



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
 - Tarjetas de crédito 3
 - Correos electrónicos 4
 - Steam Keys 5
 - Bonus 6
- Ejercicio 2..... 8
- Ejercicio 3..... 11
- Ejercicio 4 y Ejercicio 5..... 16
- Ejercicio 6..... 19
- Actividad Bonus..... 21
- Conclusión..... 22

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.

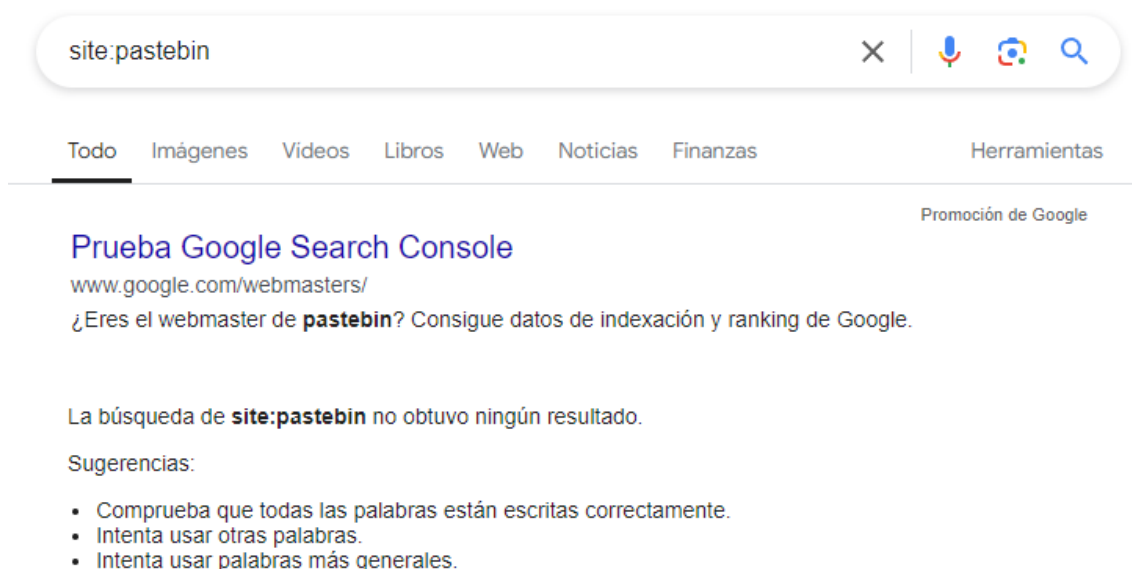
Haz uso de pastebin.com junto con las búsquedas de Google como hemos visto en el tema para buscar y encontrar leaks de correos electrónicos y tarjetas de crédito.

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.



The screenshot shows a Google search interface. The search bar contains the text "site:pastebin". Below the search bar, there are tabs for "Todo", "Imágenes", "Videos", "Libros", "Web", "Noticias", "Finanzas", and "Herramientas". The "Todo" tab is selected. Below the tabs, there is a section titled "Prueba Google Search Console" with the URL "www.google.com/webmasters/" and the text "¿Eres el webmaster de **pastebin**? Consigue datos de indexación y ranking de Google." Below this, there is a message stating "La búsqueda de **site:pastebin** no obtuvo ningún resultado." followed by "Sugerencias:" and a list of three suggestions: "Comprueba que todas las palabras están escritas correctamente.", "Intenta usar otras palabras.", and "Intenta usar palabras más generales."

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 inglés 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)



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`

PASTEBIN API TOOLS FAQ + paste Search... LOGIN SIGN UP

text 3.07 KB | None | 0 0 raw download clone embed print report

Advertisement

1. -----+ CC Info +-----
2.
3. Name of cardholder : Amanda Marrujo
4. Card Type : Visa
5. Card Number : 4653553100057431
6. Expiration Date : 11/2017
7. Card Verification Number: 314
8. Social Security Number : 525856908
9. Bank Routing Number : 112200439
10. Bank Account Number : 576824101
11. -----+ CC Info +-----
12. Name of cardholder : Matthew McElhinn
13. Card Type : Visa
14. Card Number : 4060430342925278
15. Expiration Date : 08/2016
16. Card Verification Number: 471
17. Social Security Number : 209560555
18. Bank Routing Number : 044000037
19. Bank Account Number : 619722671
20.
21. -----+ CC Info +-----
22. Name of cardholder : Phillip Hedges
23. Card Type : MasterCard
24. Card Number : 5175730101580076
25. Expiration Date : 03/2017
26. Card Verification Number: 555
27. Social Security Number : 568253799
28. Bank Routing Number : 121000358
29. Bank Account Number : 325017165529\Secure Code : 8863
30.
31. -----+ CC Info +-----
32. Name of cardholder : Alivia Trinh
33. Card Type : MasterCard
34. Card Number : 5523515370507093
35. Expiration Date : 09/2016

Selecciconar Símbolo del sistema
Microsoft Windows [Versión 10.0.19045.4894]
(c) Microsoft Corporation. Todos los derechos reservados.
C:\Users\ceti>Pablo Valladares González

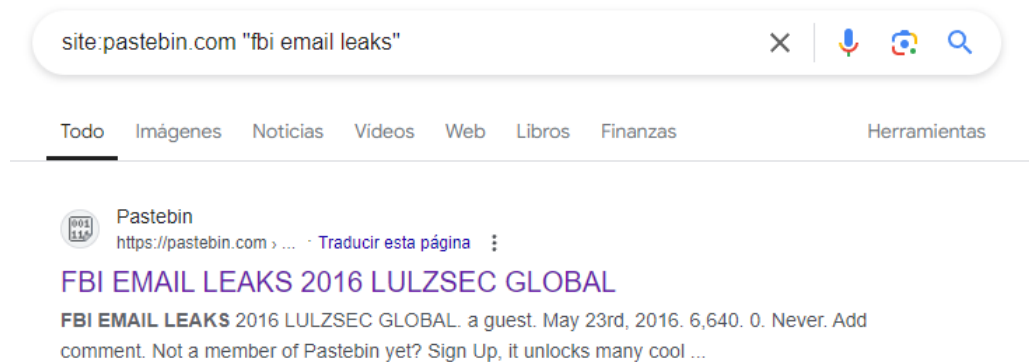
HELLO Not a member of Pastebin yet? Sign Up. it unlocks many cool features!

