

Protección de filtraciones de información

Incidentes de ciberseguridad



5 de octubre de 2024

Pablo valladares gónzalez

I.E.S Mar de Cádiz

Contenido

[Ejercicio 1 2](#_Toc179049035)

[Tarjetas de crédito 3](#_Toc179049036)

[Correos electrónicos 4](#_Toc179049037)

[Steam Keys 5](#_Toc179049038)

[Bonus 6](#_Toc179049039)

[Ejercicio 2 8](#_Toc179049040)

[Ejercicio 3 11](#_Toc179049041)

[Ejercicio 4 y Ejercicio 5 16](#_Toc179049042)

[Ejercicio 6 19](#_Toc179049043)

[Actividad Bonus 21](#_Toc179049044)

[Conclusión. 22](#_Toc179049045)

# Ejercicio 1

**Cuando hablamos de leaks estamos hablando de una fuga de información de datos. Esto es algo que puede estar accesible en Internet. Pastebin es una web donde cualquier usuario puede subir textos para que estén visibles al público, y donde podemos encontrar muchos leaks de diferentes tipos.**

**Haz uso de pastebin.com junto con las búsquedas de Google como hemos visto en el tema para buscar y encontrar leaks de correos electrónicos y tarjetas de crédito.**

**Explica todo el procedimiento desde las búsquedas hasta el momento de encontrar los leaks.**

**Enumera los enlaces de los leaks que hayas encontrado.**

**(hacerlo usando las búsquedas avanzadas de Google, como site:, "palabra", related:, info:)**

A la hora de utilizar el método site: deberemos poner el dominio entero, por ejemplo, si queremos buscar en Pastebin, deberemos poner pastebin.com, en otro caso no funcionara.

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

## Tarjetas de crédito

Para buscar leaks de tarjetas de crédito en Pastebin, usaremos la búsqueda avanzada de site:pastebin.com además, de eso escribiremos en inglés para aumentar el rango de búsquedas, ya que hay más cosas en ingles que en español.

Búsqueda realizada: site:pastebin.com credit cards leaks.

En este caso la búsqueda tenía 4 páginas de longitud, ya que es algo bastante amplio y no hemos usado las comillas para detallar aún más el margen de búsqueda. (32 enlaces)

Logotipo

Descripción generada automáticamente con confianza media

Si usáramos las comillas nos aparecerían 5 enlaces con leaks (de los cuales solamente 2 tienen tarjetas de créditos de fácil acceso)

URL: https://pastebin.com/vyispz9n

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

## Correos electrónicos

En este caso hemos usado un conjunto de búsquedas avanzadas de Google, site:pastebin.com y las comillas para buscar exactamente lo que queríamos, que en mi caso han sido emails del FBI, "fbi email leaks".

Búsqueda realizada: site:pastebin.com "fbi email leaks"

En el caso de esta búsqueda ha sido el único enlace que me ha aparecido. (1 enlace)

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Este es el leak con los supuestos correos de agentes del FBI. (No he comprobado la veracidad)

URL: https://pastebin.com/dwj5BsVU

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

## Steam Keys

En este caso hemos usado un conjunto de búsquedas avanzadas de Google, site:pastebin.com y las comillas para buscar exactamente lo que queríamos, que en mi caso han sido claves de juegos en steam, "steam keys".

Búsqueda realizada: site:pastebin.com "steam keys"

En el caso de esta búsqueda han aparecido hasta 4 páginas de Google. (33 enlaces)

Interfaz de usuario gráfica

Descripción generada automáticamente con confianza media

Este es uno de los leaks con las supuestas claves de Steam (No he comprobado la veracidad)

URL: [https://pastebin.com/dm8y8n3YUna captura de pantalla de una computadora

Descripción generada automáticamente](https://pastebin.com/dm8y8n3Y)

## Bonus

Algunos de los enlaces de Pastebin te dan enlaces a grupos de telegram o similares para que puedas obtener más enlaces o estafarte de alguna manera, por regla general no recomiendo entrar a enlaces externos y similares, ya que a priori pueden no ser peligrosos, al estar en un entorno “ilegal” es mucho más probable que te encuentres con gente mal intencionada queriéndote atacar.

Captura de pantalla de un celular

Descripción generada automáticamente

Además, he buscado mi propio nombre para comprobar si había algunos de mis datos personales en pastebin y estos han sido los resultados: Texto

Descripción generada automáticamente

Texto

Descripción generada automáticamente

Una captura de pantalla de un celular con texto e imagen

Descripción generada automáticamente con confianza baja

Una captura de pantalla de un celular con texto e imagen

Descripción generada automáticamente con confianza media

# Ejercicio 2

**Para comprobar qué filtraciones puede haber sufrido nuestro correo electrónico existen diversas webs que nos pueden ayudar. Una de ellas es HaveIBeenPwnd. Usa dicha web para comprobar si tus correos habituales han formado parte de una filtración de datos.**

**Una alternativa a HaveIBeenPwnd es BreachDirectory (https://breachdirectory.org/), aunque probablemente la base de datos en la que se basan sea similar.**

Para no poner las imágenes por repetido (de una página y de la otra), lo hare solamente del primer correo.

Interfaz de usuario gráfica

Descripción generada automáticamente

Como las capturas serán principalmente de HaveIBeenPwnd, voy a hacer una breve demostración de como aparecería un correo que ha sido filtrado y un correo que no.

En el caso de que un correo no haya sido filtrado, nos saldrá el siguiente mensaje debajo de la barra de búsqueda de correo:

Texto

Descripción generada automáticamente

En el caso contrario, nos saldrá un mensaje avisándonos de que, si ha sido filtrado, poniendo en cuentas bases de datos ha sido sacado y en cuantos sitios esta copy-pastedo. Además, nos saldrá que información ha sido comprometida en cada caso.

Texto

Descripción generada automáticamente

Yo utilizo 4 – n correos habitualmente (4 correos fijos y para páginas que no creo que vaya a visitar más de una vez o una semana utilizo un correo temporal generado con tempmail)

[waterlolbusiness@hotmail.com](mailto:waterlolbusiness@hotmail.com): Correo personal y con información importante

Captura de pantalla de un celular

Descripción generada automáticamente

[water111polo@hotmail.com](mailto:water111polo@hotmail.com): Primer correo que tuve y que uso para cosas antiguas en las cuales no me renta cambiar de correo

Interfaz de usuario gráfica, Sitio web

Descripción generada automáticamente

[valladaresgonzalezpablo@hotmail.com](mailto:valladaresgonzalezpablo@hotmail.com): Correo utilizado para temas de trabajo y búsqueda de empleo:

Interfaz de usuario gráfica, Sitio web

Descripción generada automáticamente

[waterargentino@hotmail.com](mailto:waterargentino@hotmail.com): Correo con ID de origen argentino para la compra de productos con divisa argentina.

