



UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE CIENCIAS

Práctica 8: IDlusion - The Mirage of Online Identity

ALUMNOS - Las Canijas Lagartijas

Gabriela López Diego - 318243485

Abraham Jiménez Reyes - 318230577

Javier Alejandro Rivera Zavala - 311288876

Juan Daniel San Martín Macías - 318181637

PROFESORA

Anayansi Delia Martínez Hernández

AYUDANTES

Cecilia del Carmen Villatoro Ramos

Roberto Adrián Bonilla Ruiz

Ivan Daniel Galindo Perez

Roberto Adrián Bonilla Ruiz

ASIGNATURA

Criptografía y Seguridad

Fecha de entrega: 30 de Abril del 2024

1. Introducción

En esta práctica supervisada de phishing, cada equipo tendrá la desafiante misión de suplantar un sitio web conocido, a nuestro equipo le fue asignado la plataforma de streaming Netflix. El objetivo principal será crear un sitio web falso que imite el original, induciendo a usuarios desprevenidos a revelar sus credenciales de acceso. Para lograr este objetivo, será fundamental ser creativos, aplicar algo de ingeniería social y diseño web que exploten las vulnerabilidades de los usuarios.

A lo largo de esta práctica, se fomentará la creatividad y el pensamiento crítico para desarrollar estrategias de phishing convincentes. Se analizarán los elementos clave del sitio web original, como la apariencia visual, el diseño de la interfaz, para replicarlos de manera precisa en el sitio web falso.

Para ello, utilizaremos las herramientas **Gophish**, **Zphisher** y una máquina virtual con el sistema operativo **Kali Linux**. Gophish y Zphisher son un proyecto en Github que nos permite realizar ataques de ingeniería social, es decir, *phishing*. El script Zphisher nos proporciona ya de forma predeterminada distintas plantillas de inicio de sesión de los sitios más populares como lo son Facebook, Instagram, Microsoft, Netflix, Google, entre otros. Asimismo, nos otorga algún link de acceso listo para ser enviado al usuario víctima y que al ingresar su información confidencial seremos capaces de capturar de forma inmediata desde la terminal de Kali Linux. De igual forma, Gophish a diferencia de Zphisher, te proporciona la opción de crear y personalizar plantillas de correos electrónicos para hacerlos pasar por verídicos y enviárselos a los usuarios víctima. El objetivo principal de Gophish es ayudar a organizaciones o empresas a evaluar sus respectivos sistemas de seguridad y empleados. El cual se logra, enviando correos electrónicos simulando un ataque de phishing a todos sus empleados y así observar que tan susceptibles son estos ataques. Con los resultados obtenidos (de ser necesario) se podrá brindar una mejor capacitación a los empleados e incluso, una revisión y mejora del sistema de seguridad de la empresa.

2. Desarrollo

■ Instalación de Zphisher

- Primero nos dirigimos al siguiente url <https://github.com/htr-tech/zphisher>

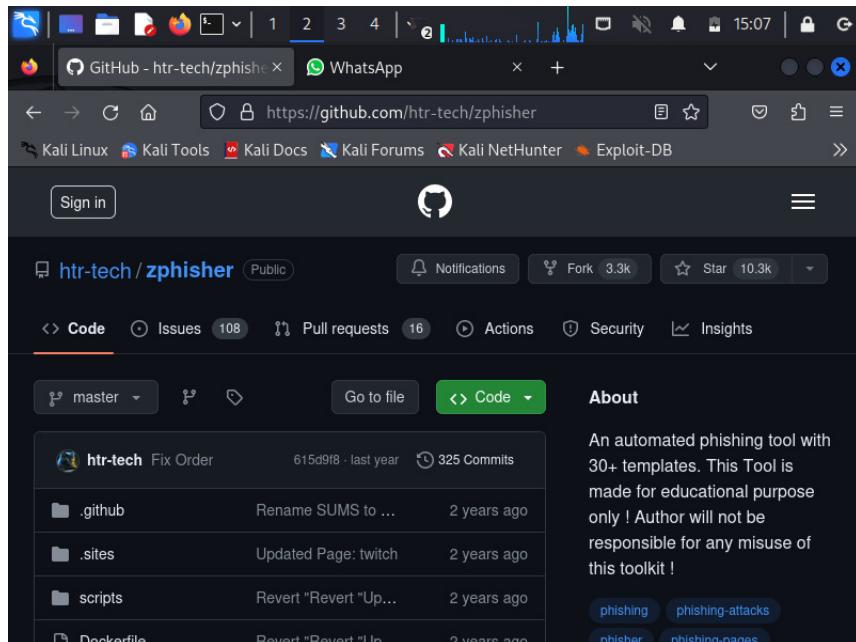


Figura 1: Github con el repositorio Zphisher

y clonaremos el repositorio dentro de una carpeta que hemos llamado Practica8, descargando directamente el proyecto o en la terminal de Kali Linux ejecutando el siguiente comando

```
git clone --depth=1 https://github.com/htr-tech/zphisher.git
```

Una vez ya hayamos clonado el proyecto, nos dirigimos dentro de la carpeta zphisher y ejecutamos el script con el siguiente comando

```
1 bash zphisher.sh
```

```
[+] CPU usage: 16.7%  
File Actions Edit View Help  
zsh: corrupt history file /home/kali/.zsh_history  
[kali㉿ kali] - [~/Desktop/Practica8]  
└─$ git clone --depth=1 https://github.com/htr-tech/zphisher.git  
Cloning into 'zphisher'...  
remote: Enumerating objects: 316, done.  
remote: Counting objects: 100% (316/316), done.  
remote: Compressing objects: 100% (297/297), done.  
remote: Total 316 (delta 49), reused 234 (delta 15), pack-reused 0  
Receiving objects: 100% (316/316), 7.90 MiB | 968.00 KiB/s, done.  
Resolving deltas: 100% (49/49), done.  
  
[kali㉿ kali] - [~/Desktop/Practica8]  
└─$ ls  
gophish-master loclx zphisher  
  
[kali㉿ kali] - [~/Desktop/Practica8]  
└─$ cd zphisher  
  
[kali㉿ kali] - [~/Desktop/Practica8/zphisher]  
└─$ bash zphisher.sh  
[+] Installing required packages...  
[+] Packages already installed.  
[+] Internet Status : Online
```

Figura 2: Instalación de Zphisher

El cual nos desplegará el siguiente menú

Figura 3: Menú Zphisher

Recordemos que para esta práctica se nos asignó la página de inicio de sesión de la plataforma Netflix, así que estaremos trabajando con la opción número 5.

■ Instalación de Gophish

Dicha herramienta esta escrita en el lenguaje de programación Go, así que necesitaremos primero instalarla en nuestra área de trabajo. Ejecutaremos los siguientes comandos en terminal para su instalación.

```
1      sudo apt update
2
3      sudo apt install golang-go
4
5      go version
```

Nota: En la siguiente captura de pantalla ya habíamos instalado Go con anterioridad.

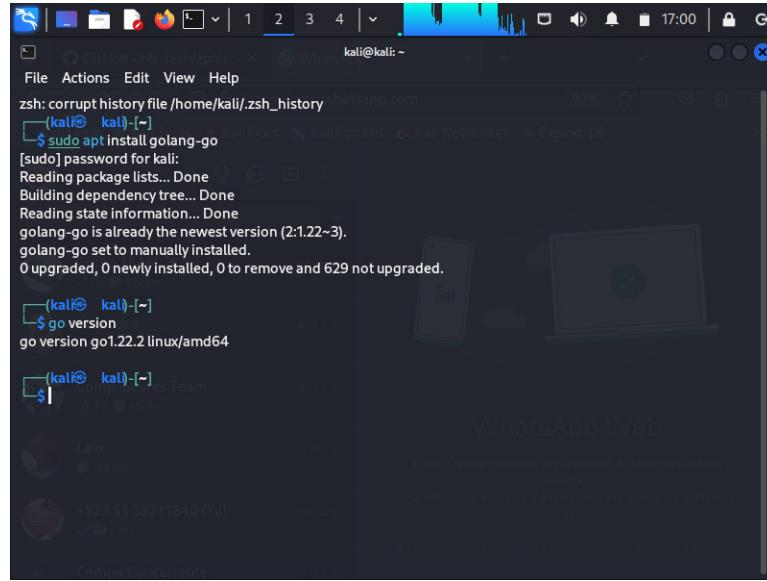


Figura 4: Instalación de Go

Procedemos a clonar el repositorio de Github del siguiente link de igual forma, dentro de la carpeta que hemos llamado Practica8 <https://github.com/gophish/gophish>

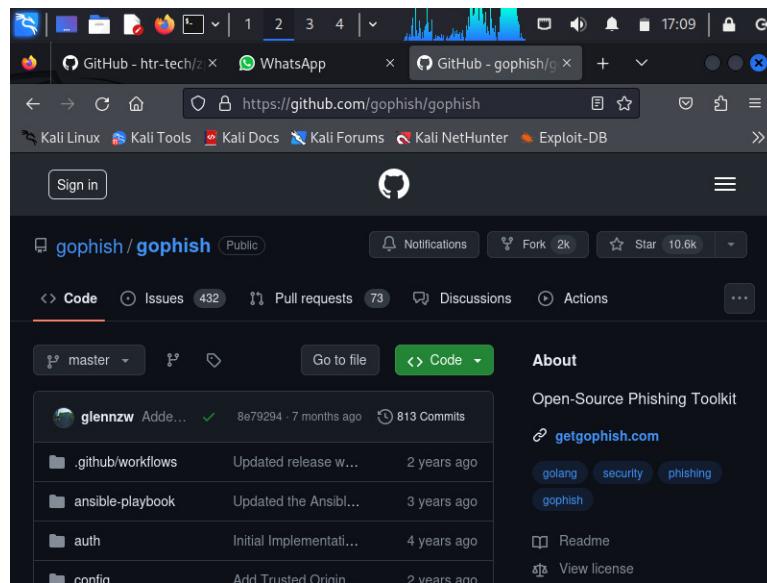


Figura 5: Repositorio Gophish

```

kali@kali: ~/Desktop/Practica8
zsh: corrupt history file /home/kali/.zsh_history
└─(kali㉿ kali) [~/Desktop/Practica8]
└─$ git clone https://github.com/gophish/gophish.git
Cloning into 'gophish'...
remote: Enumerating objects: 8065, done.
remote: Counting objects: 100% (2464/2464), done.
remote: Compressing objects: 100% (503/503), done.
remote: Total 18065 (delta 2127), reused 1961 (delta 1961), pack-reused 5601
Receiving objects: 100% (8065/8065), 52.73 MiB | 1.06 MiB/s, done.
Resolving deltas: 100% (5059/5059), done.

