



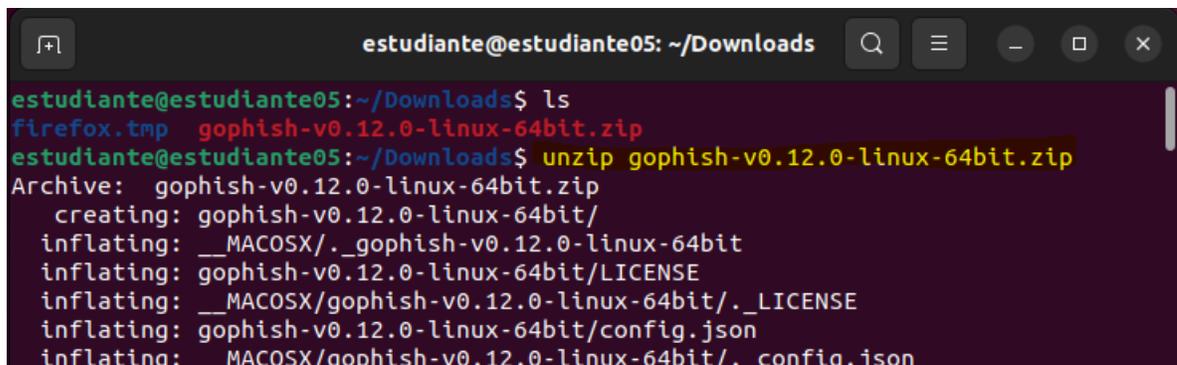
08. Es necesario utilizar una cuenta de correos para el envío del ataque de phishing, para efectos de practicidad, se le está compartiendo una cuenta de correo estudiante@araya.vip con las credenciales “ CIFTen2022! ” más adelante veremos el proceso de configuración.

Proceso de instalación

01. Descargue el archivo para su plataforma de software que funcione para el que será su servidor de Phishing. <https://github.com/gophish/gophish/releases>, para efectos de este lab, los vamos a instalar en un equipo con Ubuntu, por lo que debe descargar la primera opción.

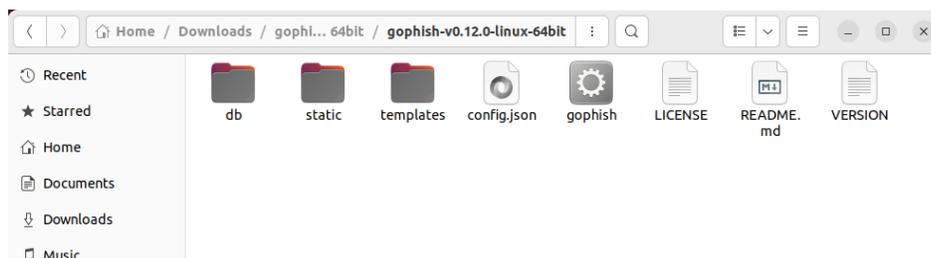
 gophish-v0.12.0-linux-64bit.zip	31.8 MB
 gophish-v0.12.0-osx-64bit.zip	33.6 MB
 gophish-v0.12.0-windows-64bit.zip	32.4 MB
 Source code (zip)	
 Source code (tar.gz)	

02. Una vez descargado el archivo zip, toca el turno de descomprimirlo, la forma fácil sería ubicar el archivo en la carpeta DOWNLOADS, clic derecho y EXTRACT HERE. Si lo quiere hacer vía comando, a continuación, se muestra una captura de pantalla que lo logra.