Interfaz de usuario gráfica, Sitio web

Descripción generada automáticamente

[pvalgon155@g.educaand.es](mailto:pvalgon155@g.educaand.es): Correo utilizado para las actividades y tareas de clase.

Interfaz de usuario gráfica, Sitio web

Descripción generada automáticamente

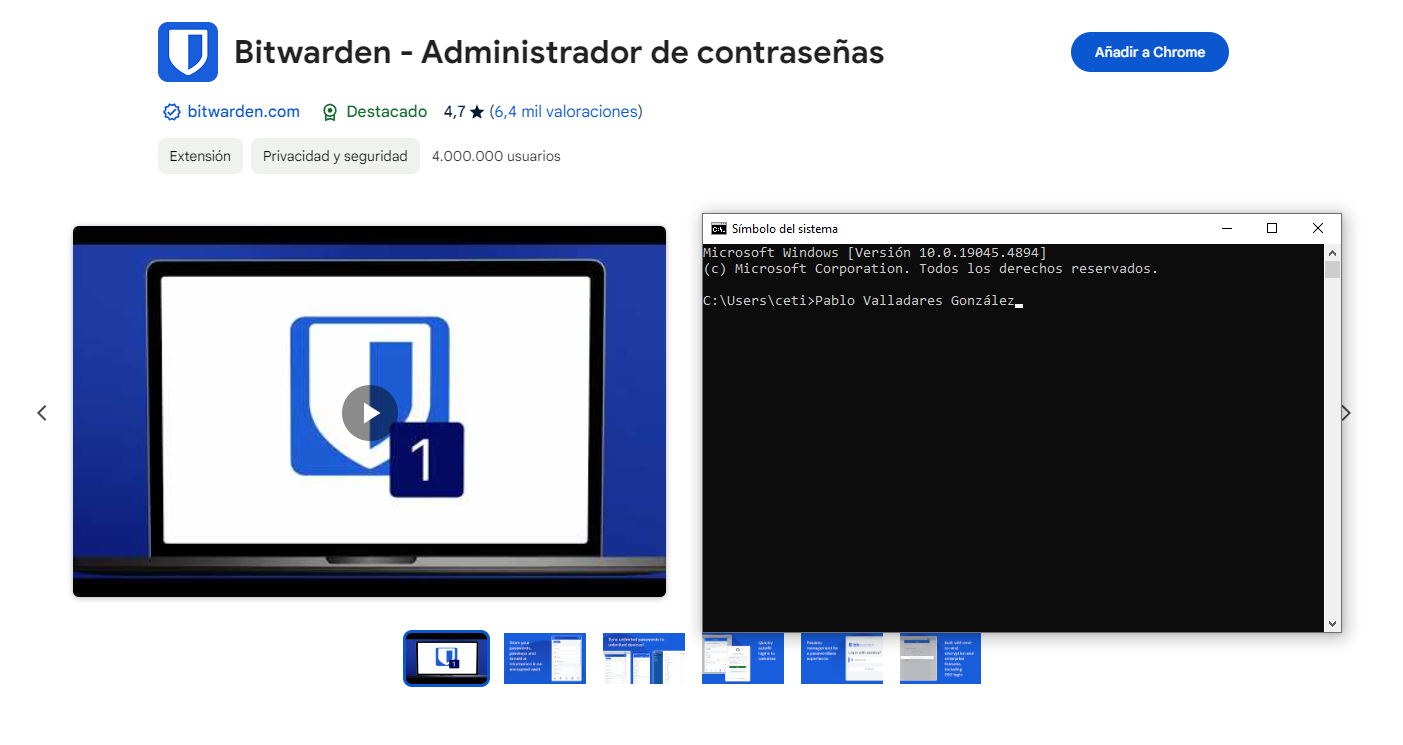
# Ejercicio 3

**Crea una cuenta en Bitwarden.com. Instala la extensión en tu navegador (**[**https://bitwarden.com/**](https://bitwarden.com/)**).**

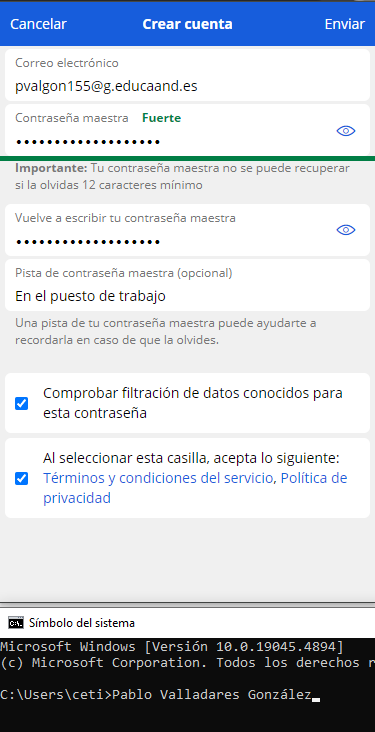
En este caso seguiremos la ruta visible que nos proporciona la página, clicando en los action buttons con call to action que por norma general son los que nos llevaran a descargar un productor en la mayoría de las páginas webs.

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente



Una vez la tengamos activada nos aparecerá arriba a la derecha (normalmente, aunque en otros navegadores como OperaGX aparecerá en la barra lateral izquierda para acceder a ella manualmente y cuando vayamos a añadir una entrada sí que nos aparecerá el pop-up arriba a la derecha).



Ya que necesitaremos saber la contraseña y es preferible no tenerla apuntada en ningún lado, podremos usar los siguientes consejos para crear una contraseña segura y fácil de recordad en vez de autogenerar una.

Para que una contraseña sea segura tiene que ser larga y contener un poco de todo.

1.-Cogueremos varios elementos (recomiendo que este en el momento en el que vayas a usar la aplicación o que estén relacionado con la aplicación).

2.-Un numero (recomiendo que sea el día de creación de la cuenta).

3.-Uno de esos elementos estará completa en mayúscula.

4.-Separar los elementos con caracteres especiales (#/-.,:).

5.-Añadirle un prefijo o un sufijo relacionado con el sitio (Netflix = NF, Facebook = FB, Bitwarden = BW).

Ejemplo:

FB#ventana-MONITOR.10 – Cuenta para Facebook.

BW#SEGURIDAD-gestor.12 – Cuenta para BitWarden.

documental-SERIE.05#NF – Cuenta para Netflix.