```

Figura 6: Clonar el repositorio Gophish

Nos movemos a la carpeta gophish y ejecutamos los siguientes comandos para ejecutar el proyecto

1 go build

```

kali@kali: ~/Desktop/Practica8/gophish-master
File Actions Edit View Help
└─(kali㉿ kali) [~/Desktop/Practica8/gophish-master]
└─$ go build
go: downloading gopkg.in/alethomas/kingpin.v2 v2.2.6
go: downloading github.com/NYTimes/gziphandler v1.1
go: downloading github.com/gorilla/csrf v1.6.2
go: downloading github.com/gorilla/handlers v1.4.2
go: downloading github.com/gorilla/mux v1.7.3
go: downloading github.com/gorilla/sessions v1.2.0
go: downloading github.com/jordan-wright/unindexed v0.0.0-20181209214434-78fa79113c0f
go: downloading github.com/emersion/go-imap v1.0.4
go: downloading github.com/emersion/go-message v0.12.0
go: downloading github.com/jordan-wright/email v4.0.1-0.20200824153738-3f5bafa1cd84+incompatibl
e
go: downloading github.com/sirupsen/logrus v1.4.2
go: downloading github.com/gorilla/securecookie v1.1.1
go: downloading bitbucket.org/liamtask/goose v0.0.0-20150115234039-8488cc47d90c
go: downloading github.com/PuerkitBio/goquery v1.5.0
go: downloading github.com/go-sql-driver/mysql v1.5.0
go: downloading github.com/gophish/gomail v0.0.0-20200818021916-1f6d0dfd512e
go: downloading github.com/jinzhu/gorm v1.9.12
go: downloading github.com/mattn/go-sqlite3 v2.0.3+incompatible
go: downloading github.com/oschwald/maxminddb-golang v1.6.0
go: downloading github.com/alethomas/template v0.0.0-20190718012654-fb15b899a751
go: downloading github.com/alethomas/units v0.0.0-20190924025748-f65c72e2690d
go: downloading golang.org/x/crypto v0.0.0-20200128174031-69ecbb4d6d5d
go: downloading golang.org/x/time v0.0.0-20200416051211-89c76fbcd5d1

```

Figura 7: Compilamos los archivos fuente del programa Go

Luego, el comando

1 ./gophish

```

kali㉿kali:~/Desktop/Practices8/gophish
File Actions Edit View Help
OK 20191104103306_0.9.0_create_webhooks.sql
OK 2020011600000_0.9.0_imap.sql
OK 2020061900000_0.11.0_password_policy.sql
OK 2020073000000_0.11.0_imap_ignore_cert_errors.sql
OK 2020091400000_0.11.0_last_login.sql
OK 2020120100000_0.11.0_account_locked.sql
OK 20220321133237_0.4.1_envelope_sender.sql
time="2024-04-26T18:17:43-04:00" level=info msg="Please login with the username admin and the p[REDACTED] password a16b3b4f42ea8693"
time="2024-04-26T18:17:43-04:00" level=info msg="Creating new self-signed certificates for administration interface"
time="2024-04-26T18:17:43-04:00" level=info msg="TLS Certificate Generation complete"
time="2024-04-26T18:17:43-04:00" level=info msg="Starting admin server at https://127.0.0.1:3333"
time="2024-04-26T18:17:43-04:00" level=info msg="Starting IMAP monitor manager"
time="2024-04-26T18:17:43-04:00" level=info msg="Starting phishing server at http://0.0.0.0:80"
time="2024-04-26T18:17:43-04:00" level=info msg="Background Worker Started Successfully - Waiting for Campaigns"
time="2024-04-26T18:17:43-04:00" level=info msg="Starting new IMAP monitor for user admin"
2024/04/26 18:17:49 http: TLS handshake error from 127.0.0.1:55354: remote error: tls: bad certificate
2024/04/26 18:17:49 http: TLS handshake error from 127.0.0.1:55364: remote error: tls: bad certificate
2024/04/26 18:17:49 http: TLS handshake error from 127.0.0.1:55368: remote error: tls: bad certificate
time="2024-04-26T18:17:54-04:00" level=info msg="127.0.0.1 -- [26/Apr/2024:18:17:54 -0400] \\"G

```

Figura 8: Ejecución de Gophish

El cual nos mostrará una dirección IP que tiene asignada el adaptador de red y nos permitirá acceder al sitio Gophish. Observemos que en nuestro caso, se nos asignó el siguiente url <https://127.0.0.1:3333> con usuario **admin** y contraseña **a16b3b4f42ea8693**. Nos dirigimos a dicho sitio web e ingresamos con la información proporcionada.

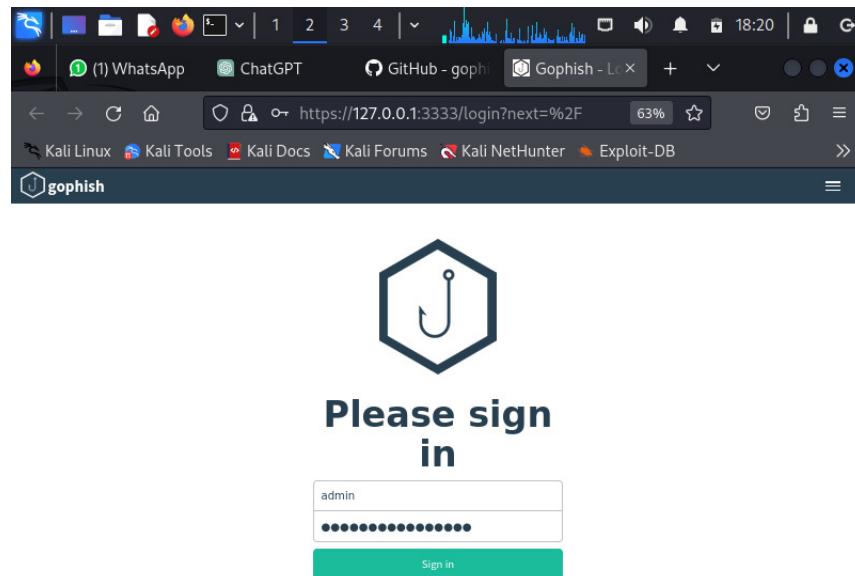


Figura 9: Inicio de sesión de Gophish

Después de que hayamos realizado lo anterior, se nos pide restablecer nuestra contraseña. Ingresaremos una contraseña privada.

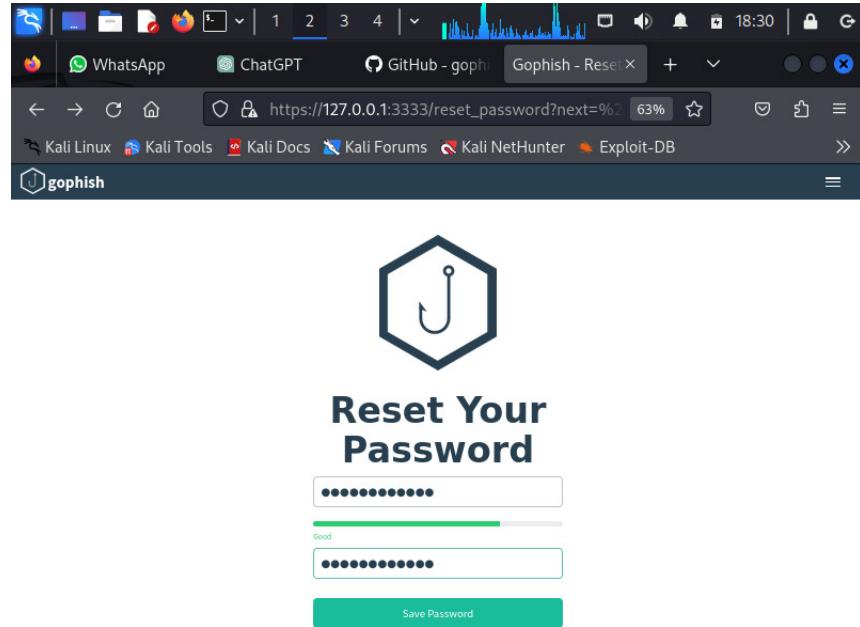


Figura 10: Nueva contraseña en Gophish

Lo primero que nos muestra Gophish es la sección de **Dashboard**

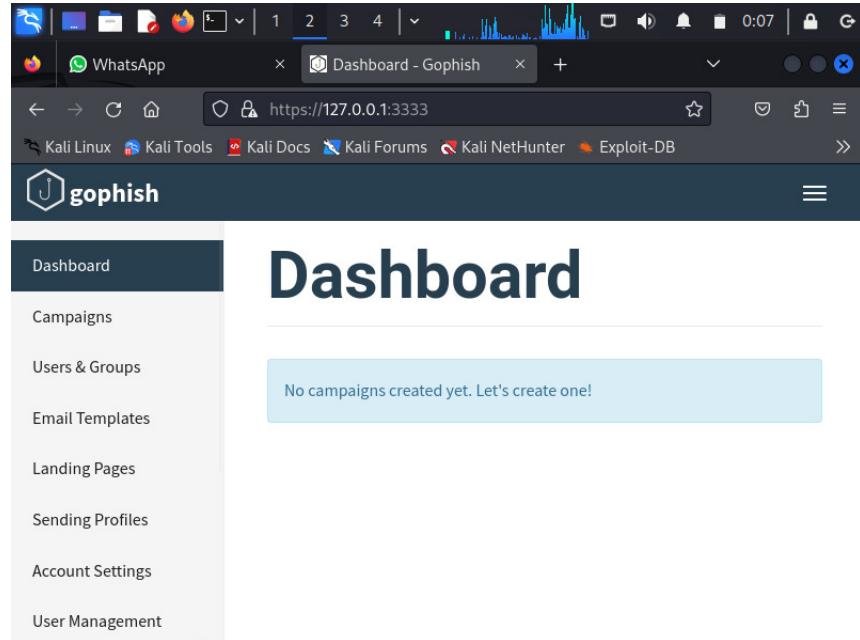


Figura 11: Panel principal de Gophish

Luego, procederemos a la creación de nuestro Perfil de envío. Sección que se encarga de recopilar los datos de donde se envía las simulaciones de correos electrónicos con ataques phishing.