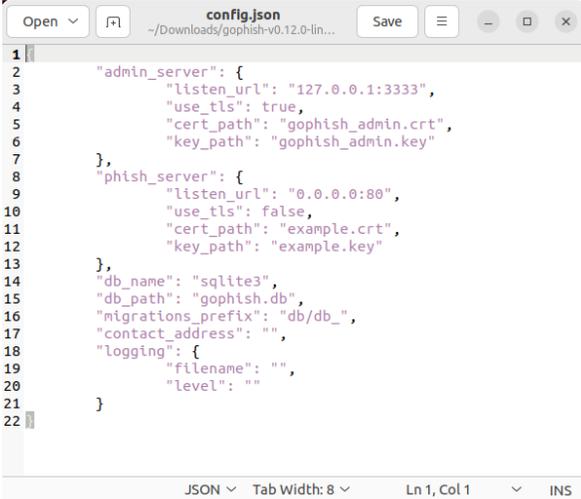


```
estudiante@estudiante05: ~/Downloads
estudiante@estudiante05:~/Downloads$ ls
firefox.tmp  gophish-v0.12.0-linux-64bit.zip
estudiante@estudiante05:~/Downloads$ unzip gophish-v0.12.0-linux-64bit.zip
Archive:  gophish-v0.12.0-linux-64bit.zip
  creating: gophish-v0.12.0-linux-64bit/
  inflating: __MACOSX/.gophish-v0.12.0-linux-64bit
  inflating: gophish-v0.12.0-linux-64bit/LICENSE
  inflating: __MACOSX/gophish-v0.12.0-linux-64bit/._LICENSE
  inflating: gophish-v0.12.0-linux-64bit/config.json
  inflating: __MACOSX/gophish-v0.12.0-linux-64bit/._config.json
```

03. Una vez que se haya ejecutado el proceso para su descompresión, ubique la carpeta y dentro de la estructura, abra con su editor de texto favorito el archivo config.json



04. En la siguiente imagen, se aprecia el config.json abierto con el editor de texto de Ubuntu.



```
1 |
2   "admin_server": {
3     "listen_url": "127.0.0.1:3333",
4     "use_tls": true,
5     "cert_path": "gophish_admin.crt",
6     "key_path": "gophish_admin.key"
7   },
8   "phish_server": {
9     "listen_url": "0.0.0.0:80",
10    "use_tls": false,
11    "cert_path": "example.crt",
12    "key_path": "example.key"
13  },
14  "db_name": "sqlite3",
15  "db_path": "gophish.db",
16  "migrations_prefix": "db/db_",
17  "contact_address": "",
18  "logging": {
19    "filename": "",
20    "level": ""
21  }
22 |
```

05. El apartado de admin_server le permite configurar la forma en que se gestiona el servidor de gophish.

06. El apartado de phish_server, le permite definir los parámetros del servidor que almacenará las páginas web de phishing.

07. Se pueden agregar más secciones, por ejemplo, la configuración smtp, pero para efectos de este lab no serán necesarios.

08. Reemplace el listen_url del admin_server, con este cambio, ya podrá conectarse al servidor por ese puerto desde otros equipos vía la IP que tenga asignado físicamente el servidor. Si el certificado le da problemas, cambie a false la opción "use_tls"

```
"admin_server": {
  "listen_url": "0.0.0.0:3333",
  "use_tls": true,
  "cert_path": "gophish_admin.crt",
  "key_path": "gophish_admin.key"
}
```

09. Si está corriendo esta máquina en su proveedor de nube, deberá habilitar los permisos en su firewall correspondiente.

10. Ejecute el archivo gophish.exe (Windows) o en nuestro caso, abra una terminal en la carpeta donde están los archivos de gophish y ejecute el comando:

```
estudiante@estudiante05: ~/Downloads/gophish-v0.12.0-linux-64bit
estudiante@estudiante05:~/Downloads/gophish-v0.12.0-linux-64bit$ ls
config.json  gophish_admin.crt  LICENSE  templates
db           gophish_admin.key  README.md  VERSION
estudiante@estudiante05:~/Downloads/gophish-v0.12.0-linux-64bit$ sudo ./gophish
```