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)



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

URL: <https://pastebin.com/dwj5BsVU>

PASTEBIN API TOOLS FAQ + paste Search... LOGIN SIGN UP

Advertisement

18. '-----'
19.
20. FBI emails leaked by V01p3r44 (Leader of lulzsec) :
21.
22. [*] %20joyce.smith@ic.fbi.gov
23. [*] -4e377fd3ef7a192693c02bdfc02c1881-larry.freeland@ic.fbi.gov
24. [*] -ad33cfb0dd2097daf26e35a19bddbb4-karen.king@ic.fbi.gov
25. [*] alexis.krieger@ic.fbi.gov
26. [*] angi.christensen@ic.fbi.gov
27. [*] aranda@ic.fbi.gov
28. [*] brian.herrick@ic.fbi.gov
29. [*] buffalo@ic.fbi.gov
30. [*] christina.martinez@ic.fbi.gov
31. [*] christopher.acton@ic.fbi.gov
32. [*] colonial_parkway_murders@ic.fbi.gov
33. [*] cywatch@ic.fbi.gov
34. [*] david.couvertier@ic.fbi.gov
35. [*] erickbolt@ic.fbi.gov
36. [*] fauerso@ic.fbi.gov
37. [*] fbinncp@ic.fbi.gov
38. [*] foipaquestions@ic.fbi.gov
39. [*] foiparequest@ic.fbi.gov
40. [*] ic_complaints@ic.fbi.gov
41. [*] j.colleen.brown@ic.fbi.gov
42. [*] jeffrey.mckinney@ic.fbi.gov
43. [*] john.caruthers@ic.fbi.gov
44. [*] john.tolarski@ic.fbi.gov
45. [*] josephine.vandervoort@ic.fbi.gov
46. [*] joyce.smith@ic.fbi.gov
47. [*] lampo@ic.fbi.gov
48. [*] larry.enmon@ic.fbi.gov
49. [*] larry.wallace@ic.fbi.gov
50. [*] lenka.statistics@ic.fbi.gov
51. [*] linda.f.smith@ic.fbi.gov
52. [*] little.rock@ic.fbi.gov
53. [*] markgiuliano@ic.fbi.gov

Microsoft Windows [Versión 10.0.19045.4894]
(c) Microsoft Corporation. Todos los derechos reservados
C:\Users\ceti>Pablo Valladares González_

Not a member of Pastebin yet?
Sign Up, it unlocks many cool features!

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".

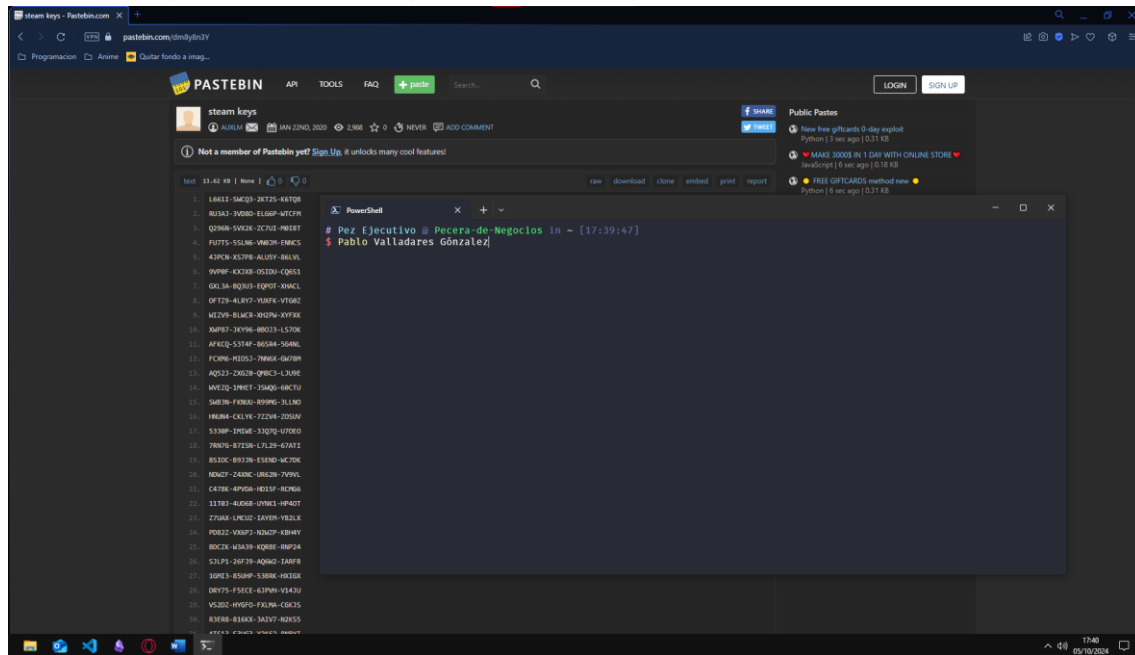
Búsqueda realizada: `site:pastebin.com "steam keys"`