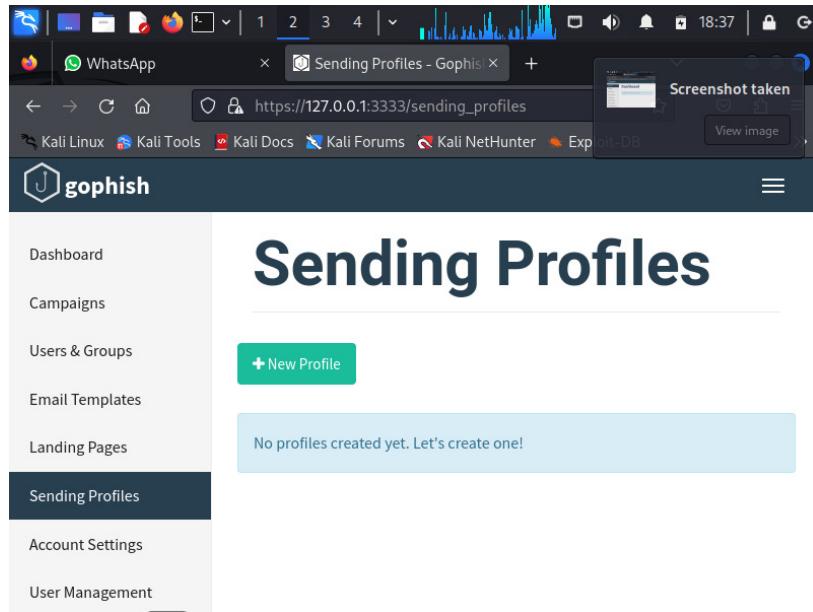


Figura 12: Sección perfil de envío de Gophish

Para ello, creamos un nuevo correo electrónico en Google Gmail. Lo hicimos lo más parecido a un correo verídico que enviaría Netflix a sus usuarios subscriptos. Comparamos con algún correo electrónico real que nos llegó de la plataforma de streaming el cual era

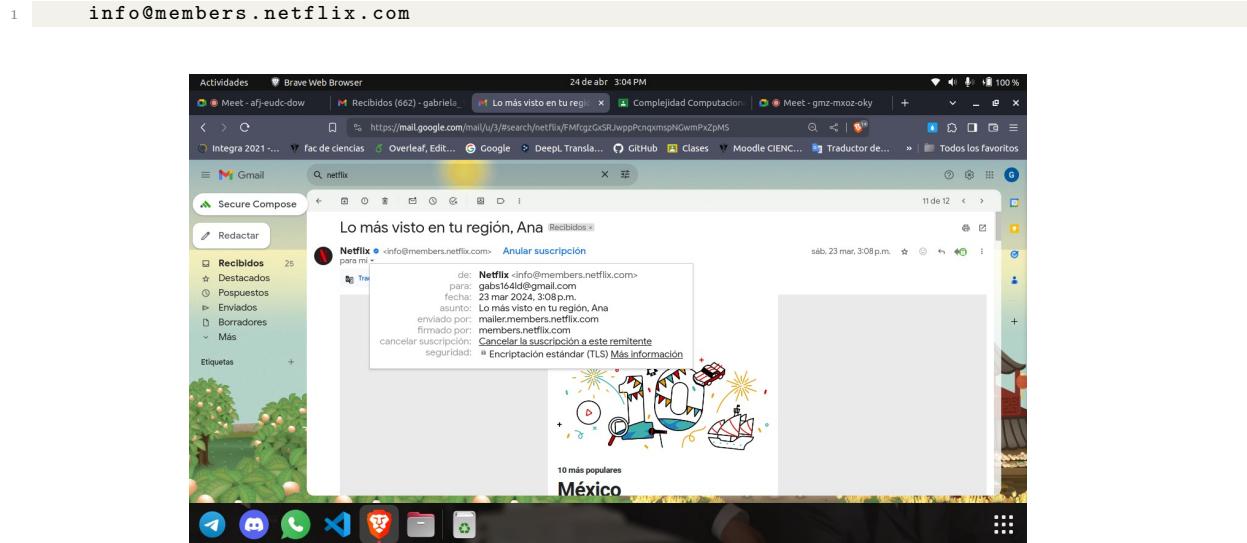


Figura 13: Evidencia de un correo verídico recibido por Netflix

Sabemos que cambiar el dominio de un correo es un tanto complicado, así que crearemos una cuenta de Google Mail. Sin embargo, por las reglas y políticas de Google Gmail fue imposible la creación de un correo con el nombre de perfil igual a Netflix, así que decidimos asignarle el nombre **Netflix México** ya que no es muy lejano al nombre original y es confiable al contener la región de los usuarios víctima. Nuestro correo final quedó de la siguiente manera

Luego, le colocamos como foto de perfil el logotipo original de la plataforma.

The screenshot shows two sections of a Google account profile. The first section, 'Basic info', includes a placeholder profile picture with a 'N' logo, a name field set to 'Netflix México', a birthday field set to 'April 30, 2002', and a gender field set to 'Female'. The second section, 'Contact info', lists two email addresses: 'info.netflix.mexico@gmail.com' and 'gabs164ld@gmail.com'.

Figura 14: Información del correo nuevo creado para la simulación de un correo enviado por la plataforma Netflix

Continuando con la sección de **Edit Sending Profile**, al nombre de la plantilla le asignaremos *Netflix México n1*, colocaremos en SMTP FROM (al igual que username) el correo electrónico que habíamos creado con anterioridad. SMTP es la abreviación de *Protocolo Simple de Transferencia de Correo* que nos ayuda a enviar correos entre servidores de correo. Luego en la casilla Host, colocaremos el portal que utiliza Gmail para el envío de correos el cual es **465**.

The screenshot shows the 'Edit Sending Profile' configuration interface. It includes fields for Name (set to 'Netflix México n1'), Interface Type (set to 'SMTP'), SMTP From (set to 'info.netflix.mexico@gmail.com'), Host (set to 'smtp.gmail.com:465'), Username (set to 'info.netflix.mexico@gmail.com'), and Password (represented by a redacted yellow bar). The 'Username' and 'Password' fields are highlighted with a yellow background.

Figura 15: Edición perfil de envío de Gophish

En password, colocamos la contraseña creada por Google Gmail Security de la sección **App passwords**. Dicha sección ofrece una medida de seguridad adicional para proteger la cuenta de Gmail que no permiten o no son compatibles con la verificación en dos pasos estándar de Google. El cual fue necesario introducir algún número de celular como respaldo.

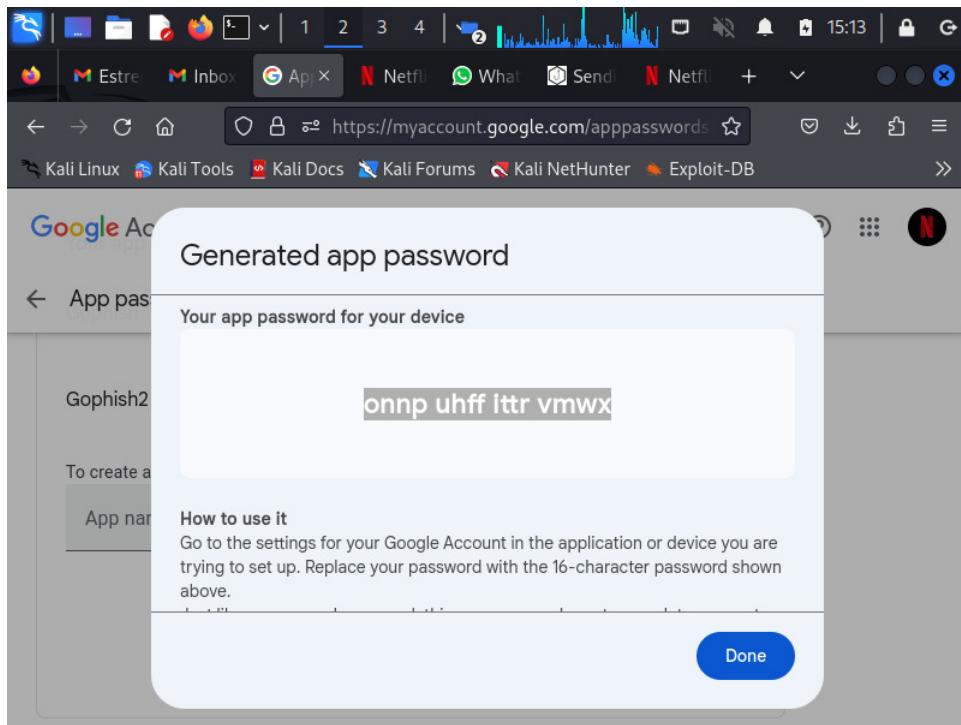


Figura 16: Contraseña de app passwords de Google Gmail

Lo anterior nos permite crear un perfil de envío en Gophish para enviar correos en Gmail. Simplemente lo copiamos y pegamos en la sección de passwords. Para los demás apartados, simplemente los dejamos en blanco y damos click en **Save Profile**

A screenshot of the Gophish profile editor. The top part shows an 'Ignore Certificate Errors' checkbox. Below it is a section for 'Email Headers' with two input fields: 'X-Custom-Header' and '{{.URL}}-gophish', and a red '+ Add Custom Header' button. There are buttons for 'Show 10 entries', 'Search', and 'Send Test Email'. At the bottom are 'Cancel' and 'Save Profile' buttons.

Figura 17: Edición de perfil de envío de Gophish

Después continuamos con la sección **Landing Page**. Dicho apartado se encarga de el clonado de cualquier pagina web.