11. En la consola, al tratarse de la primera vez que se ejecuta el GoPhish, debe estar atento ya que aparece la contraseña aleatoria asignada.

```
Seleccionar C:\Users\alex\Desktop\gophish-v0.11.0-windows-64bit\gophish.exe
eOK 20160217211342_0.1.2_create_from_col_results.sql
cOK 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 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
OK 20190105192341_0.8.0_rbac.sql
OK 20191104103306_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
time="2021-08-31T23:35:40-06:00" level=info msg="Please login with the username admin and the password ca899cf8b23a31ba"
time="2021-08-31T23:35:40-06:00" level=info msg="Starting phishing server at http://0.0.0.0:80"
time="2021-08-31T23:35:40-06:00" level=info msg="Starting IMAP monitor manager"
time="2021-08-31T23:35:40-06:00" level=info msg="Background Worker Started Successfully - Waiting for Campaigns"
time="2021-08-31T23:35:40-06:00" level=info msg="Creating new self-signed certificates for administration interface"
time="2021-08-31T23:35:40-06:00" level=info msg="Starting new IMAP monitor for user admin"
time="2021-08-31T23:35:40-06:00" level=info msg="TLS Certificate Generation complete"
time="2021-08-31T23:35:40-06:00" level=info msg="Starting admin server at https://0.0.0.0:3333"
```

```
estudiante@estudiante05: ~/Downloads/gophish-v0.12.0-linux-64bit
estudiante@estudiante05:~/Downloads/gophish-v0.12.0-linux-64bit$ sudo ./gophish
time="2022-08-20T10:11:03-06:00" level=warning msg="No contact address has been configured."
time="2022-08-20T10:11:03-06:00" level=warning msg="Please consider adding a contact_address entry in your config.json"
goose: no migrations to run. current version: 20220321133237
time="2022-08-20T10:11:03-06:00" level=info msg="Please login with the username admin and the password c9cd5abeca3009b9"
time="2022-08-20T10:11:03-06:00" level=info msg="Starting IMAP monitor manager"
time="2022-08-20T10:11:03-06:00" level=info msg="Starting new IMAP monitor for user admin"
time="2022-08-20T10:11:03-06:00" level=info msg="Starting admin server at https://0.0.0.0:3333"
time="2022-08-20T10:11:03-06:00" level=info msg="Starting phishing server at http://0.0.0.0:80"
time="2022-08-20T10:11:03-06:00" level=info msg="Background Worker Started Successfully - Waiting for Campaigns"
```

12. Ingrese a la consola de administración del GoPhish y deberá ver la página de inicio de sesión.



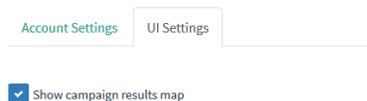
13. La primera vez que ingrese deberá cambiar el password de la consola de administración, como recomendación, utilice CIFTen2022!



The image shows a 'Reset Your Password' form. At the top is a logo consisting of a hexagon with an anchor inside. Below the logo, the text 'Reset Your Password' is displayed in a bold, dark font. The form contains two password input fields, each with a green underline. The first field is empty, and the second field has a green underline and the text 'Very Good' above it. A green button labeled 'Save Password' is positioned at the bottom of the form.

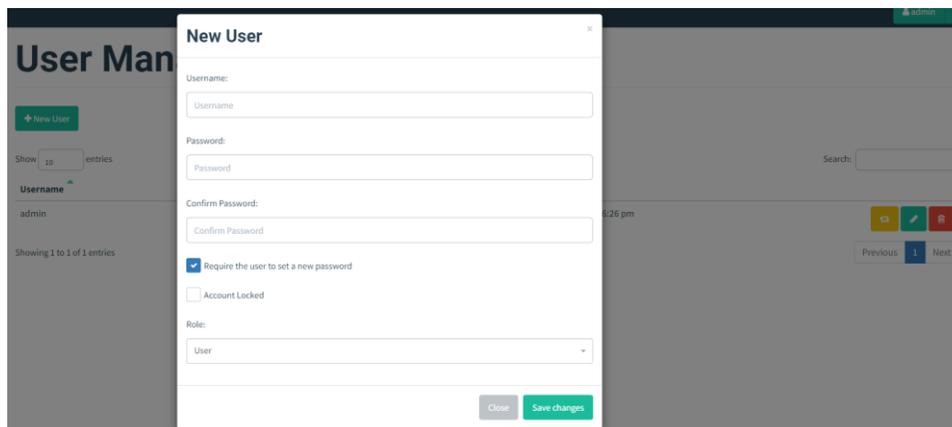
14. Marque la opción del mapa en Account Settings, esto le permitirá tener una visualización gráfica de la apertura de nuestros correos.