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



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

URL: <https://pastebin.com/dm8y8n3Y>

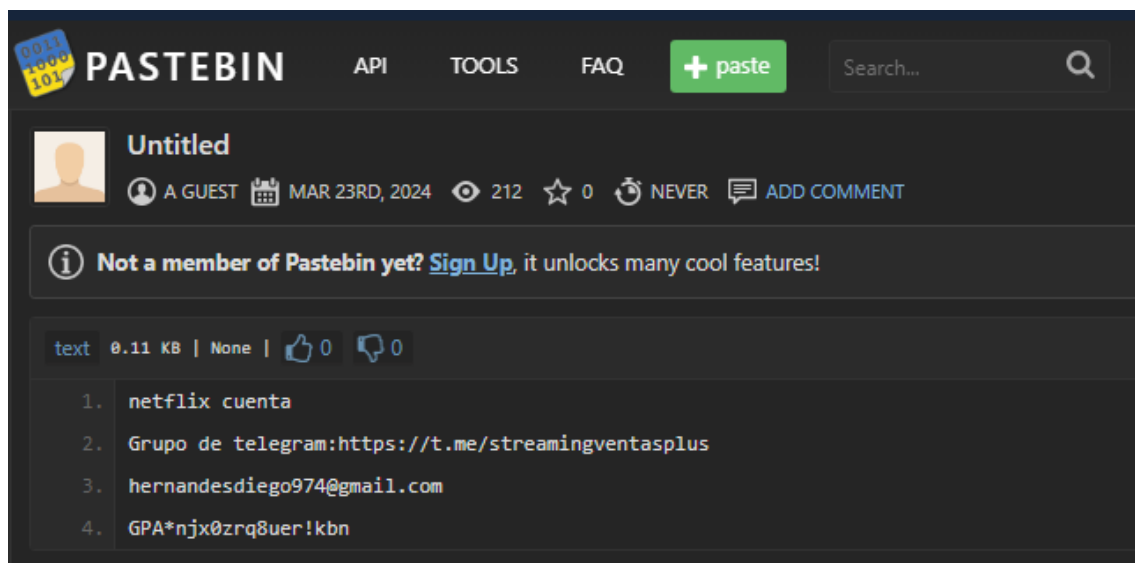


The screenshot shows a Pastebin page titled "steam keys" with a list of 25 Steam keys. A terminal window is open over the list, showing a command prompt with the text "Pez Ejecutivo @ Pecera-de-Negocios in ~ (17:39:47)" and a prompt "\$ Pablo Valladares González".

```
1. L6611-5AC03-2K725-6K708
2. RU343-3V08D-EL66P-WTC0M
3. Q2988-5V62X-2C70E-0M88T
4. RU776-55106-0M82B-EM8C5
5. 43K28-K5708-AL05F-B61VL
6. 9V98P-KK308-05320-C0851
7. 00L3A-BQ303-EQ05T-39AC1
8. OF728-4L8V7-V08F6-VT68Z
9. MEZ09-BLMC8-K02N4-X0F8X
10. XAP87-3K796-88033-L570K
11. AFKQ2-53T4F-86584-S68ML
12. FC096-M2053-7886X-0u70M
13. AQ213-ZML09-Q8C3-L309E
14. ME128-1M8E7-0M82B-0M82U
15. 2M828-F082U-0M82B-3L180
16. H0828-C0L0E-72208-7220V
17. 5338P-1M82E-1302Q-1070D
18. 78070-87258-L7L29-67AT1
19. 8510C-8933N-8510D-4C70K
20. N0M27-2400C-0M82B-7V90U
21. C4708-4P058-8E15F-8C96A
22. 11803-4L058-07083-0P80T
23. Z708A-1M82E-1A70H-Y82LX
24. P0822-V0827-80207-4B84Y
25. 80C28-45839-10848-8AP24
26. 52178-24729-8Q802-1A8F8
27. 10M13-8080P-5388X-8K10X
28. 8R775-F58CE-6398A-V543U
29. V5302-H080F-F0L0A-C0K35
30. 83688-8188X-3A2V7-82655
```

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.



The screenshot shows a Pastebin page titled "Untitled" with a list of 4 items. A terminal window is open over the list, showing a command prompt with the text "Pez Ejecutivo @ Pecera-de-Negocios in ~ (17:39:47)" and a prompt "\$ Pablo Valladares González".

```
1. netflix cuenta
2. Grupo de telegram:https://t.me/streamingventasplus
3. hernandesdiego974@gmail.com
4. GPA*njx0zrq8uer!kbn
```

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

No se ha encontrado ningún resultado para **site:pastebin.com "pablo valladares gonzalez"**.

No se ha encontrado ningún resultado para **site:pastebin.com "valladares gonzalez, pablo"**.

No se ha encontrado ningún resultado para **site:pastebin.com "waterlolbusiness@hotmail.com"**.

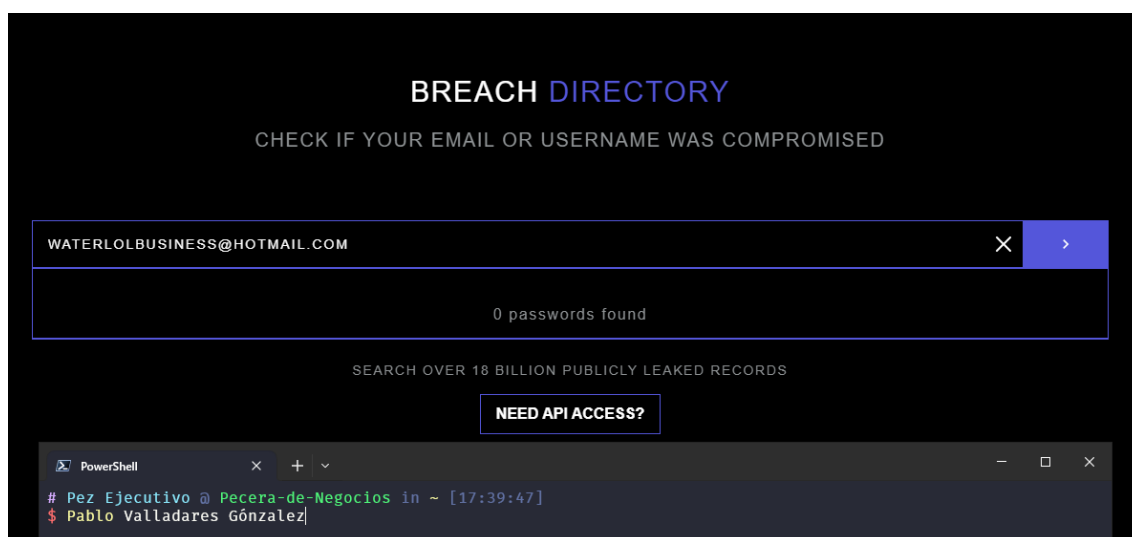
No se ha encontrado ningún resultado para **site:pastebin.com "pvalgon155@g.educaand.es"**.

Ejercicio 2

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

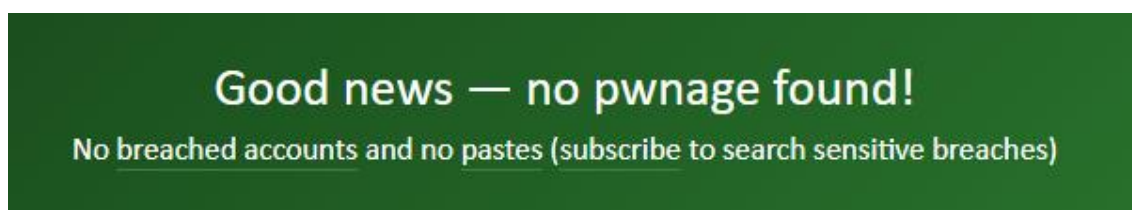
Una alternativa a HavelBeenPwnd es BreachDirectory (<https://breachdirectory.org/>), aunque probablemente la base de datos en la que se basan sea similar.

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



Como las capturas serán principalmente de HavelBeenPwnd, 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:



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-pastado. Además, nos saldrá que información ha sido comprometida en cada caso.


Oh no — pwned!

Pwned in 189 data breaches and found 56 pastes (subscribe to search sensitive breaches)

Facebook Twitter Bitcoin PayPal Donate

Breaches you were pwned in

A "breach" is an incident where data has been unintentionally exposed to the public.



000webhost: In approximately March 2015, the free web hosting provider 000webhost suffered a major data breach that exposed almost 15 million customer records. The data was sold and traded before 000webhost was alerted in October. The breach included names, email addresses and plain text passwords.

Compromised data: Email addresses, IP addresses, Names, Passwords

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: Correo personal y con información importante

waterlolbusiness@hotmail.com pwned?

Good news — no pwnage found!

No breached accounts and no pastes (subscribe to search sensitive breaches)

```
PowerShell
# Pez Ejecutivo @ Pecera-de-Negocios in ~ [17:39:47]
$ Pablo Valladares González
```

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

water111polo@hotmail.com pwned?

Good news — no pwnage found!

No breached accounts and no pastes (subscribe to search sensitive breaches)

```
PowerShell
# Pez Ejecutivo @ Pecera-de-Negocios in ~ [17:39:47]
$ Pablo Valladares González
```

valladaresgonzalezpablo@hotmail.com: Correo utilizado para temas de trabajo y búsqueda de empleo:

valladaresgonzalezpablo@hotmail.com **pwned?**

Good news — no pwnage found!

No breached accounts and no pastes (subscribe to search sensitive breaches)

```
PowerShell
# Pez Ejecutivo @ Pecera-de-Negocios in ~ [17:39:47]
$ Pablo Valladares González
```

waterargentino@hotmail.com: Correo con ID de origen argentino para la compra de productos con divisa argentina.

waterargentino@hotmail.com **pwned?**

Good news — no pwnage found!