En el caso de que añadamos una pista de contraseña, cuando la necesitemos, en vez de mostrárnosla directamente lo que hará es pedirnos que introduzcamos el correo para que nos envíen a él la pista de la contraseña. Deberás usar una pista que entiendas pero que no de demasiado información, aun así, con nuestro método si la pista da mucha información seguirá siendo complicado el adivinar nuestra contraseña.

Texto

Descripción generada automáticamente

Una captura de pantalla de un celular

Descripción generada automáticamente con confianza mediaBitwarden tiene una serie de pestañas que tienen usos diferentes:

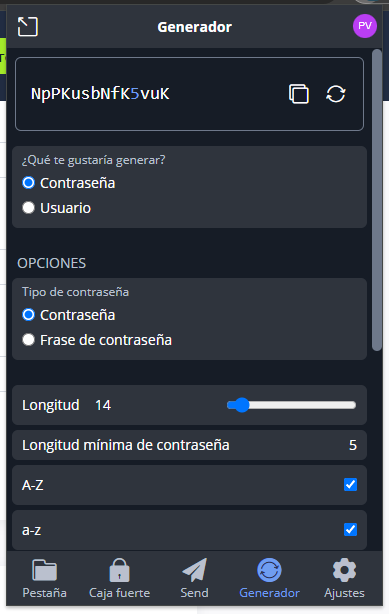
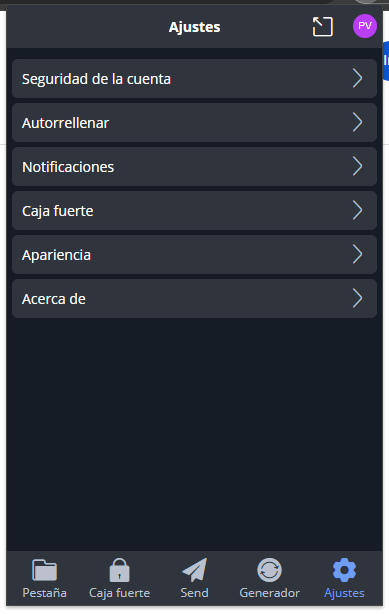
En la caja fuerte nos aparece todos los correos que tengamos asociados con Bitwarden, además de la cantidad de cada tipo que tenemos y la papelera.

Captura de pantalla de un celular

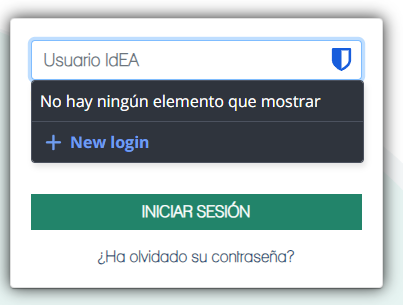
Descripción generada automáticamenteEn la pestaña aparecerán todas las entradas/tarjetas/identidad que estén asociadas a la pestaña que tengas abierta actualmente en google.

Captura de pantalla de un celular

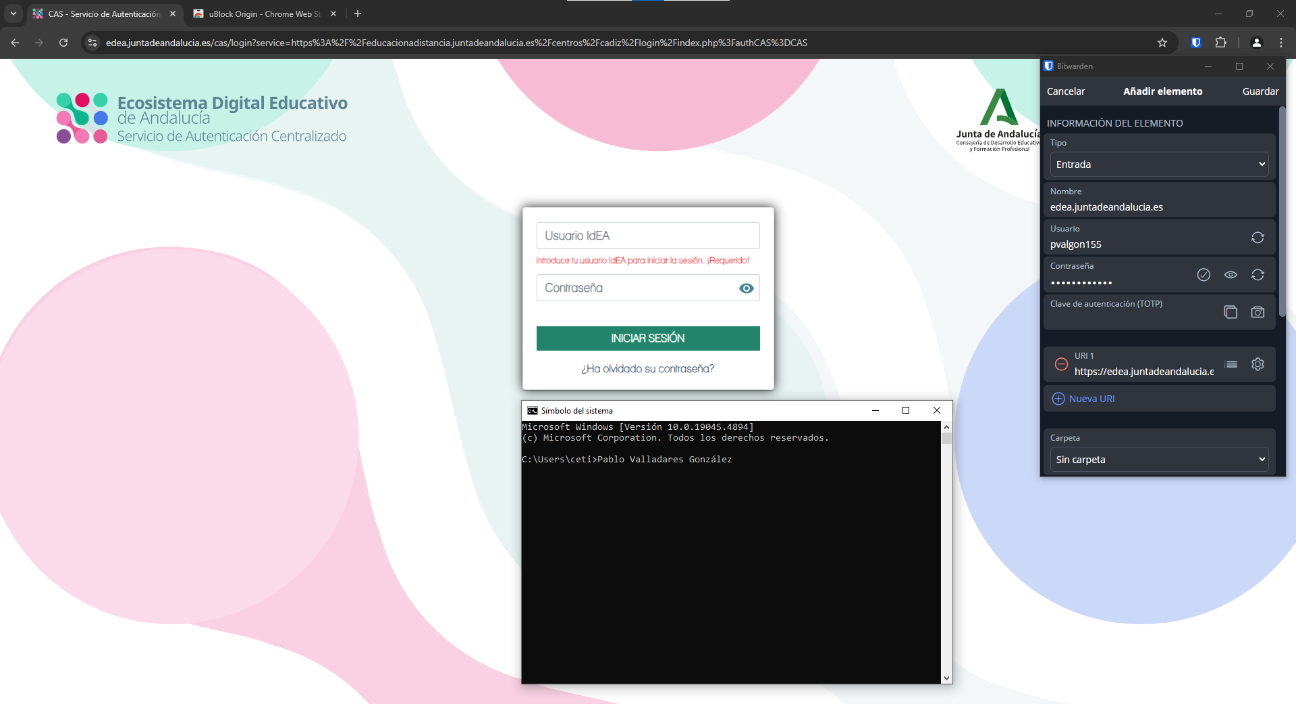
Descripción generada automáticamenteEl apartado Send sirve para enviar correos directamente desde el propio Bitwarden sin necesidad de usar una aplicación externa a el.

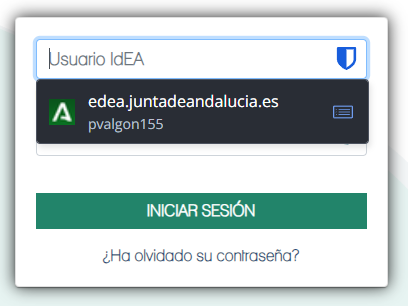
En Generador, podremos generar contraseñas automáticamente con las características que marquemos, además de poder generar un alias de usuario por si no queremos usar el nuestro.