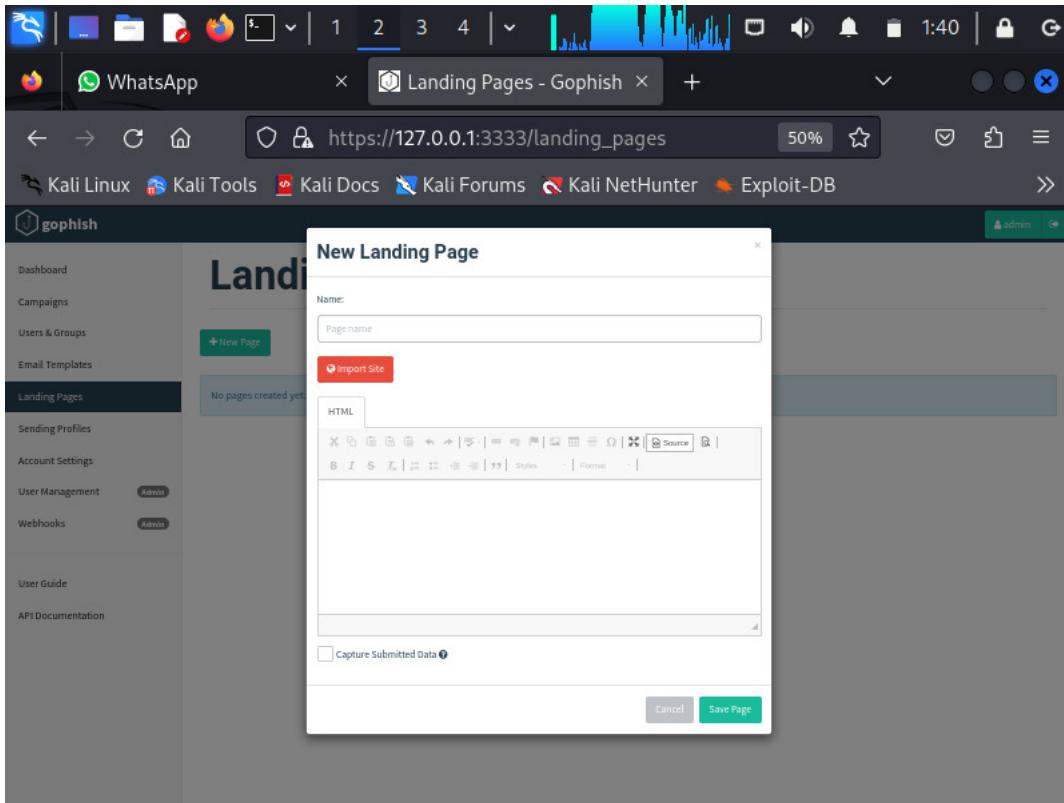


Figura 18: Sección Landing Page

Le damos click en **Import Site** y le colocamos el link del inicio de sesión original de Netflix, al igual que en el apartado *redirige a*. Sin embargo, no obtuvimos éxito pues al crear una campaña como prueba con localhost obtuvimos el siguiente resultado

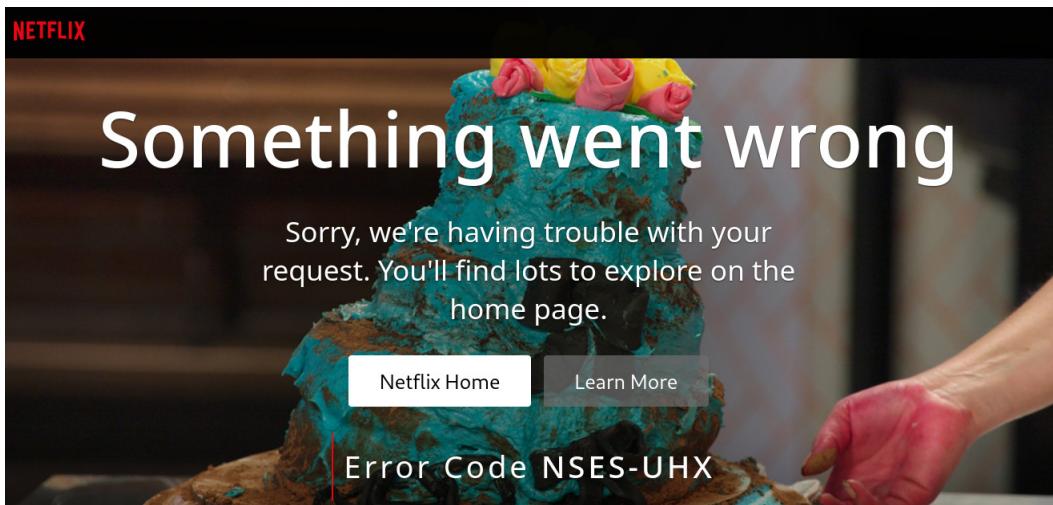


Figura 19: Link inicio de sesión error Netflix

Así que intentamos con el html obtenido de la pagina fuente, el cual nos mostro con exito la página de inicio de sesión de Netflix pero cuando probamos la captura de datos con tal página, tal función no logró concretarse pues nos arrojaba un error con clave 404.

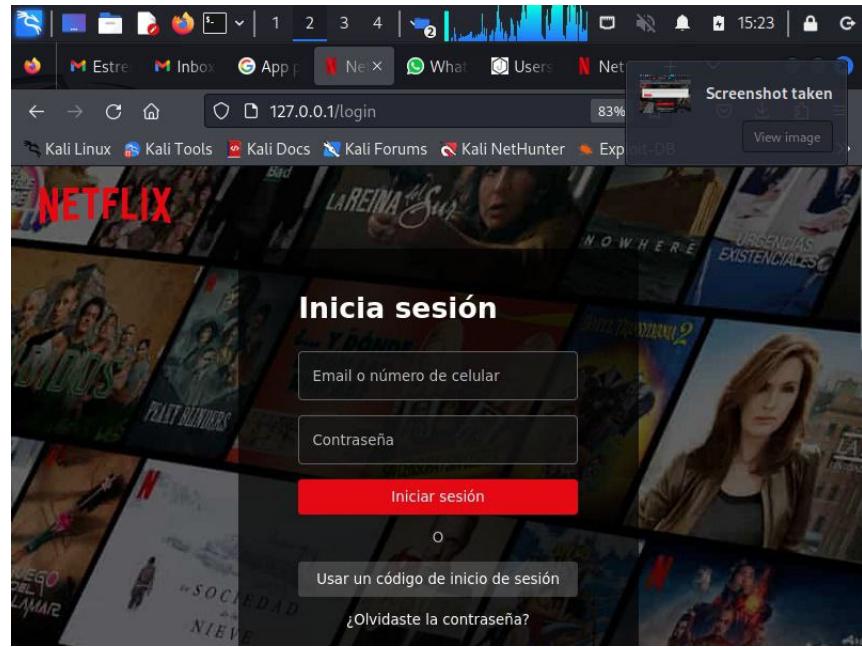


Figura 20: Página de Inicio de sesión clonada de la plataforma Netflix

Fue entonces que decidimos hacer un uso combinado de Gophish y Zphisher, usando este último para la captura de datos y por ende para generar la página falsa de login para Netflix:

Para ello elegimos la opción 05 que nos genera una página señuelo de Netflix, después elegimos un puerto

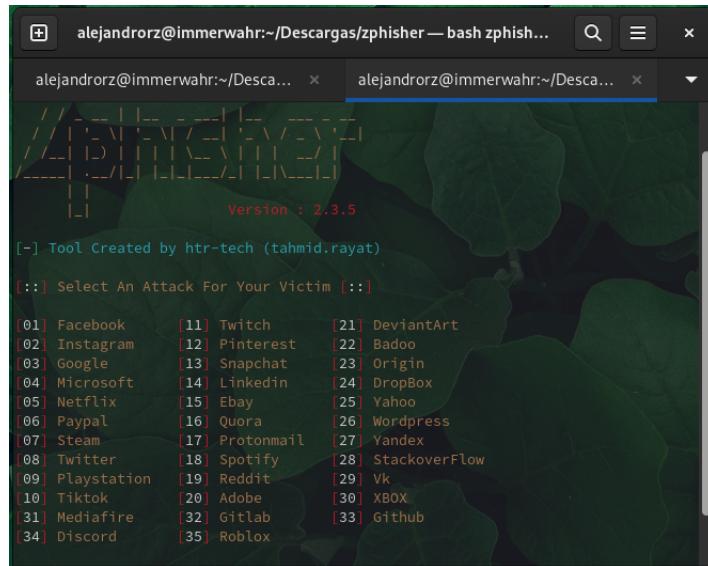


Figura 21: Vista de inicio de Zphisher

a través de Local Xpose que nos permita exhibir nuestro servidor local en la internet y enmascaramos la url con una falsa, similar a la original.

Para lograr todo lo anterior, primero necesitamos de hacernos una cuenta en Local Xpose y enlazarla con Zphisher haciendo uso de nuestro token de acceso:



Figura 22: Cuenta y token de acceso en local Xpose

Ya que estamos enlazados con Local Xpose, procedemos a la creación del puerto y su enmascaramiento



Figura 23: Creación del puerto Local Xpose

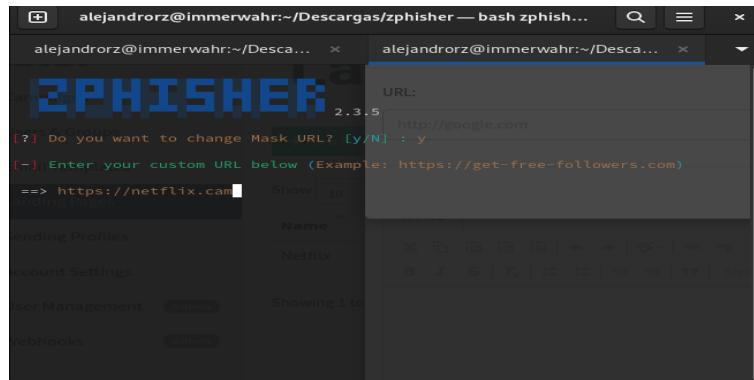


Figura 24: Mascara para el nuevo puerto: https://netflix.cam

Una vez que terminamos con la creación del puerto, Zphisher nos generara una url para nuestra página señuelo

```
1 https://netflix.cam@is.gd/jCPsy9
```

, misma que emplearemos en nuestra landing page de Gophish y que luce como se muestra a continuación:

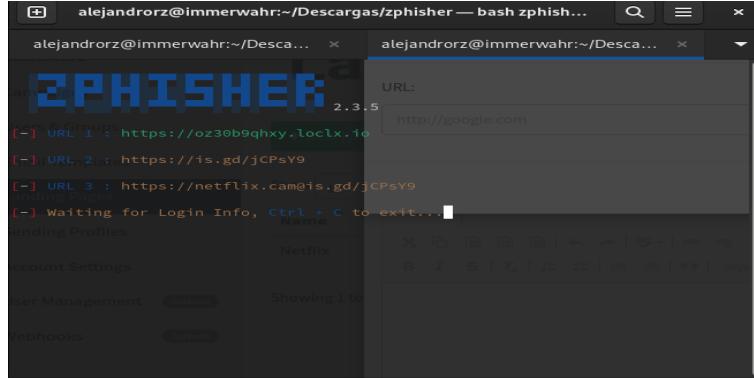


Figura 25: URL's generadas por Zphisher

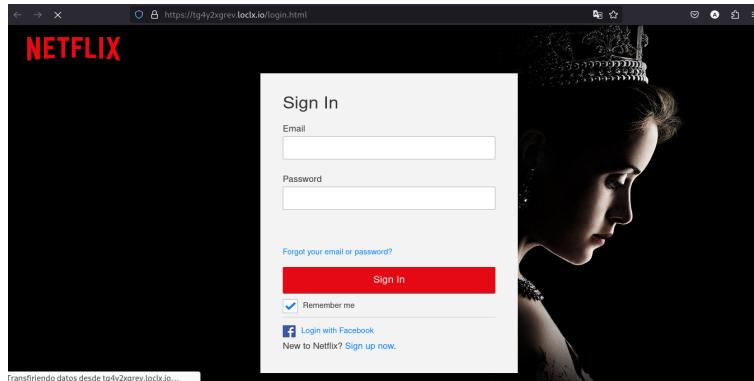


Figura 26: Página señuelo con el login de Netflix

Con la página señuelo y la URL generada, inmediatamente después generamos nuestra landing page dentro de Gophish. Para lograr lo anterior, importaremos el sitio recién creado, no sin antes haberlo abierto desde el navegador para pasar por la verificación de Local Xpose.