Settings



The image shows the 'Settings' page. At the top, there are two tabs: 'Account Settings' and 'UI Settings'. Below the tabs, there is a checkbox labeled 'Show campaign results map' which is checked.

15. En la opción de User Management, podrá crear otros administradores y usuarios con privilegio, esto en caso de ser necesario brindar acceso a terceros para seguimiento.



The image shows the 'User Management' interface. A modal window titled 'New User' is open, allowing the creation of a new user. The form includes fields for 'Username', 'Password', and 'Confirm Password'. There are also checkboxes for 'Require the user to set a new password' (checked) and 'Account Locked'. A 'Role' dropdown menu is set to 'User'. At the bottom of the modal, there are 'Close' and 'Save changes' buttons. The background shows the 'User Management' page with a table of users, including one named 'admin'.

16. Debe ahora crear un sending profile para enviar los correos utilizando su cuenta de correo creamos para este ejercicio. Complete los campos para utilizar según los valores suministrados.

Name:

Interface Type:

SMTP From: ⓘ

Host:

Username:

Password:

Ignore Certificate Errors ⓘ

17. Si desea agregar encabezados al correo para que alguna aplicación los pueda marcar, esta es la sección para hacerlo.

Ignore Certificate Errors ⓘ

Email Headers:

Show entries Search:

Header	Value
No data available in table	

Showing 0 to 0 of 0 entries

18. Puede probar la configuración del envío de correos con el botón correspondiente, no avance si esto no funciona. No olvide guardar el profile!!

Send Test Email ×

Email Sent!

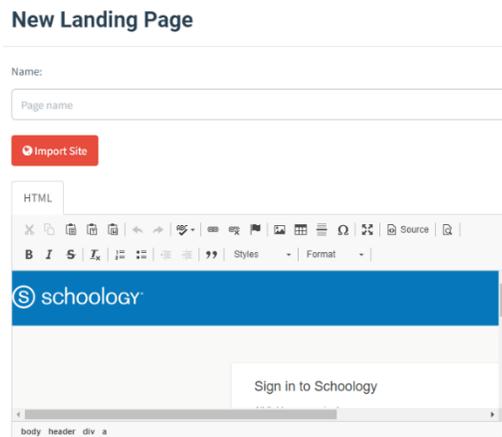
Send Test Email to:

19. El landing page es donde irán nuestras víctimas cuando hagan click en nuestro link malicioso. Puede importarla y la herramienta clonará el sitio por usted.

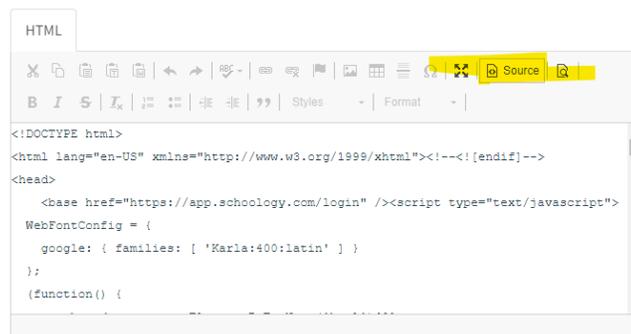
20. Elija bien el sitio, debe contener el campo de username y password para que el ejercicio funcione. Sino tiene una página, puede utilizar <https://app.schoology.com/login>



21. Ahora puede ver el contenido de la página y hacer modificaciones, le recomiendo que elimine todo el código tipo script del sitio clonado y haga pruebas hasta que la captura de la contraseña funcione y la apariencia de la página sea la apropiada.



22. Utilice la opción de ver el código para ayudarse en la depuración de la página.



23. Si desea guardar las credenciales de las víctimas, deberá marcar estas casillas, así como la opción de redirigir a la víctima al sitio real.