En Ajustes podremos cambiar un montón de cosas, tales como la apariencia y ponerlo en modo oscuro y demás opciones libres a tu elección.

Una vez ya hemos hecho un repaso general sobre los apartados de la aplicación, veremos el uso de dicha aplicación, cuando vayamos a iniciar sesión en algún sitio nos aparecerá el icono de Bitwarden y si queremos añadir una nueva entrada.

Cuando le demos a “New login” nos saldrá arriba a la derecha un pop-up al cual introducir los datos para que este guarde los datos y la próxima vez en vez de aparecer “New login” aparecerá la entrada para poder iniciar directamente de ahí, ya que este te auto rellenara los datos.



Como podemos ver en esta captura, una vez lo pulsemos ya nos autocompletara los datos y solo tendremos que darle continuar/iniciar sesión dependiendo de la página en cuestión.

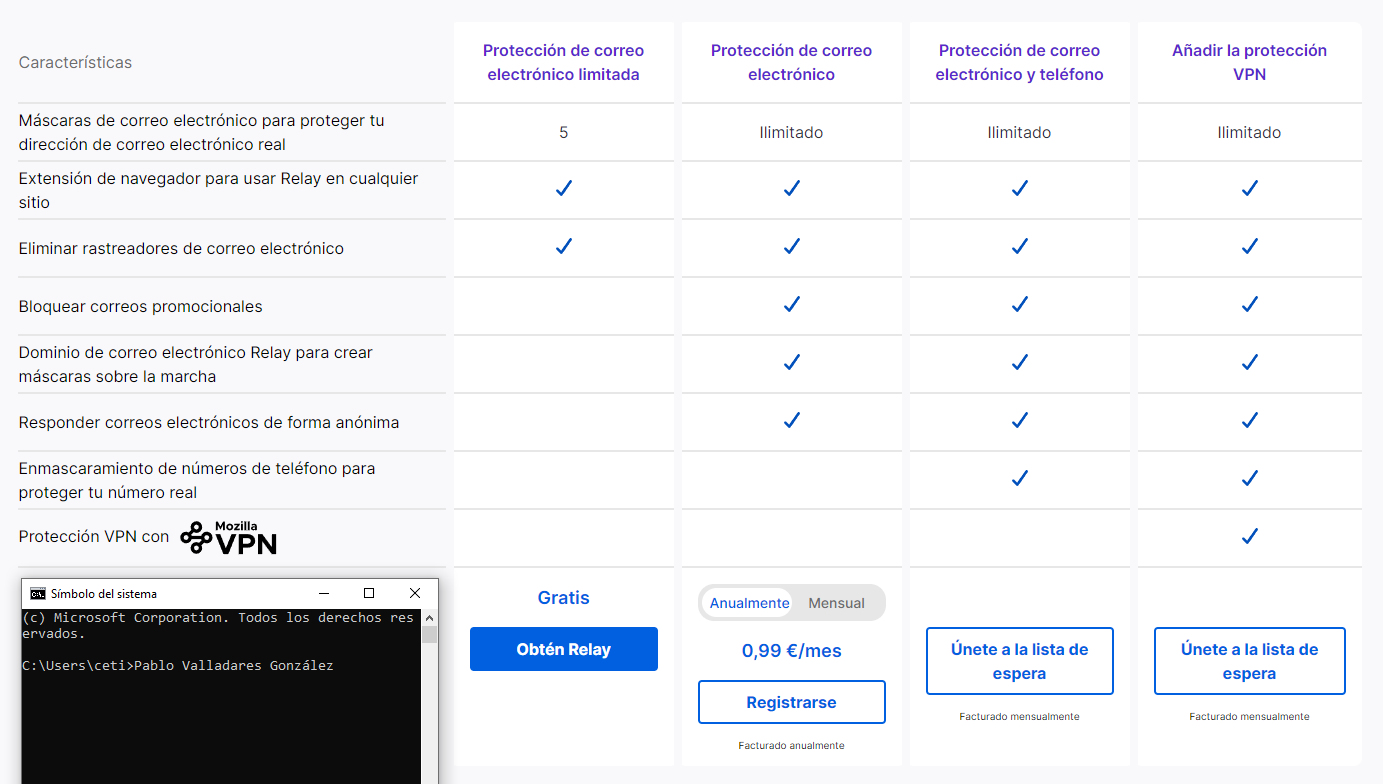
# Ejercicio 4 y Ejercicio 5

**Crea una cuenta en Firefox y usa Firefox Relay (**[**https://relay.firefox.com/**](https://relay.firefox.com/)**).**

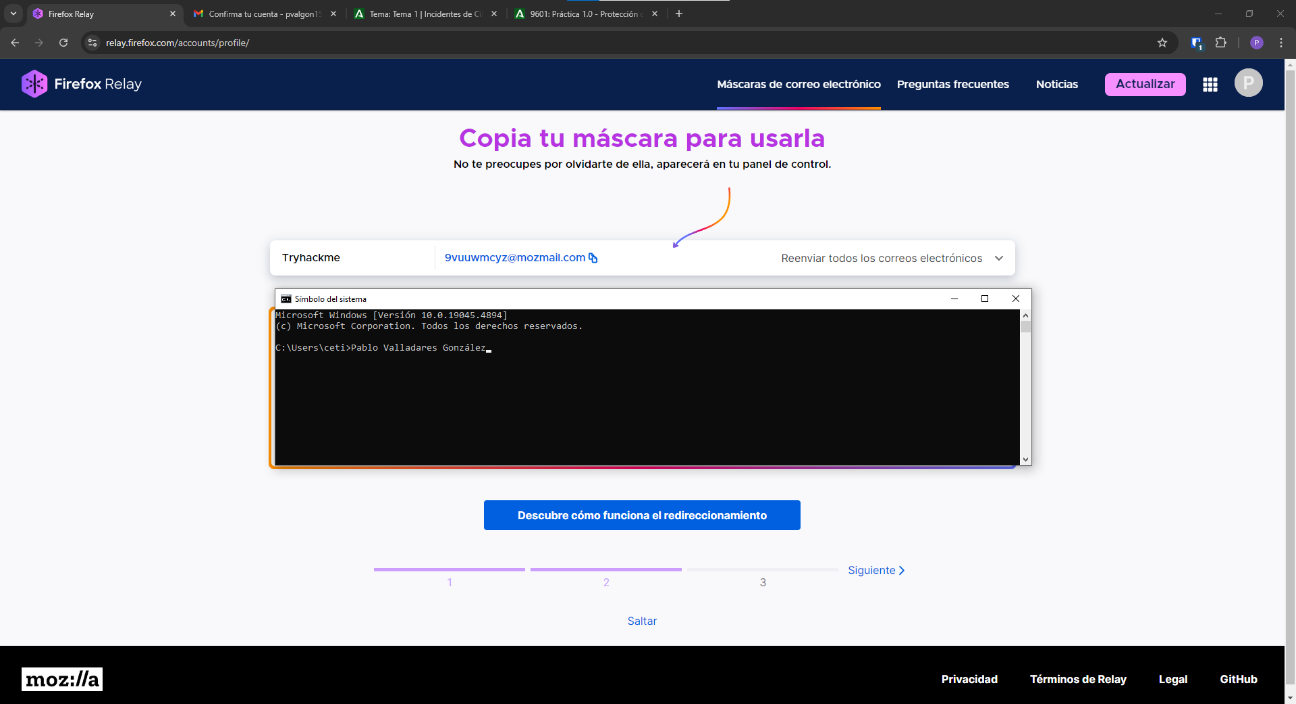
**Crea una cuenta en tryhackme con un alias de firefox relay y generando una contraseña con bitwarden. Almacena la contraseña en bitwarden.**