No breached accounts and no pastes (subscribe to search sensitive breaches)

```
PowerShell
# Pez Ejecutivo @ Pecera-de-Negocios in ~ [17:39:47]
$ Pablo Valladares González
```

pvalgon155@g.educaand.es: Correo utilizado para las actividades y tareas de clase.

pvalgon155@g.educaand.es **pwned?**

Good news — no pwnage found!

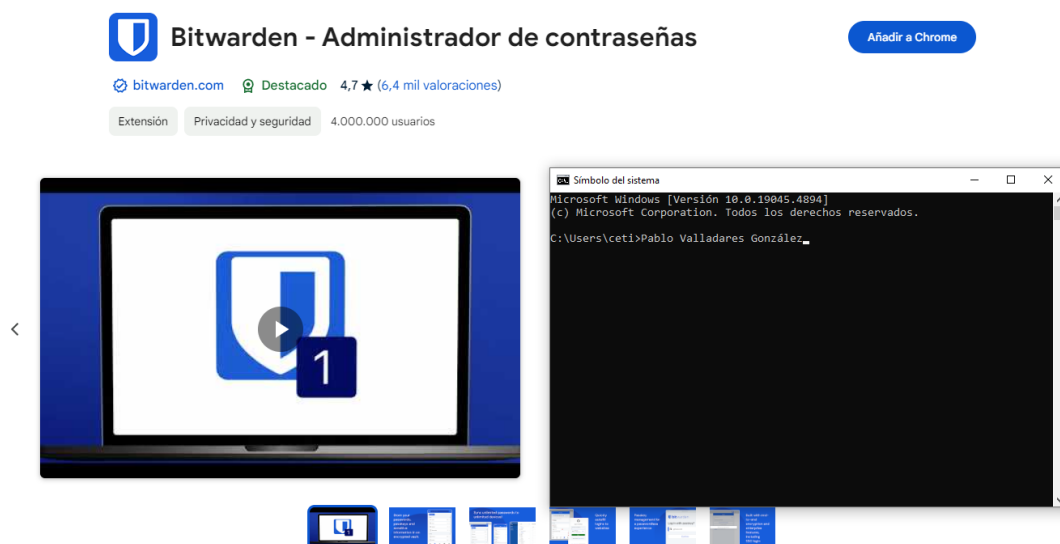
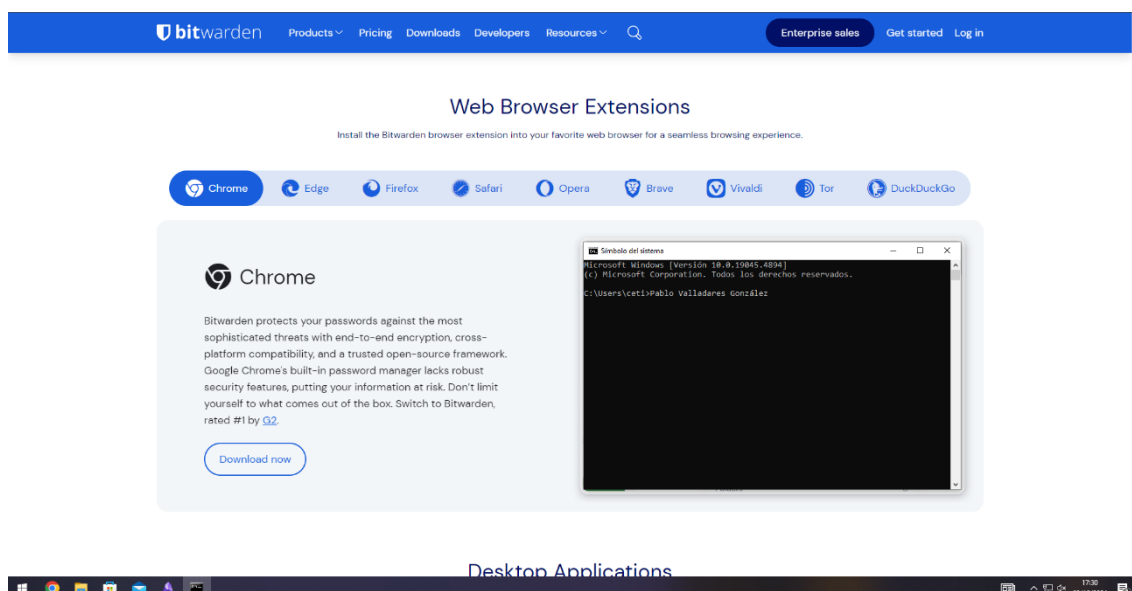
No breached accounts and no pastes (subscribe to search sensitive breaches)

```
PowerShell
# Pez Ejecutivo @ Pecera-de-Negocios in ~ [17:39:47]
$ Pablo Valladares González
```

Ejercicio 3

Crea una cuenta en Bitwarden.com. Instala la extensión en tu navegador (<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.



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).

Cancelar Crear cuenta Enviar

Correo electrónico
pvalgon155@g.educaand.es

Contraseña maestra **Fuerte**

.....

Importante: Tu contraseña maestra no se puede recuperar si la olvidas 12 caracteres mínimo

Vuelve a escribir tu contraseña maestra

.....

Pista de contraseña maestra (opcional)
En el puesto de trabajo

Una pista de tu contraseña maestra puede ayudarte a recordarla en caso de que la olvides.

☒ Comprobar filtración de datos conocidos para esta contraseña

Al seleccionar esta casilla, acepta lo siguiente:

☒ Términos y condiciones del servicio, Política de privacidad

Microsoft Windows [Versión 10.0.19045.4894]
(c) Microsoft Corporation. Todos los derechos reservados.
C:\Users\ceti>Pablo Valladares González_

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).

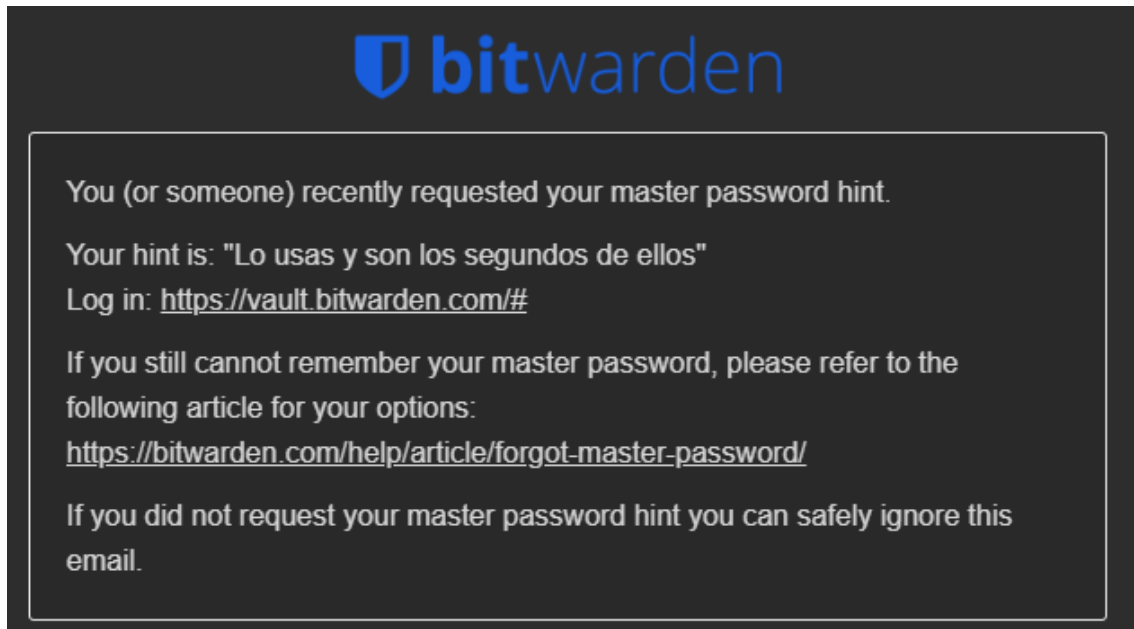
Ejemplo:

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

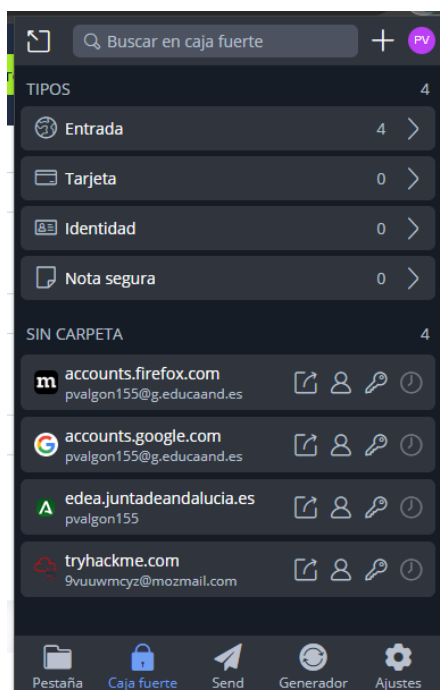
BW#SEGURIDAD-gestor.12 – Cuenta para BitWarden.

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

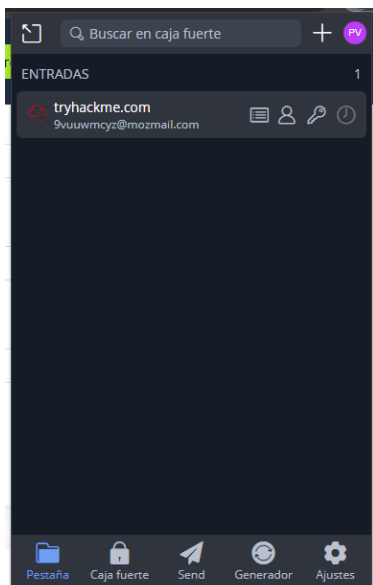
En el caso de que añadamos una pista de contraseña, cuando la necesitemos, en vez de mostrárnosla directamente lo que hará es pedirnos que introduzcamos el correo para que nos envíen a él la pista de la contraseña. Deberás usar una pista que entiendas pero que no de demasiada información, aun así, con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



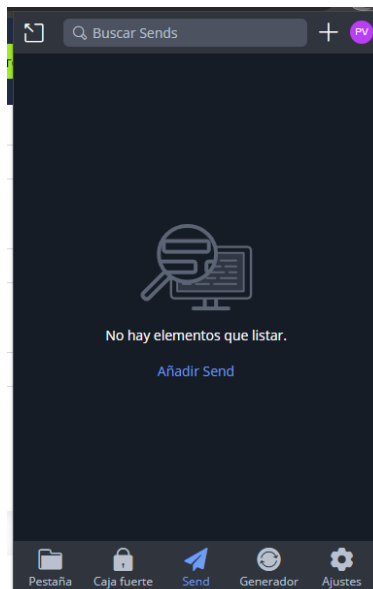
Bitwarden tiene una serie de pestañas que tienen usos diferentes:



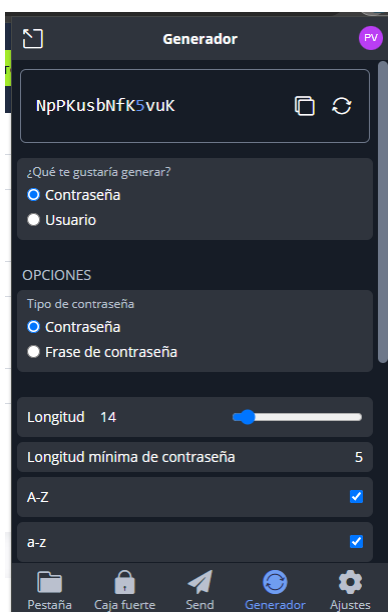
En la caja fuerte nos aparece todos los correos que tengamos asociados con Bitwarden, además de la cantidad de cada tipo que tenemos y la papelera.



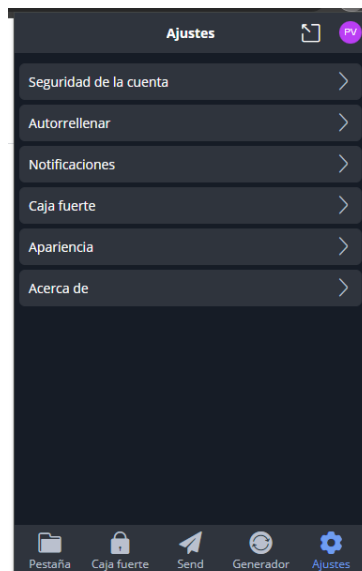
En la pestaña aparecerán todas las entradas/tarjetas/identidad que estén asociadas a la pestaña que tengas abierta actualmente en google.