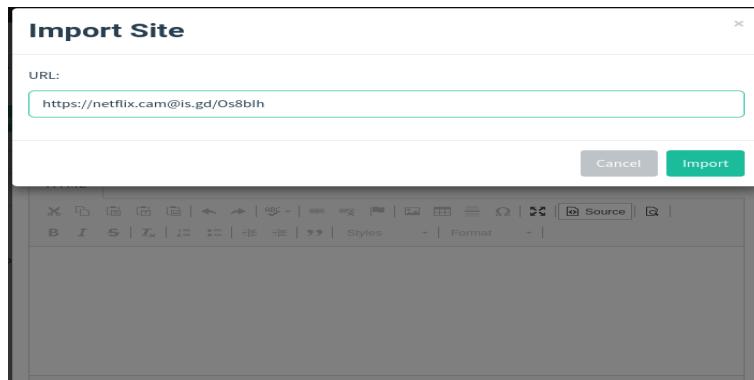


Figura 27: Importación del sitio generado con Zphisher

Después de ello configuramos las demás opciones de modo que se capturen las credenciales de la víctima y que se nos redirija al login real del sitio web de Netflix.

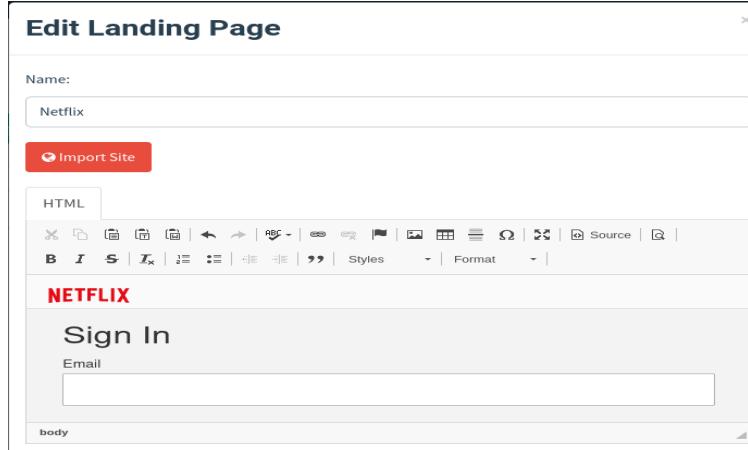


Figura 28: Vista de la página de inicio importada

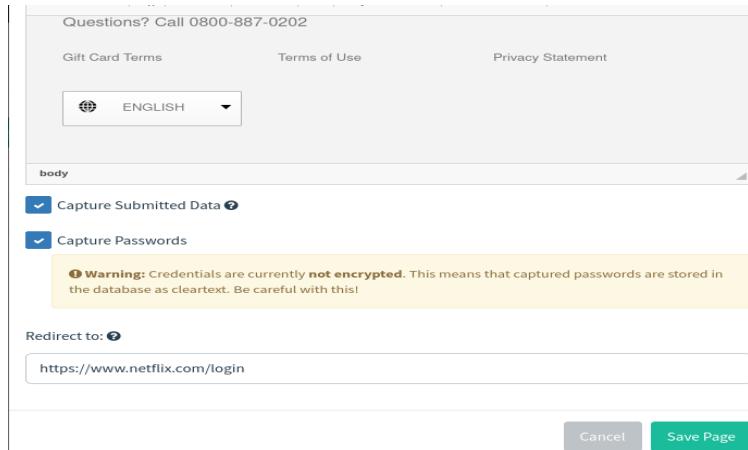


Figura 29: Configuración de las opciones del landing page

Luego, procedemos con la sección **Email Template**.

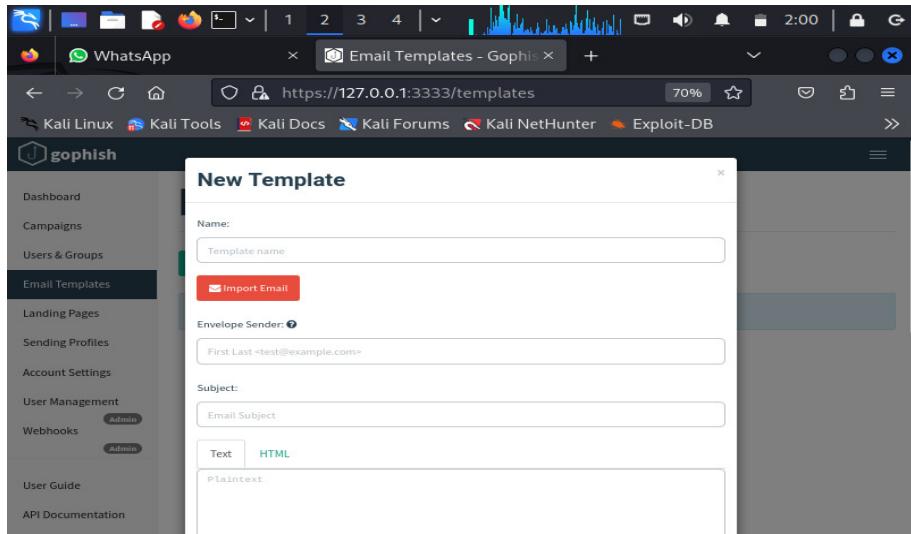


Figura 30: Plantilla creación de un nuevo correo electrónico

De este modo, consultamos algún correo real que hayamos recibido de Netflix y que nos rediriga a su página de inicio de sesión ya que intentamos con **Restablecimiento de contraseña** pero obtuvimos varias complicaciones y observamos que nos redirigía a una página distinta y un tanto sospechosa si el usuario no solicitaba el cambio de su contraseña, por lo que mejor decidimos por un correo que incluía alguna promoción que haría Netflix en cualquier día y hora de la semana. El correo que decidimos imitar fue el siguiente

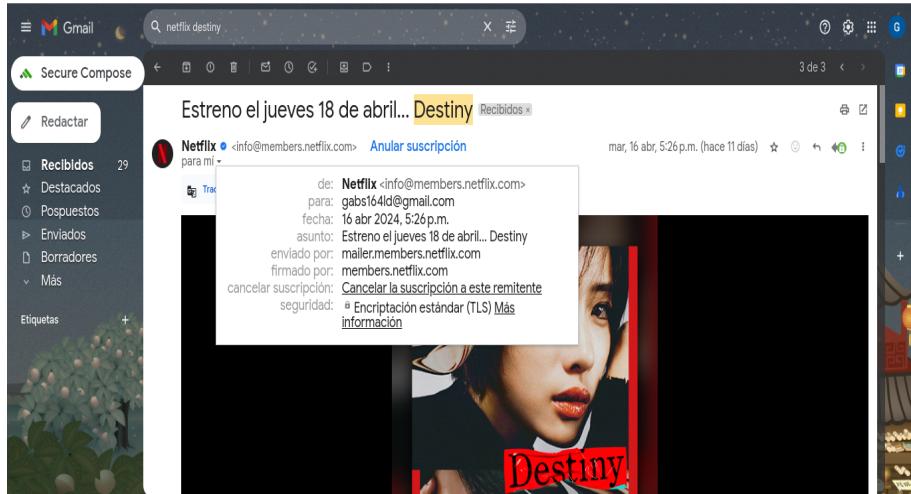


Figura 31: Correo electrónico verídico enviado por Netflix

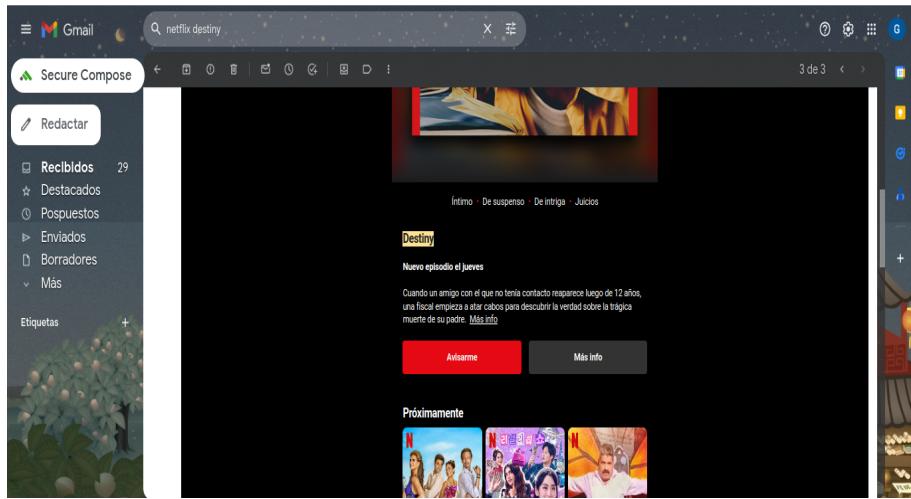


Figura 32: Correo electrónico verídico enviado por Netflix

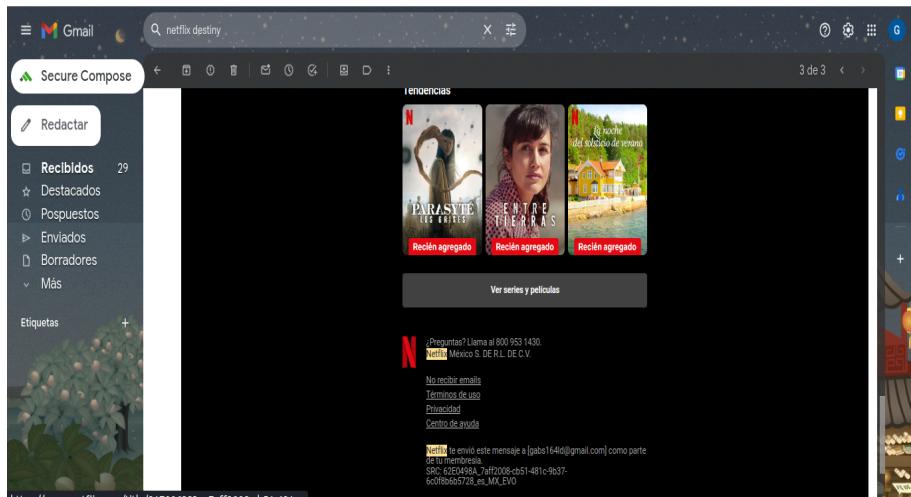


Figura 33: Correo electrónico verídico enviado por Netflix

Le damos click en los 3 puntitos ubicados en la parte superior derecha y seleccionamos **Mostrar Original** el cual nos permite la opción de copiar el html del correo electrónico en cuestión en portapapeles

Una vez hecho lo anterior, lo pegamos en la parte de html de la plantilla **Email template** realizando modificaciones pertinentes para que coincida con el correo de Tim y sea atractivo para él. De igual forma, le asignamos un asunto llamativo para nuestro usuario víctima confié en nuestro correo.