Ya que vamos a crear una cuenta en tryhackme, lo haremos con una máscara de Firefox relay para aumentar así la seguridad y darle una utilización de verdad.

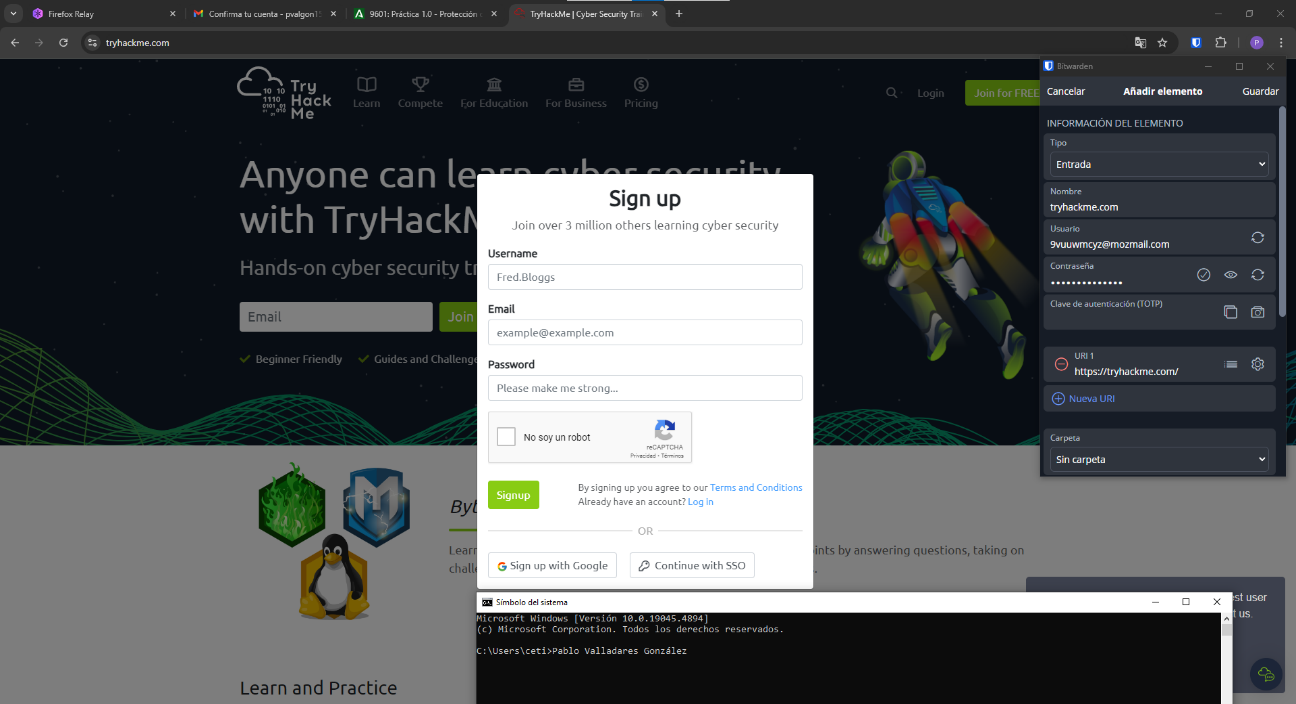
Iremos a descargar Firefox Relay, la versión gratuita la cual te da 5 mascaras de email.



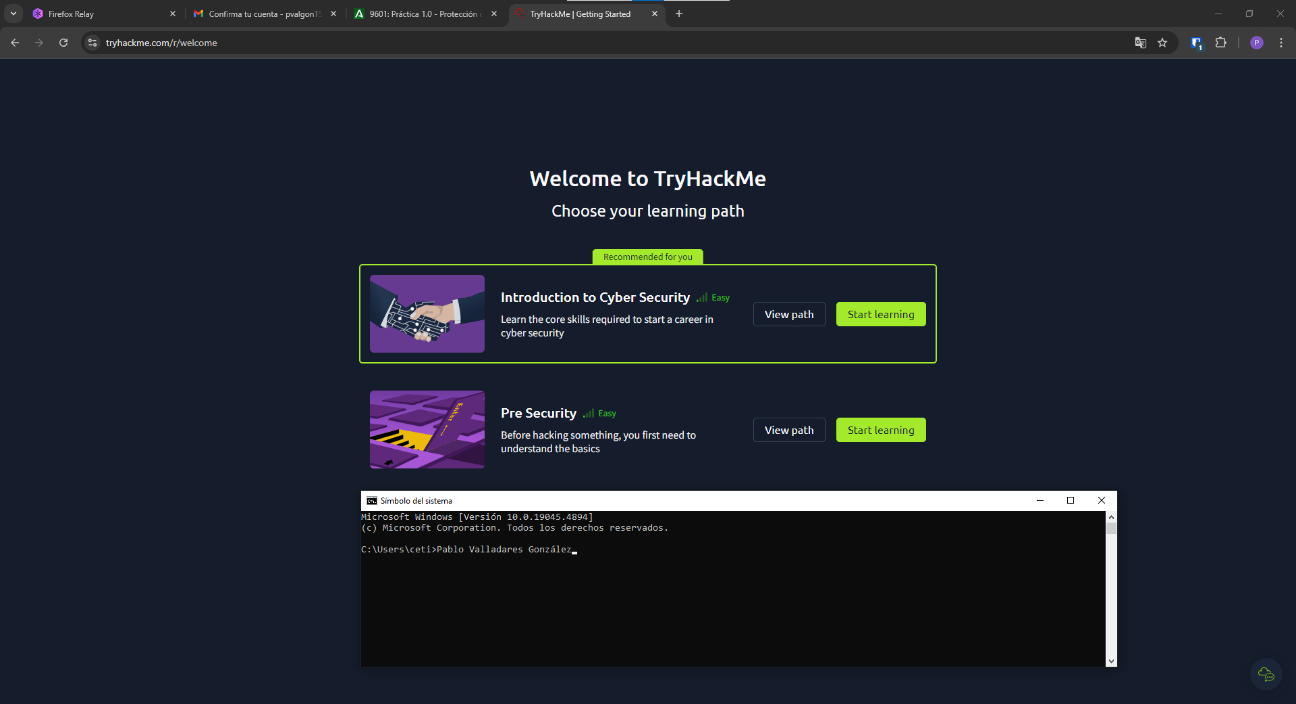
Una vez entremos nos dará una mascara de red a la cual podemos darle un alias a dicha mascara para poder identificar el uso que le vamos a dar a esa mascara.