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



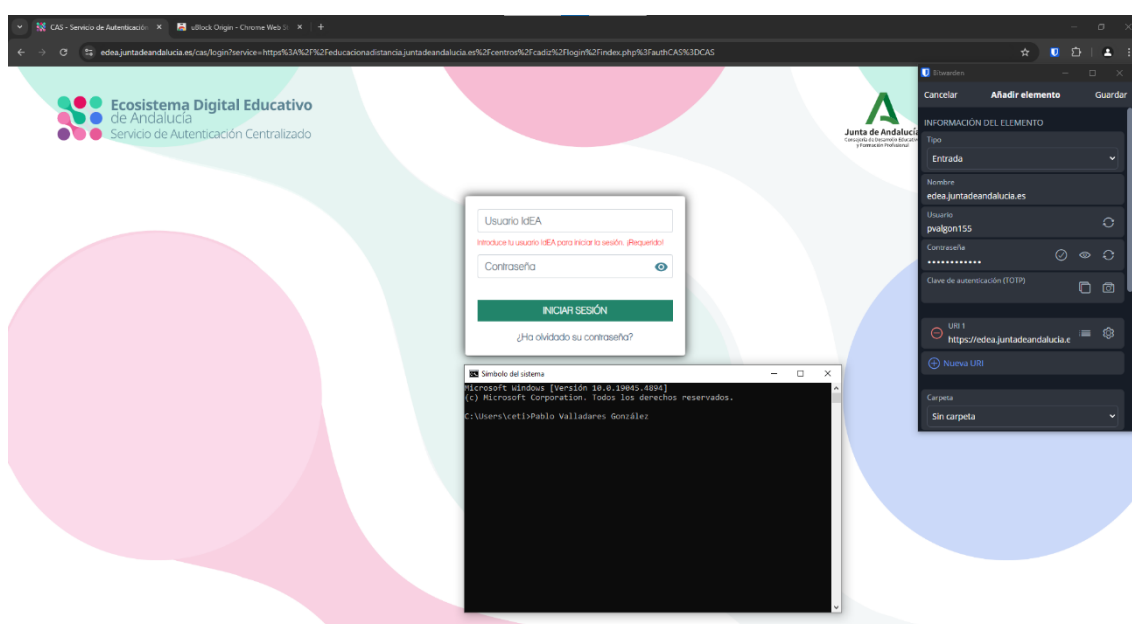
En Generador, podremos generar contraseñas automáticamente con las características que marquemos, además de poder generar un alias de usuario por si no queremos usar el nuestro.



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.


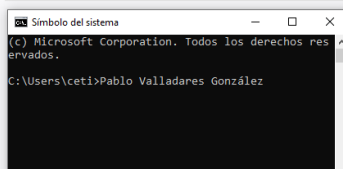
Ejercicio 4 y Ejercicio 5

Crea una cuenta en Firefox y usa Firefox Relay (<https://relay.firefox.com/>).

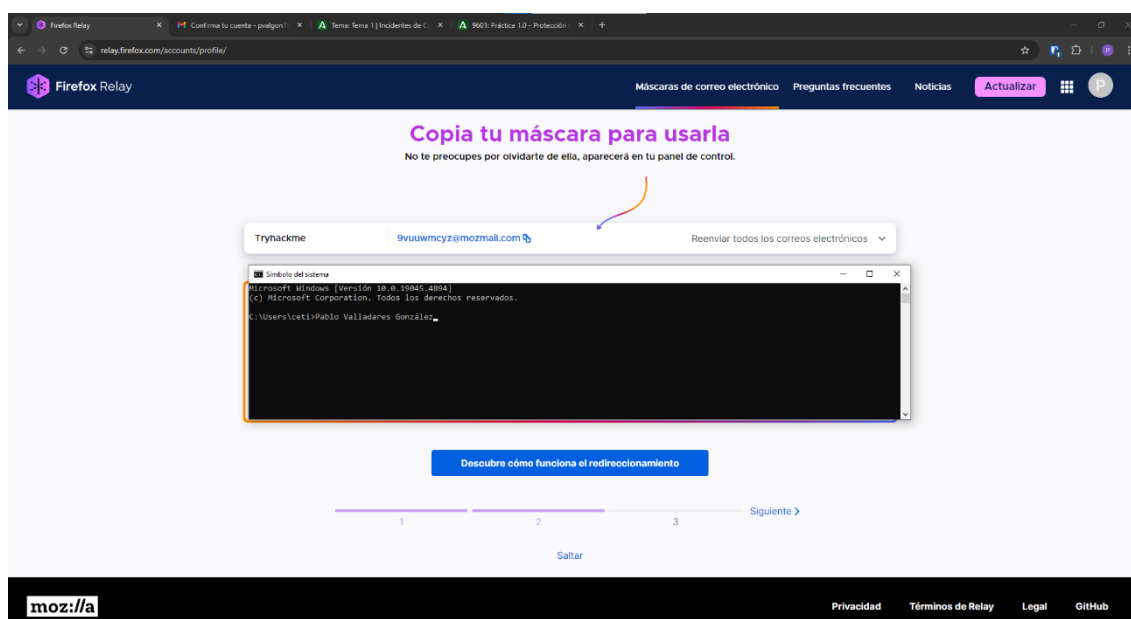
Crea una cuenta en tryhackme con un alias de firefox relay y generando una contraseña con bitwarden. Almacena la contraseña en bitwarden.

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.

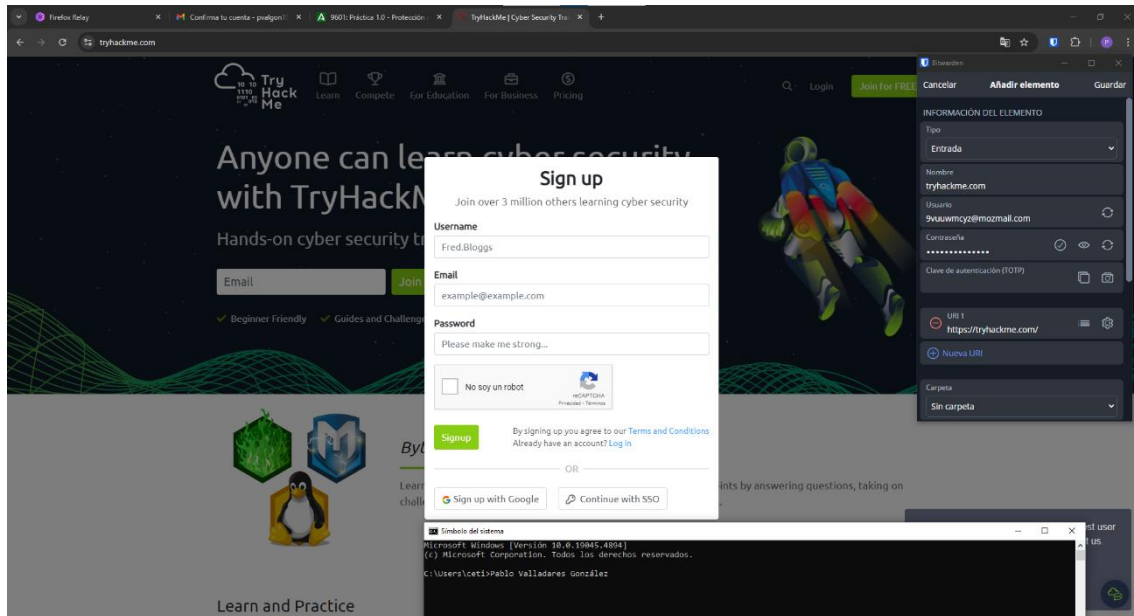
Iremos a descargar Firefox Relay, la versión gratuita la cual te da 5 mascaras de email.