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: [?](#)

https://app.schoolology.com/login

24. El template de email es la estructura de correo que será enviada a las víctimas.

25. Puede obtener un correo real y clonarlo o podrá armarlo usted mismo, tal y como verá en las siguientes filminas.

New Template x

Name:

Template name

✉ Import Email

Subject:

Email Subject

26. Debe agregar imágenes al correo que le hagan pensar a la víctima que es un correo real, una firma, una invitación, etc.

27. Sea creativo, el correo es la pieza clave para el engaño!!!!

Add Tracking Image

+ Add Files

Show entries Search:

Name ▲

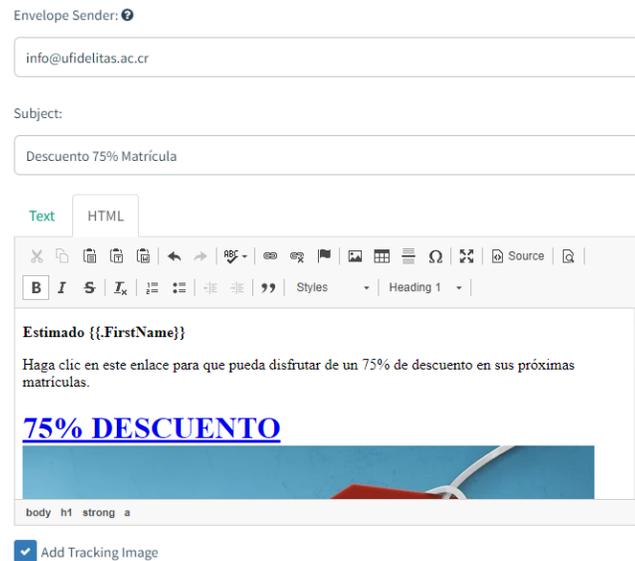
No data available in table

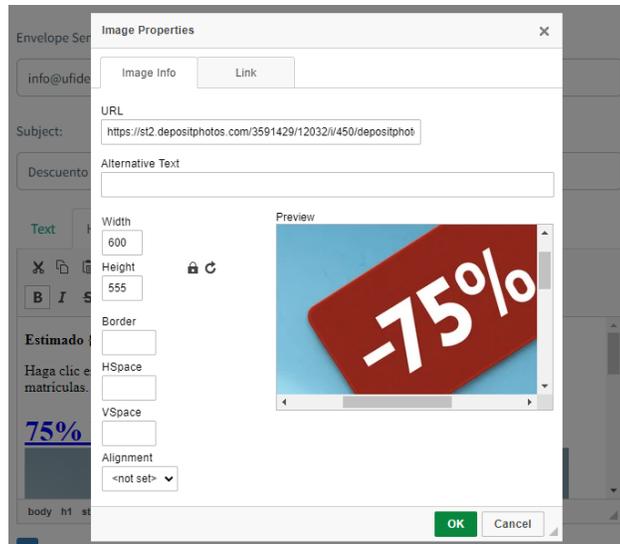
Showing 0 to 0 of 0 entries

28. Utilice imágenes representativas para la empresa.

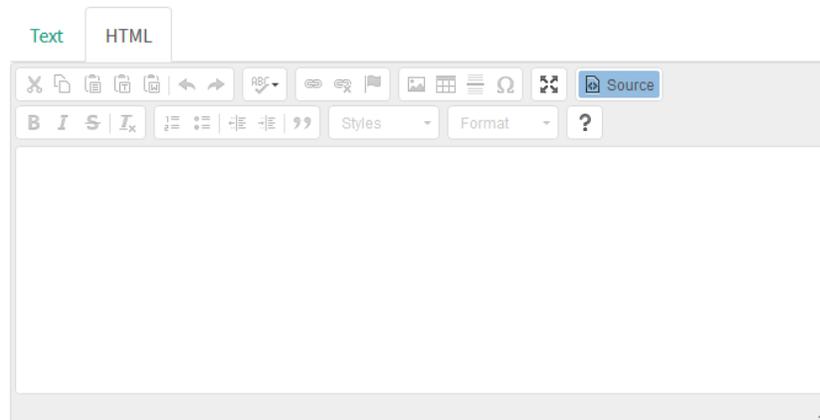
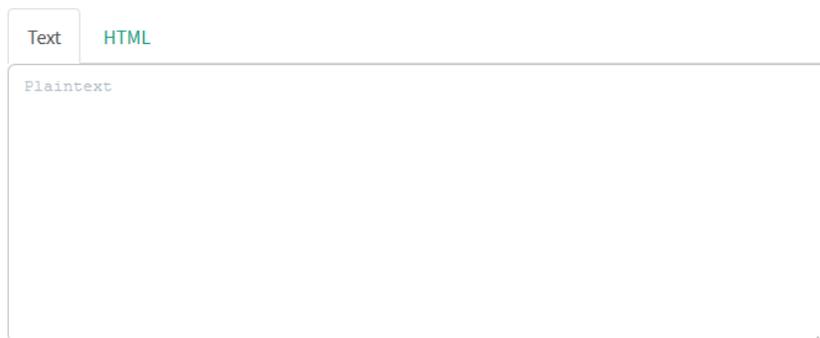


29. Aquí podrá modificar el cuerpo del correo electrónico, puede incluir las variables `{{.XXX}}` para que sea más personalizado. Para incluir el link, la variable que debe utilizar es `{{.URL}}` que hará referencia al url de la campaña.