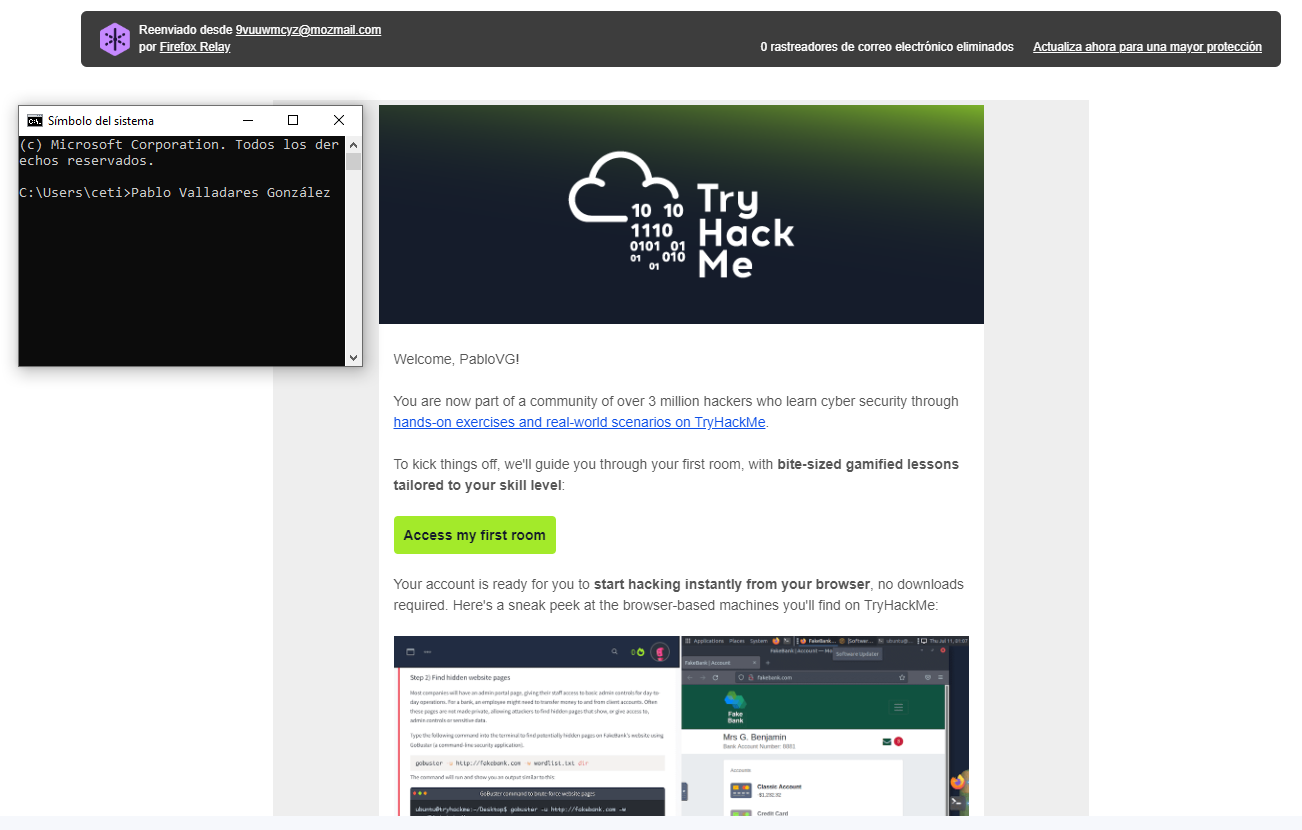
Crearemos la cuenta de Tryhackme, usando la mascara de email que hemos copiado de Firefox y a la hora de crear la contraseña, le daremos al botón que nos aparece en el input el cual nos generara una contraseña el propio Bitwarden, en este caso hay un pequeño problema en este caso y es que el sign up de esta pagina tiene 3 apartados en vez de 2, y Bitwarden solo tiene 2, por lo que tendremos que rellenar uno de ellos a mano, en este caso lo haremos con el generador de alias que esta en el apartado de alias.



Una vez hagamos el login, configuraremos un par de cositas y ya tendremos acceso a la tryhackme