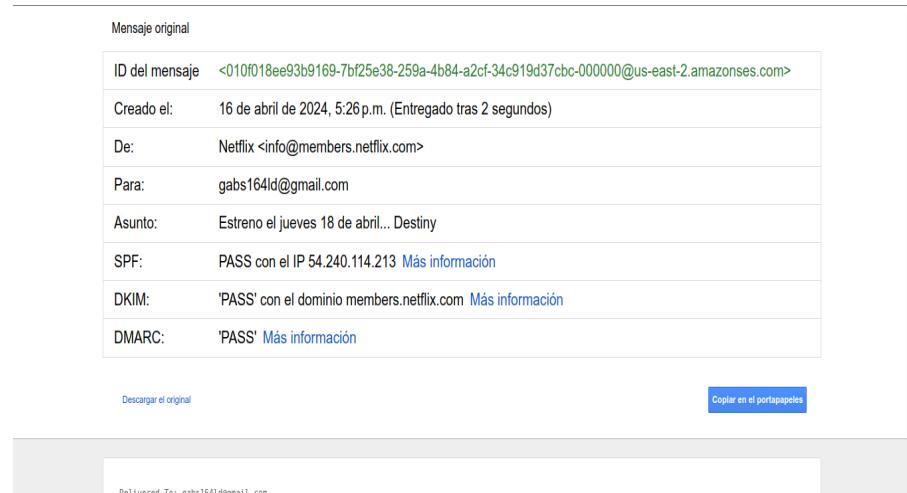


Figura 34: Html del correo que deseamos imitar

The screenshot shows the 'Edit Template' interface in Mailchimp. The template is named 'Netflix'. The imported email content includes:

- Name:** Netflix
- Envelope Sender:** info.netflix.mexico@gmail.com
- Subject:** "Destiny" llega a Netflix, ¡Acceso anticipado!
- Text** and **HTML** tabs are present, with the HTML tab selected. The HTML code is as follows:

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional //EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html style="background-color: #e5e5e5; margin-top: 0; padding: 0; margin: 0;">
```

Figura 35: Plantilla para el envío de un correo electrónico que imita un correo real de Netflix



Figura 36: Texto modificado en el HTML original

Procedemos ahora con la sección **Users & Groups**. Aquí simplemente nos encargamos de ingresar los datos de los usuarios a quienes les enviaremos la simulación del ataque de phishing. Creamos dos apartados, uno para el envío de nuestros correos prueba (que serían enviados a los integrantes del equipo) y otro para nuestro enviar nuestro correo final que era para el usuario víctima **Tim** con el correo electrónico **tbergling9@gmail.com**

The screenshot shows the 'Edit Group' interface with the following details:

- Name:** pruebas
- Bulk Import Users:** + Bulk Import Users, Download CSV Template
- Search Fields:** First Name, Last Name, Email, Position
- Show:** 10 entries
- Search:** Search bar
- User List:**

First Name	Last Name	Email	Position
Abraham		jimeneza@cien...	
Alex		alejandro_river...	
Gabs		gabriela_164@c...	
Juan		juansanmartin...	
- Pagination:** Showing 1 to 4 of 4 entries, Previous, Next
- Buttons:** Close, Save changes

Figura 37: Datos personales de los usuarios víctima como prueba (integrantes del equipo)

The screenshot shows the 'Edit Group' interface with the following details:

- Name:** phished
- Bulk Import Users:** + Bulk Import Users, Download CSV Template
- Search Fields:** First Name, Last Name, Email, Position
- Show:** 10 entries
- Search:** Search bar
- User List:**

First Name	Last Name	Email	Position
Tim		tbergling9@gm...	victim
- Pagination:** Showing 1 to 1 of 1 entries, Previous, Next
- Buttons:** Close, Save changes

Figura 38: Datos personales del usuario víctima Tim

Finalmente, será necesario crear una campaña para lanzar el ataque sobre nuestra víctima, para ello desde el dashboard de Gophish nos dirigimos a la sección de campañas y creamos una nueva tal y como se ve

a continuación, haciendo uso de el perfil de envío que creamos, el grupo que contiene al usuario Tim, la plantilla de email falso, la URL que nos da Zphisher y la página señuelo de los pasos anteriores:

New Campaign

Name:

Email Template:

Landing Page:

URL:

Launch Date Send Emails By (Optional)

Sending Profile:

Groups:

Figura 39: Formulario para la creación de una nueva campaña

Guardamos la nueva campaña y la programamos para ser lanzada, una vez hecho eso podremos darle seguimiento desde el dashboard de Gophish, aunque los datos no serán reportados ahí sino que los obtendremos por la terminal en Zphisher:

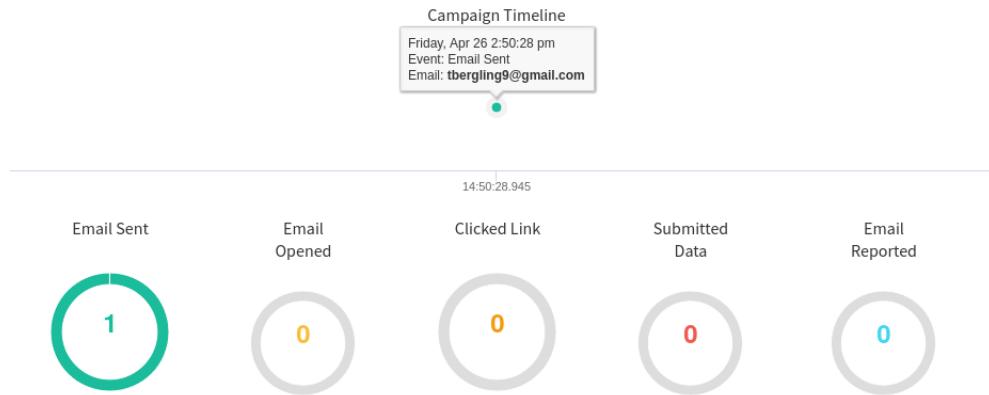
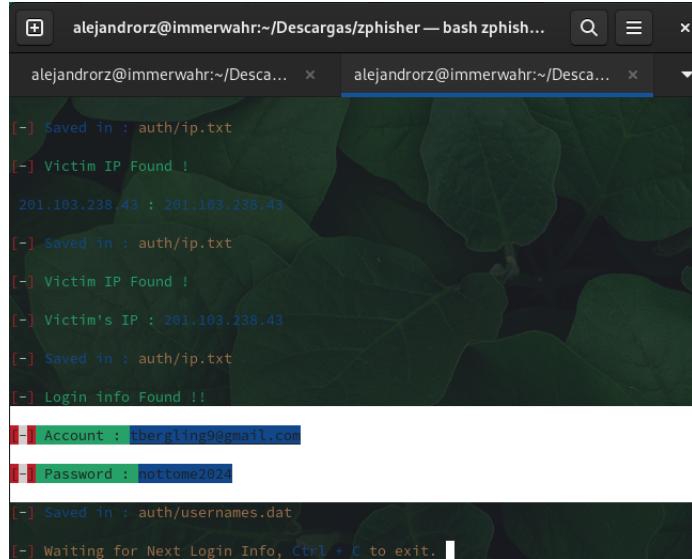


Figura 40: Dashboard con la campaña recién lanzada

Gracias a todo el proceso anterior, logramos capturar las credenciales de Tim que son su dirección de email (tbergling9@gmail.com) y su contraseña (nottome2024):

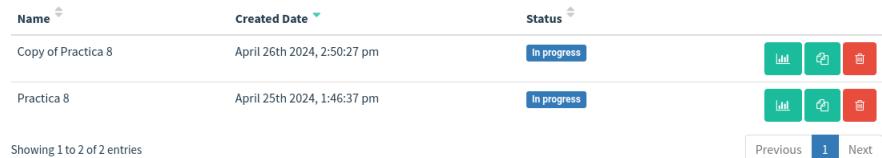


The screenshot shows a terminal window titled "alejandr0rz@immerwahr:~/Descargas/zphisher — bash zphish...". It displays several lines of text output from the Zphisher tool, indicating successful login attempts and credential saving. A specific section highlights captured credentials:

```
[+] Saved in : auth/ip.txt
[-] Victim IP Found !
201.103.238.43 : 201.103.238.43
[+] Saved in : auth/ip.txt
[-] Victim IP Found !
[-] Victim's IP : 201.103.238.43
[+] Saved in : auth/ip.txt
[+] Login info Found !!
Account : tbergling9@gmail.com
Password : nottome2024
[+] Saved in : auth/usernames.dat
[+] Waiting for Next Login Info, Ctrl + C to exit.
```

Figura 41: Credenciales de Tim capturadas desde Zphisher

Incluso hicimos algunas pruebas lanzando campañas entre los miembros del equipo antes de atacar finalmente a Tim, siguiendo el mismo proceso que antes e incluso copiando la campaña, pero modificando el grupo para atacar:



Name	Created Date	Status	Action Buttons
Copy of Practica 8	April 26th 2024, 2:50:27 pm	In progress	
Practica 8	April 25th 2024, 1:46:37 pm	In progress	

Figura 42: Copia de la campaña

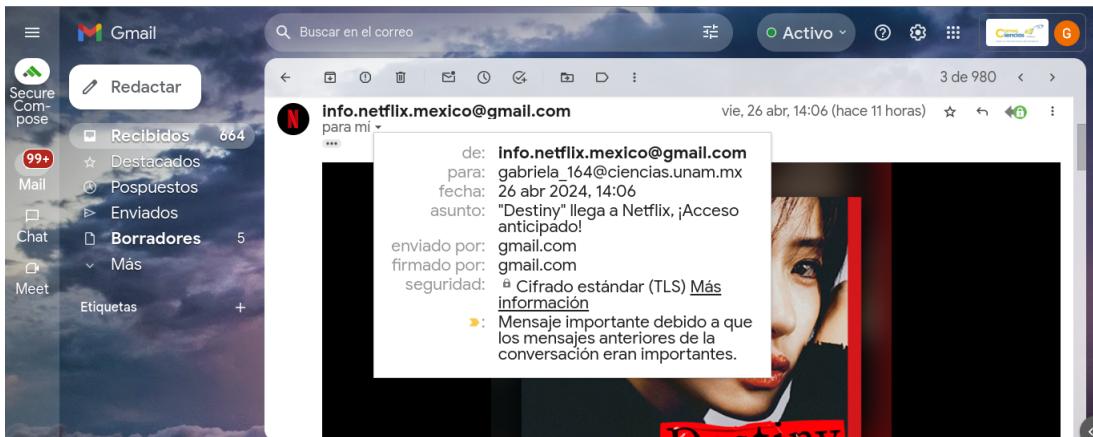


Figura 43: Evidencia del envío del correo falso a Gabriela López

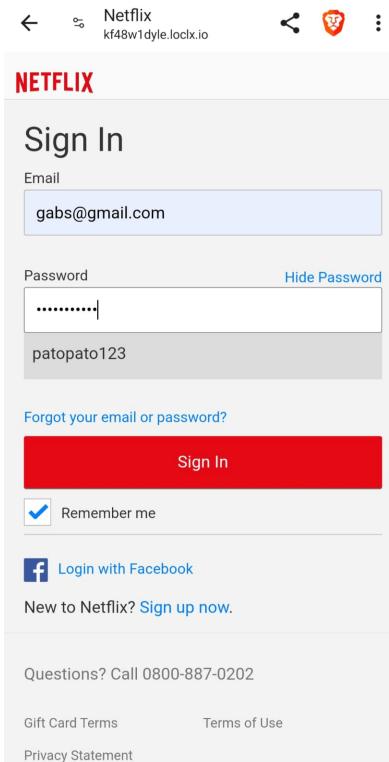


Figura 44: Evidencia del ingreso de datos personales falsos proporcionados por Gabriela López

Preguntas

1. ¿Cuál es el código postal de la casa de Tim?

Lo que hicimos para encontrar éste dato fue buscar en Google Contactos de Tim, así encontramos uno de nombre **Casa**, por lo que al darle clic, nos desglosó los detalles del contacto, entre esos el código postal que es 03810

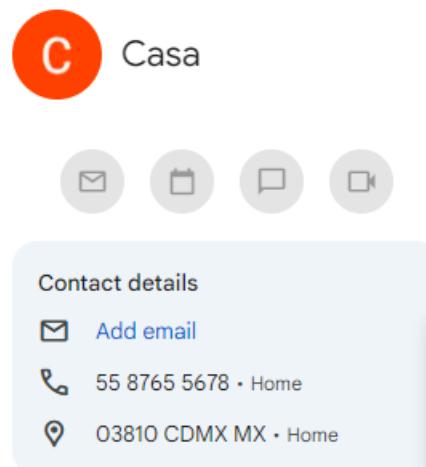
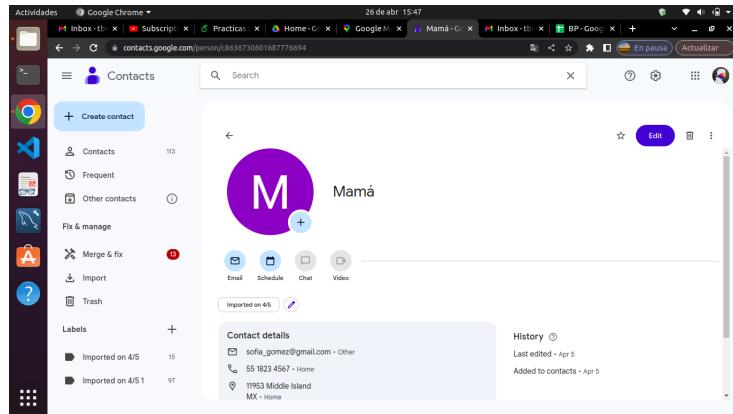


Figura 45: Contacto Casa en Google Contacts

2. ¿Cómo se llama la mamá de Tim?

Para poder contestar ésta pregunta se llevó un proceso similar al de la pregunta anterior, sólo que en ésta ocasión vimos que por lo que se puede ver en el correo, el nombre de la mamá es **Sofía Gómez**

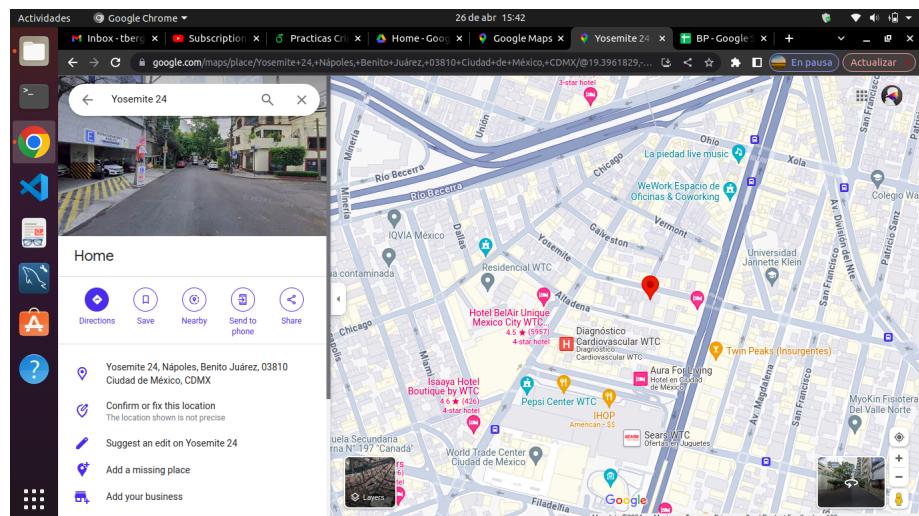


3. ¿Dónde vive Tim? Proporciona su dirección completa?
 Buscamos en sus contactos y encontramos uno llamado Casa

Contact details
✉ Add email
📞 55 8765 5678 • Home
📍 03810 CDMX MX • Home

Figura 46: Contacto Casa en Google Contacts

Luego damos click en la dirección y se nos redireccionó a una pestaña de Google Maps con la siguiente información:
 Yosemite 24, Nápoles, Benito Juárez, 03810 Ciudad de México, CDMX.



4. ¿De qué estado es el mejor amigo de Tim?

Ésta fue la más complicada de contestar, tuvimos que buscar muy bien, pero ya viendo los contactos vimos que es el único que tiene registrado con su fecha de cumpleaños es la de Bob, por lo cual deducimos que son mejores amigos. El estado que vive vive Bob, mejor amigo de Tim es **Texas, US**.

Figura 47: Contacto de Bob

5. ¿Cuántos años tiene el mejor amigo de Tim? ¿Cuando es su cumpleaños?

Actualmente, Bob tiene 23 años y su cumpleaños es el 30 de Junio del año 2000, el próximo 30 de junio del 2024 cumplirá 24.

Name	Birthday	Phone number	Job title & company
Bernardo Figeroa		+529365973614	
Bette Nicka		610-492-4643	
Blair Malet		215-794-4519	
Blondell Pugh		401-300-8122	
Bob	June 30, 2000	+17136934990	
Brock Bologna		212-617-5063	
Cammy Albares		956-841-7216	

6. ¿A dónde se fue de vacaciones Tim? ¿En qué mes y qué actividades realizó?

Tim fue de vacaciones a Cancún en el mes de Abril, siendo exactos el 5 de abril del 2024. Esta información la encontramos en su carpeta de Google Drive en unos archivos con nombres abril.png y vacaciones.png dentro de la carpeta titulada **Vacaciones**. Por el archivo actividades.png deducimos fácilmente que una de las actividades que realizó fue buceo junto a su pareja sentimental e incluso realizó un tour alrededor de la ciudad para tomarse fotografías.

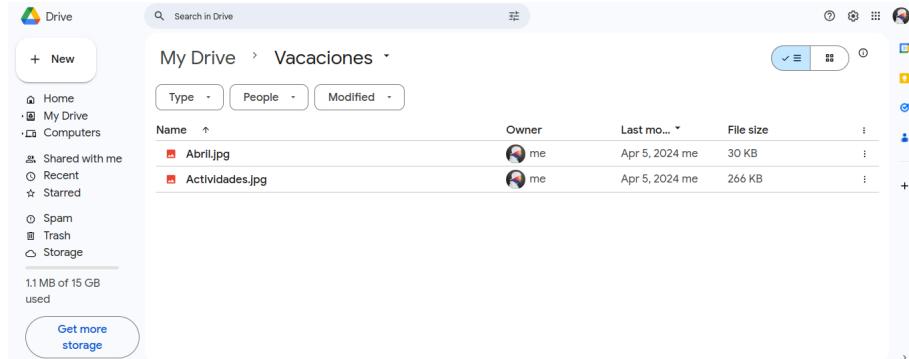


Figura 48: Carpeta Vacaciones en Google Drive de Tim

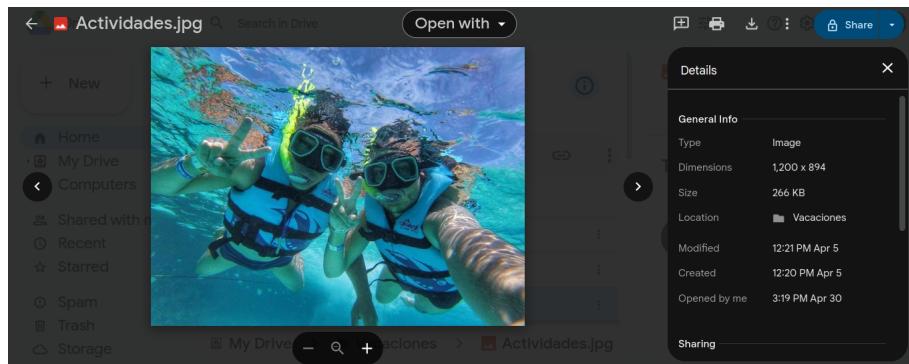


Figura 49: Archivo actividades.png dentro de la carpeta Vacaciones del Google Drive de Tim

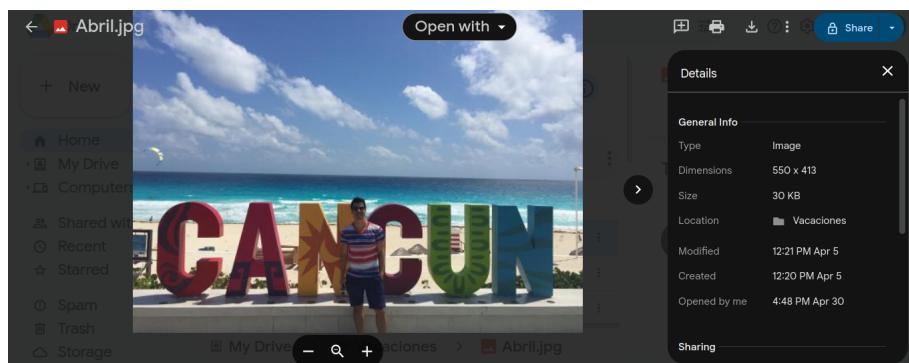


Figura 50: Archivo abril.png dentro de la carpeta Vacaciones del Google Drive de Tim

7. ¿Qué estudia Tim y dónde se encuentra su escuela?

Primeramente, al entrar a su drive nos dimos cuenta que tiene una carpeta llamada Classroom, así mismo, dentro de ésta carpeta hay otra de nombre Arte y Dibujo la cuál está compartida únicamente con `arte_y_dibujo_teachers_9f482b80@classroom.google.com`, por lo que sabemos que Tim estudia algo relacionado a ésto.

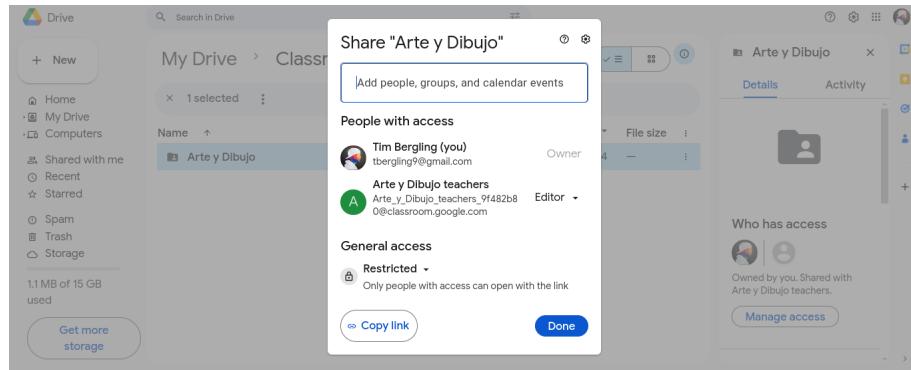


Figura 51: Carpeta Arte y diseño en Google Drive de Tim

Ya sabiendo que estudia algo relacionado al Arte, encontramos un contacto de nombre **Art Venere**, el cuál si googleamos la información del contacto (*company_name: Chemel, James L Cpa county: Gloucester*), nos da éste perfil de linkedin