30. Se adjunta una configuración de referencia:





31. Haga pruebas hasta que sea convincente.



32. Definamos ahora en Users y Groups, la lista de correos a los cuales enviaremos nuestra campaña. Puede importarlos o incluirlos uno a uno.

New Group

Name:

[+ Bulk Import Users](#) [Download CSV Template](#)

[+ Add](#)

Show entries Search:

First Name **Last Name** **Email** **Position**

No data available in table

Showing 0 to 0 of 0 entries [Previous](#) [Next](#)

[Close](#) [Save changes](#)

33. Puede definir todos los grupos que desee y seleccionarlos según sea la necesidad o temática del engaño.

34. Vaya ahora a Campaigns, al crear la campaña, deberá seleccionar de las listas desplegables los elementos creados en los pasos anteriores.

35. En el url, debe ser cuidadoso, y poner la ip pública del sitio o el dominio adquirido.

New Campaign

Name:

Email Template:

Landing Page:

URL:

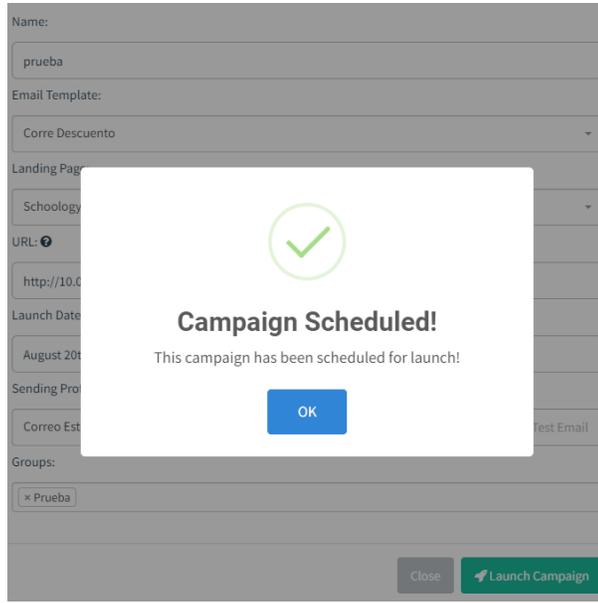
Launch Date Send Emails By (Optional)

Sending Profile:

 [Send Test Email](#)

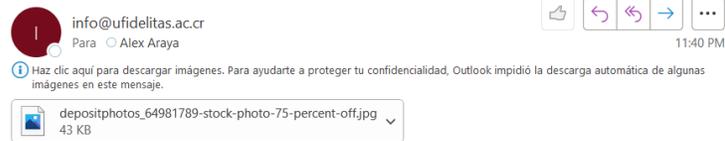
Groups:

[Close](#) [Launch Campaign](#)



36. Haga pruebas internas hasta que el resultado sea el deseado. Algunos ejemplos:

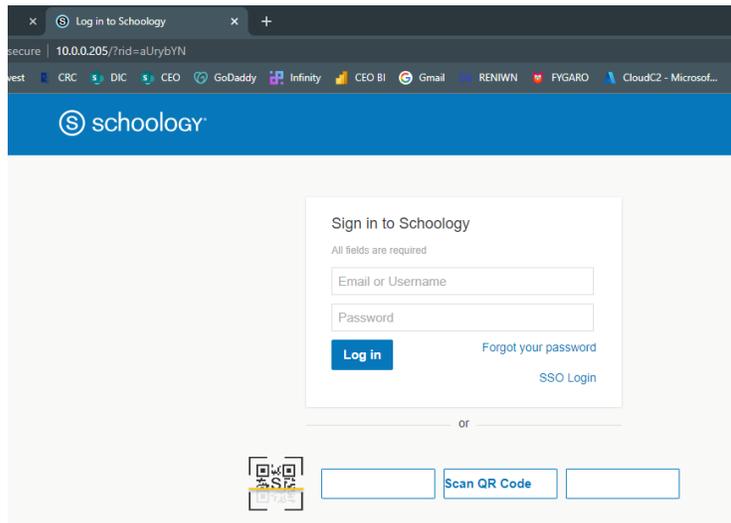
Descuento 75% Matrícula



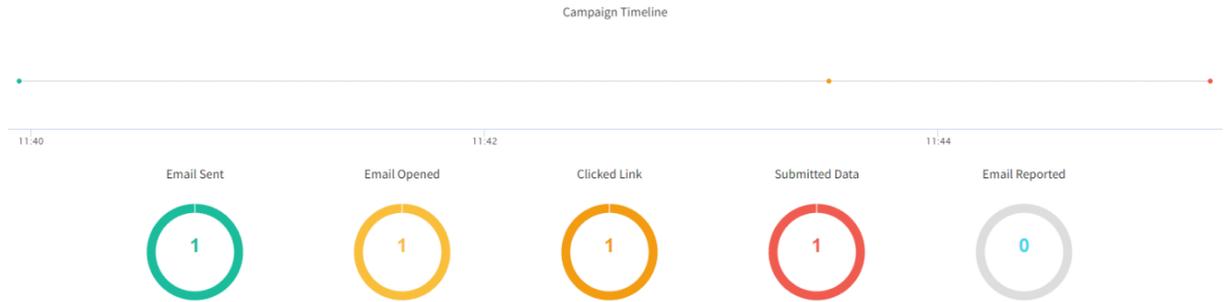
Estimado Alex

Haga clic en este enlace para que pueda disfrutar de un 75% de descuento en sus próximas matrículas.

[75% DESCUENTO](#)



37. Evalúe los resultados en el dashboard.



Details

Show entries

Search:

First Name	Last Name	Email	Position	Status	Reported
Alex	Araya	alex@arayarojas.net		Submitted Data	

Showing 1 to 1 of 1 entries

Previous **1** Next

Timeline for Alex Araya

Email: alex@arayarojas.net

Result ID: aUrybYN

- Campaign Created August 20th 2022 11:39:55 pm
- Email Sent August 20th 2022 11:39:57 pm
- Clicked Link August 20th 2022 11:43:31 pm
- Submitted Data August 20th 2022 11:45:11 pm

Windows (OS Version: 10)
 Chrome (Version: 104.0.0.0)

Windows (OS Version: 10)
 Chrome (Version: 104.0.0.0)

Replay Credentials

View Details

Parameter	Value(s)
__original_url	https://app.schoology.com/login/login
form_build_id	81e7fc6-_XeW3g6BmxgLYLZPitlI9BU5qWiW1ku3_wacRFc3zQ
form_id	s_user_login_form
mail	pedro
password	password1
school	
school_nid	