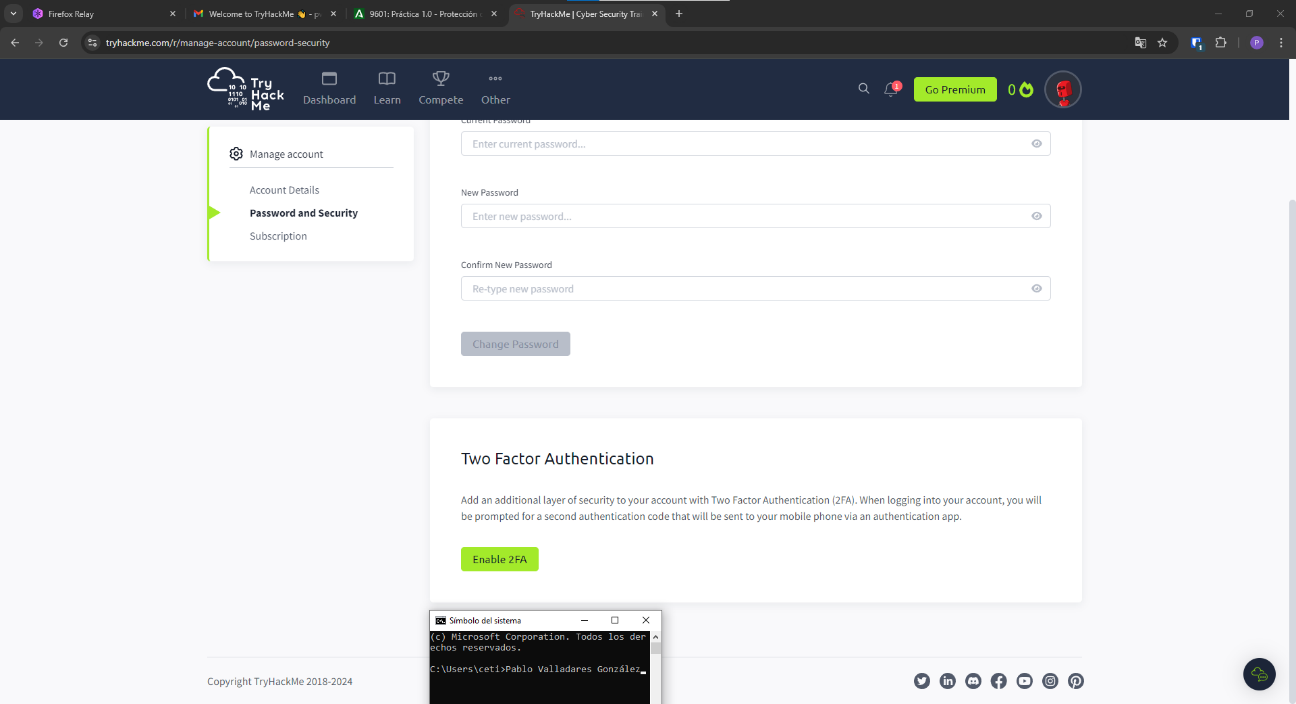
Como podemos ver, el correo en vez de enviárnoslo a nosotros ha sido enviado a la máscara de Firefox relay y este nos lo ha reenviado a nosotros, esto hace que sea mucho mas seguro, ya que si una base de datos sufre un dumpeo, no tendrá acceso a los demás servicios, solamente tendrán acceso a ese correo especifico para esa cosa especifica.



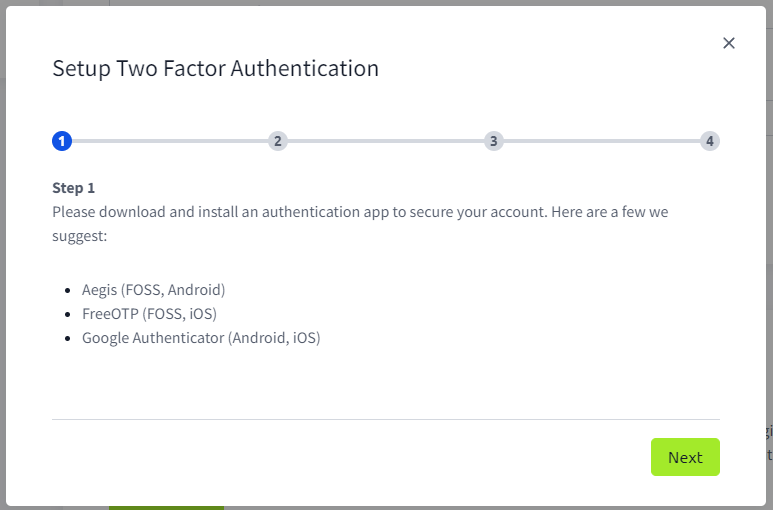
# Ejercicio 6

**Usa aegis (https://play.google.com/store/apps/details?id=com.beemdevelopment.aegis) o FreeOTP (https://apps.apple.com/mx/app/freeotp-authenticator/id872559395) desde tu móvil para activar el 2FA en Tryhackme.**

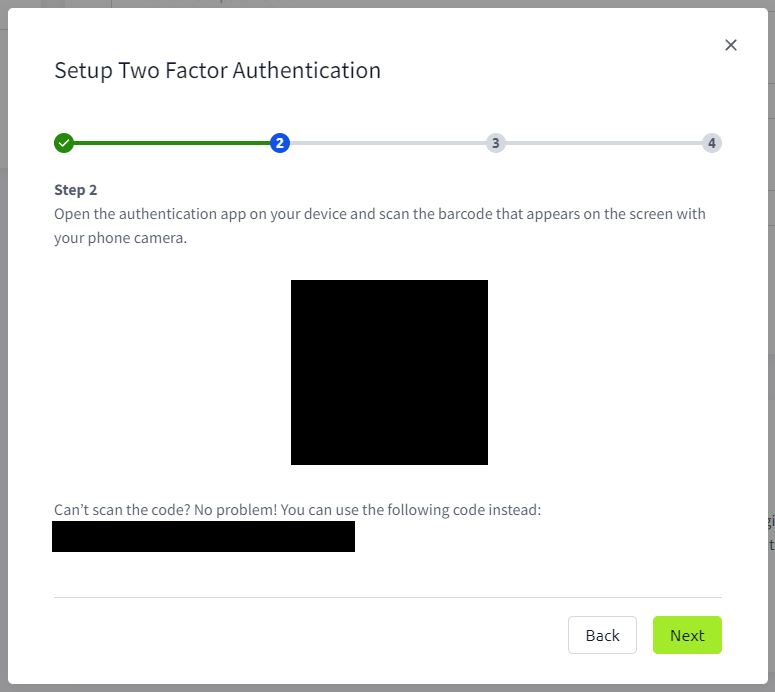
En mi caso voy a utilizar Aegis en mi teléfono, es importante recalcar que como aegis es una aplicación de seguridad esta no permite la realización de capturas de pantalla dentro de dicha aplicación, por lo que todas las capturas serán las que el propio tryhackme nos proporcione para poder realizar la verificación de dos pasos (2FA).



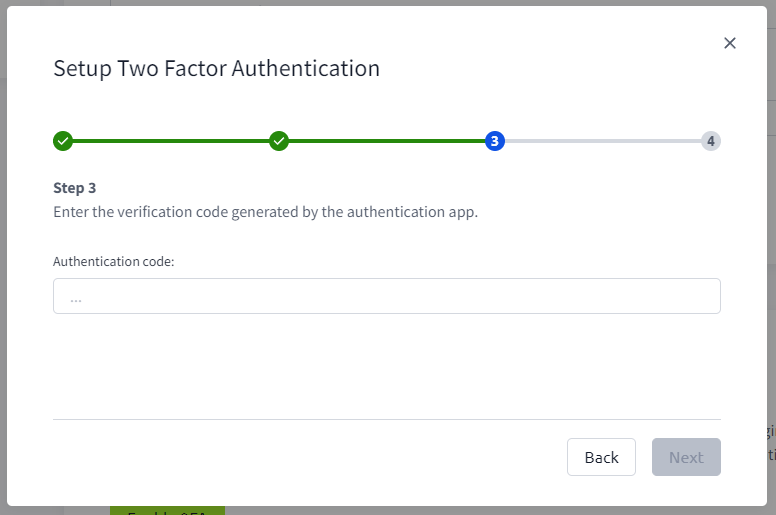
El primer paso nos indicara que necesitamos una aplicación de 2FA, en nuestro caso utilizaremos Aegis, ya que utilizo un teléfono con Android.