Figura 52: Perfil Art Venere de Linkedin

Por lo tanto, Tim estudia Arte y Diseño en Nueva Jersey, Estados Unidos.

8. Proporcionar usuarios y contraseñas almacenadas en el archivo BP.

Para ello, indagamos un poco en el Google Drive de Tim y dimos con un excel titulado **BP**. El cual, nos muestra los siguientes usuarios y contraseñas. Dicho archivo se encontraba dentro de una carpeta titulada Personal

Name	Owner	Last modified	File size
BP	me	1:06 PM me	1 KB
BP.csv	me	Apr 25, 2024 me	533 b...

Figura 53: Contenido de la carpeta Personal del Google Drive de Tim

sin nombre de usuario sony4522*
timb189@outlook.com riseandshine11

A	B	C	D	E
1 name	url	username	password	note
2 account_jetbrains.c	https://account.jetbrains.com/reset-password	timb189@outlook.com	sony4522*	
3 github.com	https://github.com/login	time@gmail.com	risesandshine11	
4 www.adidas.mx	https://www.adidas.mx/account-login	timtim14552@hotmail.com	grandcourt15	
5 www.canva.com	https://www.canva.com/es_419/login/	timtim14552@hotmail.com	dayandsun34	
6 www.courseera.org	www.goodreads.com	https://www.goodreads.com/user/new	timberglin15@yopmail.com	music8998
7 www.notion.so	https://www.notion.so/login	tim9@gmail.com	radio15	
8				
9				
10				
11				

Figura 54: Usuarios y contraseñas de Tim guardadas en Google Drive

tim@gmail.com.com grandcourt15

timtim14552@hotmail.com dayandsun34

https://www.goodreads.com/user/new timberglin15@yopmail.com tim9@gmail.com

tim9@gmail.com radio15

9. ¿Cómo se llama la exnovia de Tim y en qué lugar estuvieron el 14/02/2021?

Su ex novia se llama Dayana y estuvieron en el Restaurante Giratorio Bellini el 14 de Febrero del 2021. Ésto lo encontramos ingresando a Google Fotos de Tim, y dándole click en detalle de foto, además como la fecha coincidía con la mencionada en la pregunta podíamos asegurarnos que la foto correspondía a su ex novia. Finalmente, el nombre de la ex novia lo encontramos en el nombre de la foto.

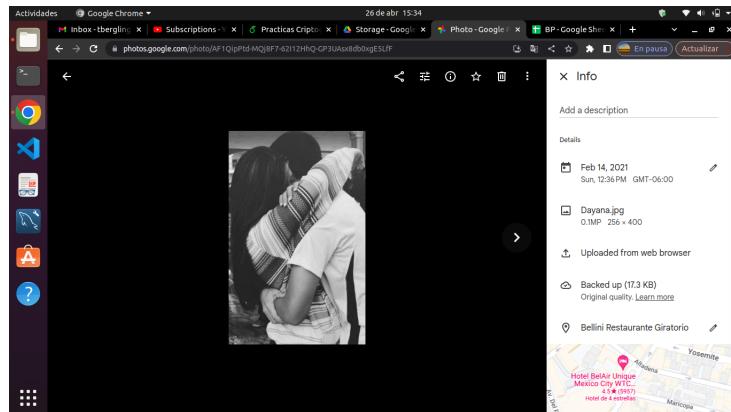


Figura 55: Fotografía encontrada en Google Fotos de Tim y su ex novia Dayana

-
10. ¿Cómo se llama la actual novia de Tim y cuál es el nombre de su mascota de Tim?

Su novia actual se llama Ximena y su mascota se llama Tobby. Esta pregunta la contestamos bajo la misma lógica que la pregunta anterior, y aseguramos que Ximena es su actual novia porque la fecha es más reciente que la foto que se tomó Tim con Dayana.

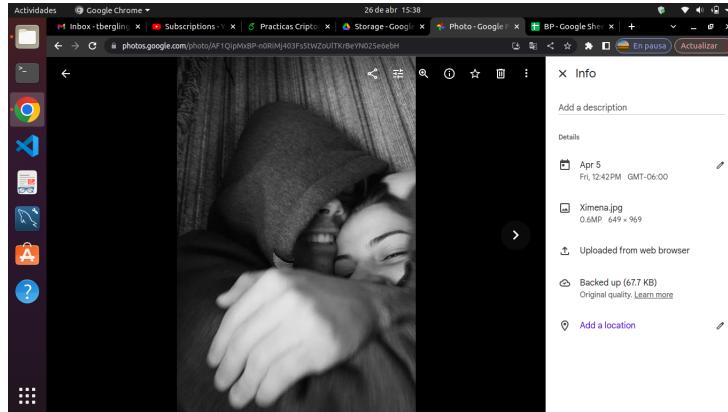


Figura 56: Fotografía encontrada en Google Fotos de Tim y su novia actual Ximena

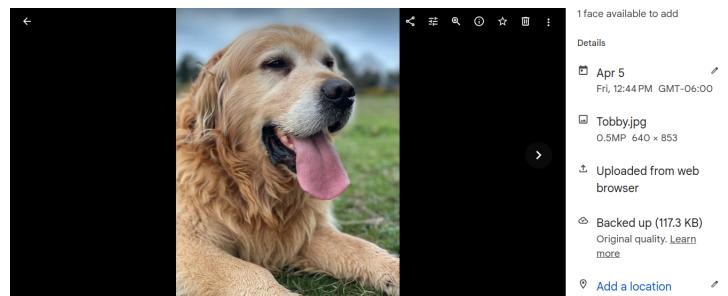


Figura 57: Fotografía encontrada en Google Fotos de Tobby y mascota de Tim

11. ¿A qué canales está suscrito Tim en las redes sociales ?

En youtube esta suscrito a Ibai, s4vitar y S4viOnLive (Backup Directos de Twitch). Esto por ver su cuenta de youtube.

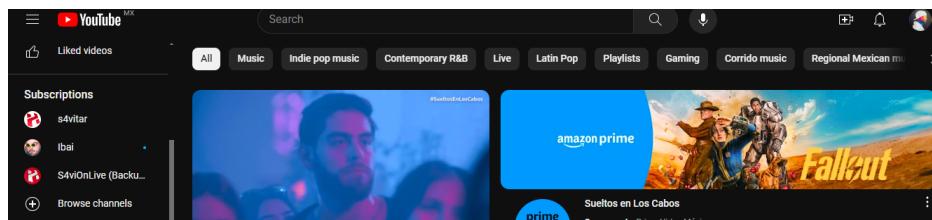


Figura 58: Suscripciones de Tim en la plataforma Youtube

3. Conclusión

La simulación de este ataque de phishing a través del caso de Tim destaca la importancia crítica de la conciencia y la educación en seguridad digital. Tim, como muchos otros usuarios, cayó en la trampa de un correo electrónico aparentemente legítimo y terminó comprometiendo sus credenciales de inicio de sesión debido a la falta de conocimiento sobre los riesgos asociados con la suplantación de identidad en línea.

El ataque ilustra cómo los ciberdelincuentes aprovechan la confianza y la ingenuidad de los usuarios para obtener acceso a información confidencial. El hecho de que Tim utilizara la misma contraseña en varios sitios aumentó aún más su vulnerabilidad, ya que una vez comprometida, su cuenta de Google también quedó expuesta. Nunca confies en un link por mas bonito que se vea, no quiero que vean las fotos con mi ex :(. Además, si vas a caer en un correo phishing de Netflix, asegurate que no tenga ésta foto de perfil.



4. Referencias

- Derechodelared, P. (2022, abril 25). Gophish, la herramienta para entrenar usuarios contra el Phishing. Derecho de la Red; derechodelared. Recuperado el 25 de abril del 2024 de <https://derechodelared.com/gophish/>
- Publicaciones, V. (2021, abril 22). Zphisher: Script de phishing con 30 plantillas recientes y actualizadas. El curso del Hacker; Alexi A.C.V. Recuperado el 25 de abril del 2024 de <https://www.elcursodelhacker.com/zphisher/>
- Edisplay. (s.f.). Configuración del servidor y parámetros SMTP de Gmail - turboSMTP. Smtplib Mail Server - Professional SMTP Service Provider. Recuperado el 26 de abril del 2024 de <https://serversmtp.com/es/servidor-smtp-gmail/#:~:text=Nombre%20de%20servidor%20SMTP%20de,de%20Gmail%3A%2025%20o%20465>