Características	Protección de correo electrónico limitada	Protección de correo electrónico	Protección de correo electrónico y teléfono	Añadir la protección VPN
Máscaras de correo electrónico para proteger tu dirección de correo electrónico real	5	Ilimitado	Ilimitado	Ilimitado
Extensión de navegador para usar Relay en cualquier sitio	✓	✓	✓	✓
Eliminar rastreadores de correo electrónico	✓	✓	✓	✓
Bloquear correos promocionales		✓	✓	✓
Dominio de correo electrónico Relay para crear máscaras sobre la marcha		✓	✓	✓
Responder correos electrónicos de forma anónima		✓	✓	✓
Enmascaramiento de números de teléfono para proteger tu número real			✓	✓
Protección VPN con 				✓
	Gratis Obtén Relay	Anualmente Mensual 0,99 €/mes Regístrate <small>Facturado anualmente</small>	Únete a la lista de espera <small>Facturado mensualmente</small>	Únete a la lista de espera <small>Facturado mensualmente</small>

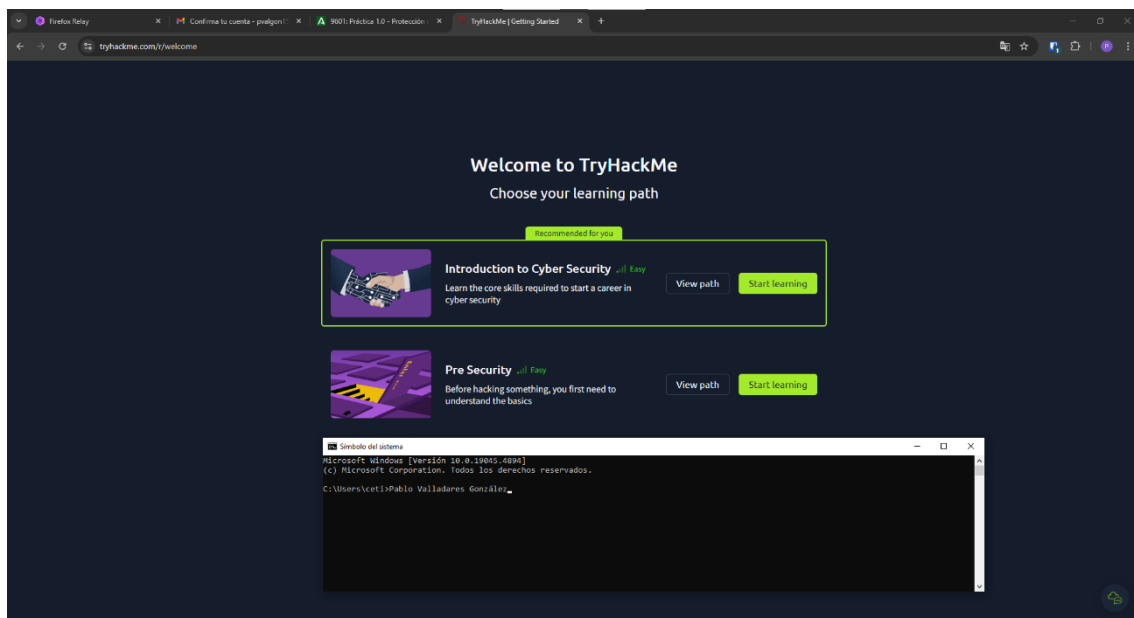
Una vez entremos nos dará una máscara de red a la cual podemos darle un alias a dicha máscara para poder identificar el uso que le vamos a dar a esa máscara.



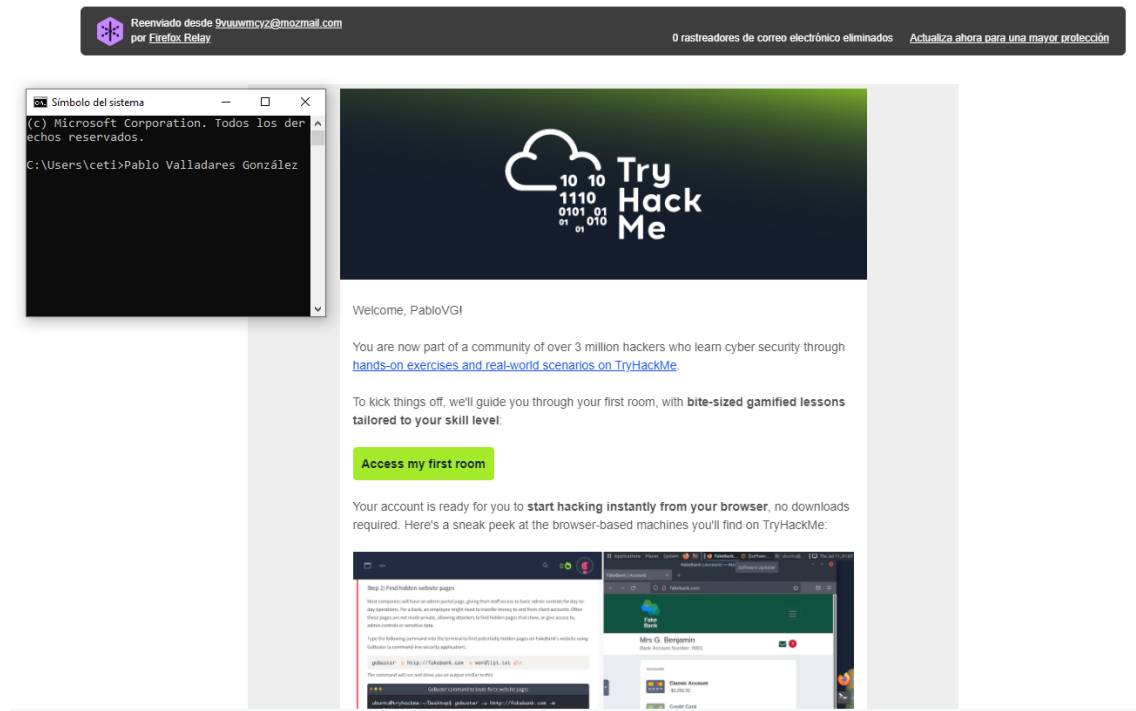
Crearemos la cuenta de Tryhackme, usando la mascara de email que hemos copiado de Firefox y a la hora de crear la contraseña, le daremos al botón que nos aparece en el input el cual nos generara una contraseña el propio Bitwarden, en este caso hay un pequeño problema en este caso y es que el sign up 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.