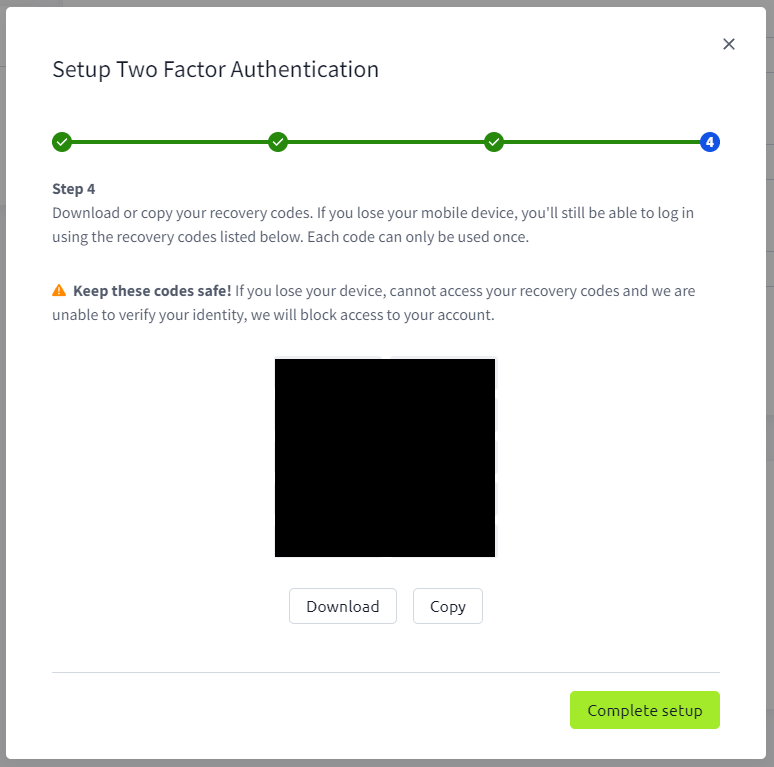
Una vez dentro de la aplicación tendremos que escanear el código QR pulsando en el botón del + abajo a la izquierda en la aplicación.



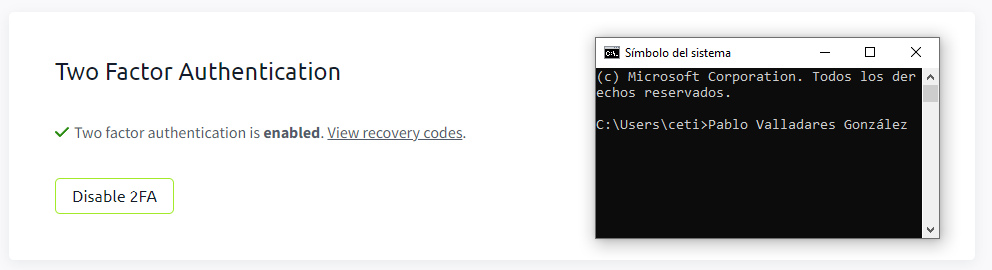
Una vez lo hayamos escaneado, en la aplicación nos aparecerá un logo, el nombre del servicio, el correo asociado y un código el cual va cambiando cada X segundos, deberemos introducir dicho código en la pagina web.



Una vez hecho esto nos darán códigos para la recuperación de dicha pagina.



Una vez lo hayamos activado nos saldrá el siguiente mensaje

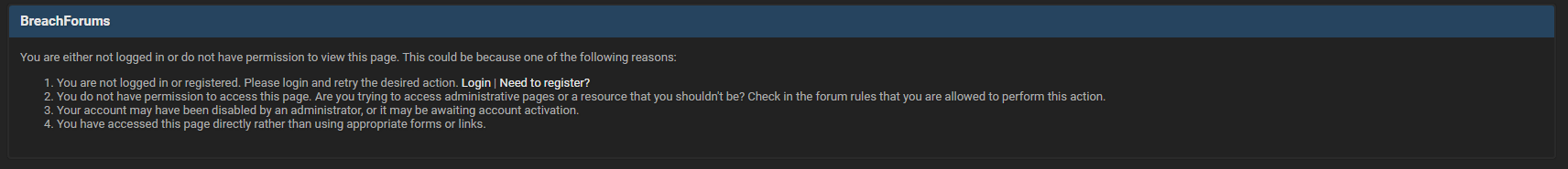


# Actividad Bonus

**Un sitio interesante que investigar y donde suelen publicarse muchas filtraciones es BreachForums. Debido a su naturaleza, el dominio suele cambiar a menudo. Investiga sobre BreachForums (https://en.wikipedia.org/wiki/BreachForums) y busca en el foro filtraciones de información que te llamen la atención (https://breachforums.is/).**

<https://breachforums.st/member?action=login>

Para buscar información en esta pagina debemos de estar logeado



# Conclusión.

Creo que, aunque creamos que estamos seguro por normal general la mayoría de gente no suele utilizar métodos para comprobar como de seguro están, ni revisan si han de cambiar alguna información debido a algún leak. Pienso que la mayoría de gente les gusta vivir sin el miedo a saber de si su información esta comprometida, a utilizar métodos que sea más seguros, aunque sean algo tediosos, hay cosas básicas que la gente no suele cumplir, como el hecho de tener activado siempre el 2FA, usar contraseñas diferentes en cada cosa y tener correos electrónicos separados para cada cosa. Aun así por muchos gestores de contraseña y demás nunca estaremos demasiado seguros ya que el eslabón mas débil de la informática es el ser humano, aunque tengamos demasiada seguridad siempre estaremos acechados por ingeniería social, como por ejemplo “Respiración automática desactivada” o cosas como dejar un posit con la contraseña encima del escritorio, o tirar los papeles con información importante en vez de destrozarlos con una trituradora de papel.

En definitiva, aunque creamos estar muy seguros siempre hay métodos para estarlos aun mas y aunque estemos muy seguro, si queremos vivir una vida normal y corriente podremos ser víctimas de un ataque de ingeniería social ya estar alerta todo el tiempo no es lo habitual en una persona normal corriente.

Con esta tarea he podido apreciar que hay muchas formas de obtener seguridad y estar a salvo de leaks y mantener la información segura aunque suceda algún leak que nos afecte.