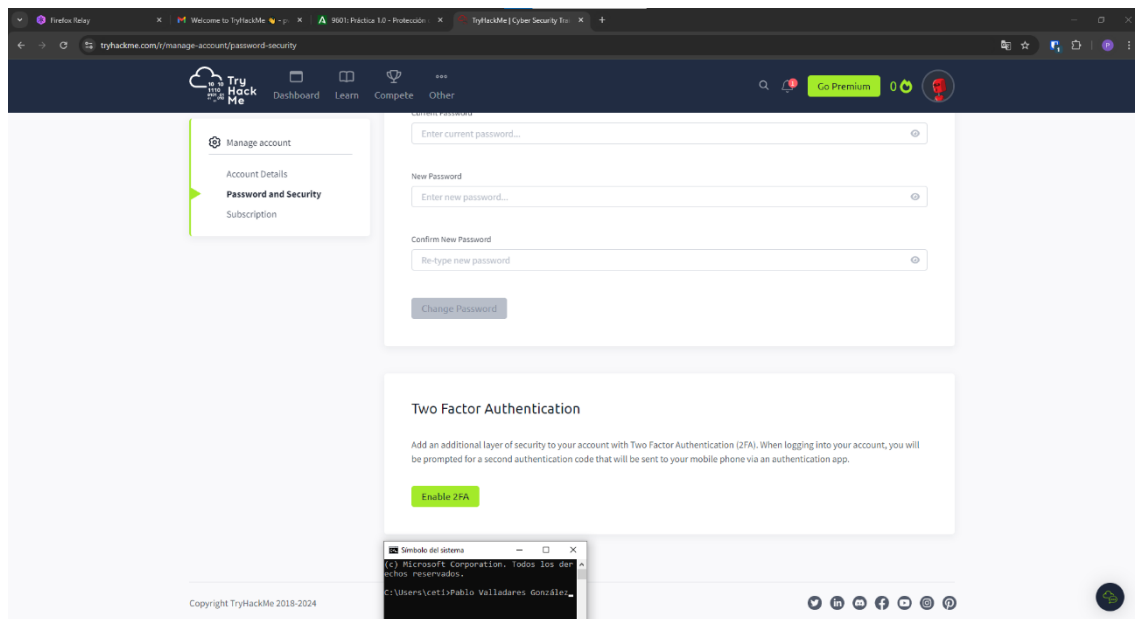
Ejercicio 6

Usa aegis

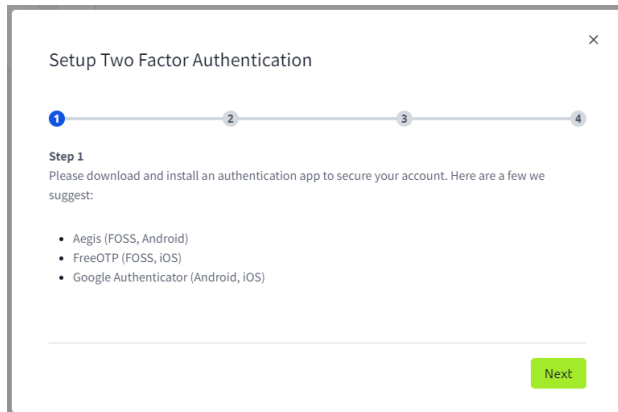
(<https://play.google.com/store/apps/details?id=com.beemdevelopment.aegis>) o

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.



Setup Two Factor Authentication

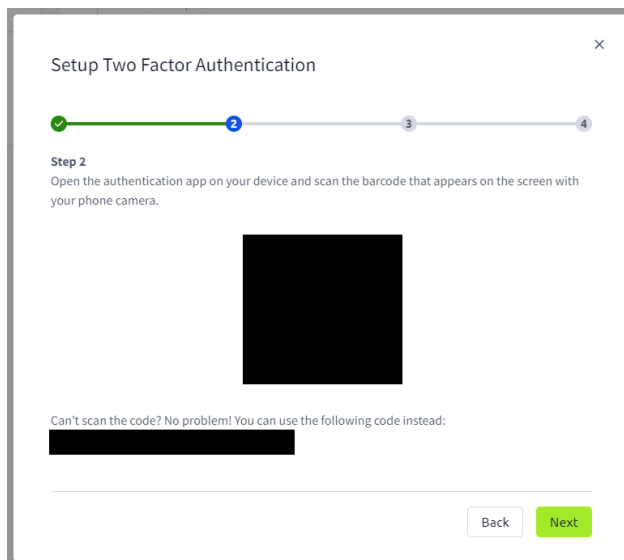
1 2 3 4

Step 1
Please download and install an authentication app to secure your account. Here are a few we suggest:

- Aegis (FOSS, Android)
- FreeOTP (FOSS, iOS)
- Google Authenticator (Android, iOS)

Next

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



Setup Two Factor Authentication

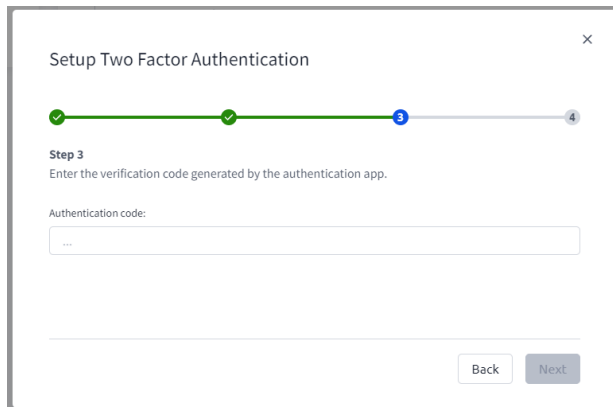
1 2 3 4

Step 2
Open the authentication app on your device and scan the barcode that appears on the screen with your phone camera.

Can't scan the code? No problem! You can use the following code instead:

Back Next

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.



Setup Two Factor Authentication

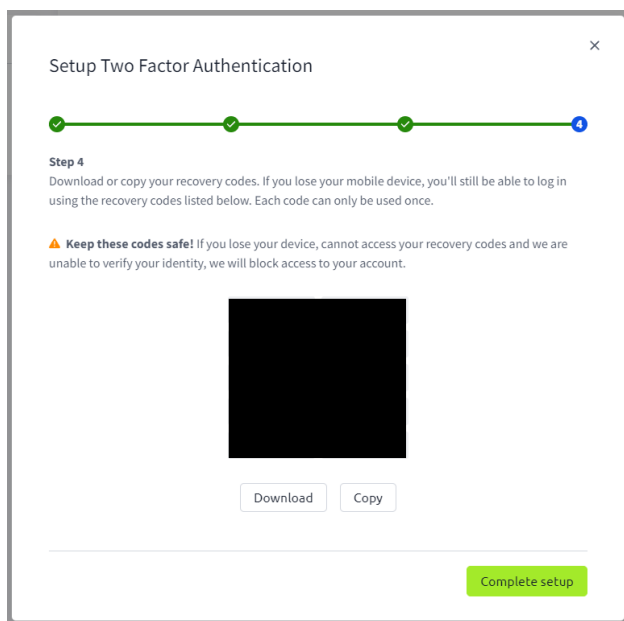
1 2 3 4

Step 3
Enter the verification code generated by the authentication app.

Authentication code:

Back Next

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



Una vez lo hayamos activado nos saldrá el siguiente mensaje

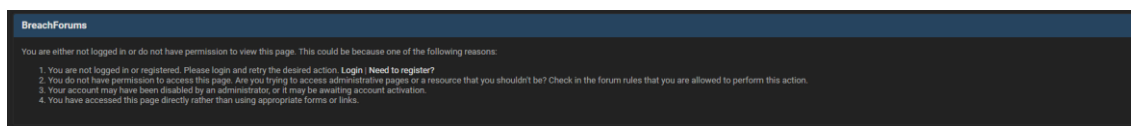


Actividad Bonus

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 posito con la contraseña encima del escritorio, o tirar los papeles con información importante en vez de destruirlos 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.