INVACI

INSTITUTO VALENCIANO

DE CIBERSEGURIDAD Y TELEMÁTICA

EBOOK GRATUITO

Aprende a identificar un ataque de phishing

www.invaci.es

ÍNDICE

I. INTRODUCCIÓN

Introducción 4
Qué es el phishing 5
En qué se basa el phishing 6
Cómo reconocer el phishing 7
Métodos de propagación 7

II. EJEMPLOS REALES

Phishing Agencia Tributaria 7
Phishing DGT 9
Phishing BBVA 10
Phishing Correos 11

III. HERRAMIENTAS 11

VirusTotal 12
HavelbeenPwned 15
DeHashed 17

IV. CONCLUSIONES 18

I. INTRODUCCION

Hoy presentamos un ebook que detalla cómo identificar los principales patrones presentes en los ataques de phishing.

Además, aprenderás herramientas fundamentales para verificar la legitimidad de los sitios web donde introduces tus datos, asegurando la protección de tu información personal y/o corporativa.

APRENDE A IDENTIFICAR UN ATAQUE DE PHISHING

¿Qué es el phishing?

Técnica utilizada para obtener datos valiosos del usuario que los atacantes pueden vender o utilizar indebidamente con fines nefastos como:

- Extorsión
- Robo monetario
- Suplantación de identidad

La forma más común de phishing consiste en suplantar la identidad de un banco o institución financiera a través de correos electrónicos con el objetivo de inducir a la víctima a completar un formulario fraudulento adjunto al mensaje o a acceder a un sitio web que solicita información confidencial, como datos de la cuenta o credenciales de inicio de sesión.

APRENDE A IDENTIFICAR UN ATAQUE DE PHISHING

¿En qué se basa el phishing?

El phishing se aprovecha de la curiosidad inherente al ser humano.

Por ejemplo, si una memoria USB aparentemente olvidada se encontrara cerca de la cafetera en la zona de descanso de la empresa o en la entrada de la oficina,

¿cuánto tiempo pasaría antes de que alguien la conectara a su ordenador para ver su contenido?

¿Qué sucedería si el USB contuviera un archivo de Excel titulado "nominafeb2023.xls"?

Muchas personas sucumbirían a la tentación de conocer el salario de un colega y abrirían el archivo. Este escenario ilustra los aspectos psicológicos que los ciberdelincuentes aprovechan mediante técnicas de ingeniería social.

Es importante señalar que los ataques tipo phishing utilizan las técnicas de ingeniería social cada vez má depuradas para aumentar su aparente autenticidad..

APRENDE A IDENTIFICAR UN ATAQUE DE PHISHING

¿Cómo reconocer el phishing?

Vamos a incluir aquí varios puntos que generalmente cumplen los ataques de phishing y que nos permitirán identificar dichos patrones para detectarlos.

- SALUDOS GENÉRICOS O INFORMALES
- SOLICITUD DE INFORMACIÓN PERSONAL
- SENSACIÓN DE URGENCIA
- GRAMÁTICA POBRE
- CORRESPONDENCIA INESPERADA
- DOMINIO SOSPECHOSO
- OFERTA U OPORTUNIDAD DEMASIADO BUENA

APRENDE A IDENTIFICAR UN ATAQUE DE PHISHING

Método de propagación de phishing

Habituamente los ataques de phishing utilizan para su propagación el correo electrónico, aunque también es habitual, sobre todo en campañas tipo, la declaración de la renta, el blackfriday, etc. utilizar mensajes de SMS para su propagación.

II. EJEMPLOS REALES

Phishing Agencia Tributaria

Como hemos comentado anteriormente, los ciberdelincuentes suelen utilizar las épocas en las que existen campañas tipo la declaración de la renta, blackfriday, navidades, etc. para asegurarse un público potencial mucho mayor en sus estafas.

Como vemos en los dos próximos ejemplos, en ambos se cumplen varios de los patrones indicados anteriormente.

Agencia Tributaria NOTIFICACION POSTAL

AT Agencia Tributaria <agencia-tributaria-es@e-sochog.cl>
Para oscar@oscarpadial.com

Responder | Responder a todos | Reenviar | ...
Wed 7/19/2023 4:04 PM

ESTE EMAIL SE CORRESPONDE CON UN AVISO DE UNA NOTIFICACIÓN POSTAL.

Le informamos que está disponible una nueva notificación para Titular con los siguientes datos:

- Titular oscar@oscarpadial.com
- Organismo emisor: Agencia Estatal de Administración Tributaria, con DIR3: EA0028512
- Identificador: 2294032215794
- Concepto: Notificación administrativa
- Vínculo: Titular

Puede acceder a esta notificación en la Dirección Electrónica Habilitada Única (DEHÚ) del Punto de Acceso General, disponible en: agenciatributaria.gob.es

Le facilitamos un enlace directo a la notificación.

Esta notificación se facilita por vía electrónica de acuerdo con lo previsto en el artículo 42.1 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, que establece la obligatoriedad para los organismos emisores de poner por vía electrónica las notificaciones que se emitan en papel.

La notificación se recibirá en todo caso en papel, aplicándose los plazos que en la misma se indiquen. Adicionalmente podrá recibir esta notificación por distintas vías electrónicas. Si accediera a su contenido por más de una de estas vías, sepa que los efectos jurídicos, si los hubiera, siempre empiezan a contar desde la fecha en que se produzca su primer acceso.

Gobierno de España

BLOQUEO JUDICIAL - Pendiente financiera - [id 186091682]

AT Administracion Tributaria <impuestos@hacienda.gob.es>
Para oscar@oscarpadial.com

Responder | Responder a todos | Reenviar | ...
lu. 31/08/2020 3:43

Los vínculos y algunas otras funciones se han deshabilitado en este mensaje. Para restaurar la función, mueva este mensaje a la Bandeja de entrada.
Haga clic aquí para descargar imágenes. Para ayudarle a proteger su confidencialidad, Outlook ha impedido la descarga automática de algunas imágenes en este mensaje.

Descargar todo como.zip archivos adjuntos (128 kb)

se anexa el seguiente comprobante fiscal digital

Remitente: Servicio de AdministraciÃ³n Tributaria.

Hemos identificado que tienes pendiente de presentar, al 01 de agosto de 2020, lo siguiente:

A quien corresponda

SERIE Y FOLIO:	2158945
FECHA DE EMISION:	01/08/2020
MONTO TOTAL:	9522.20

Servicio de AdministraciÃ³n Tributaria,
+35 1308 808 500 Capitales y Ãreas metropolitanas

APRENDE A IDENTIFICAR UN ATAQUE DE PHISHING

Phishing DGT

La Dirección General de Tráfico es también una de las entidades que utilizan los ciberdelincuentes para suplantar su identidad y “pescar” datos confidenciales.

El caso de las multas de la DGT es uno de los casos que también utilizan bastante la propagación mediante SMS.

De: Ministerio del Interior <notificaciones@dgt.ggobs.es>
Enviado el: miércoles, 18 de mayo de 2022 9:39
Para: oscar@oscarpadial.com
Asunto: MULTA NO PAGADA - [id 190743660]

DGT Dirección General de Tráfico
GOBIERNO DE ESPAÑA
MINISTERIO DEL INTERIOR

SALUDOS CORDIALES

Tienes una multa pendiente

Se ha identificado en nuestro sistema una multa de trafico no pagada dirigida a usted o su vehiculo.

Para ver la notificacion
Visite:

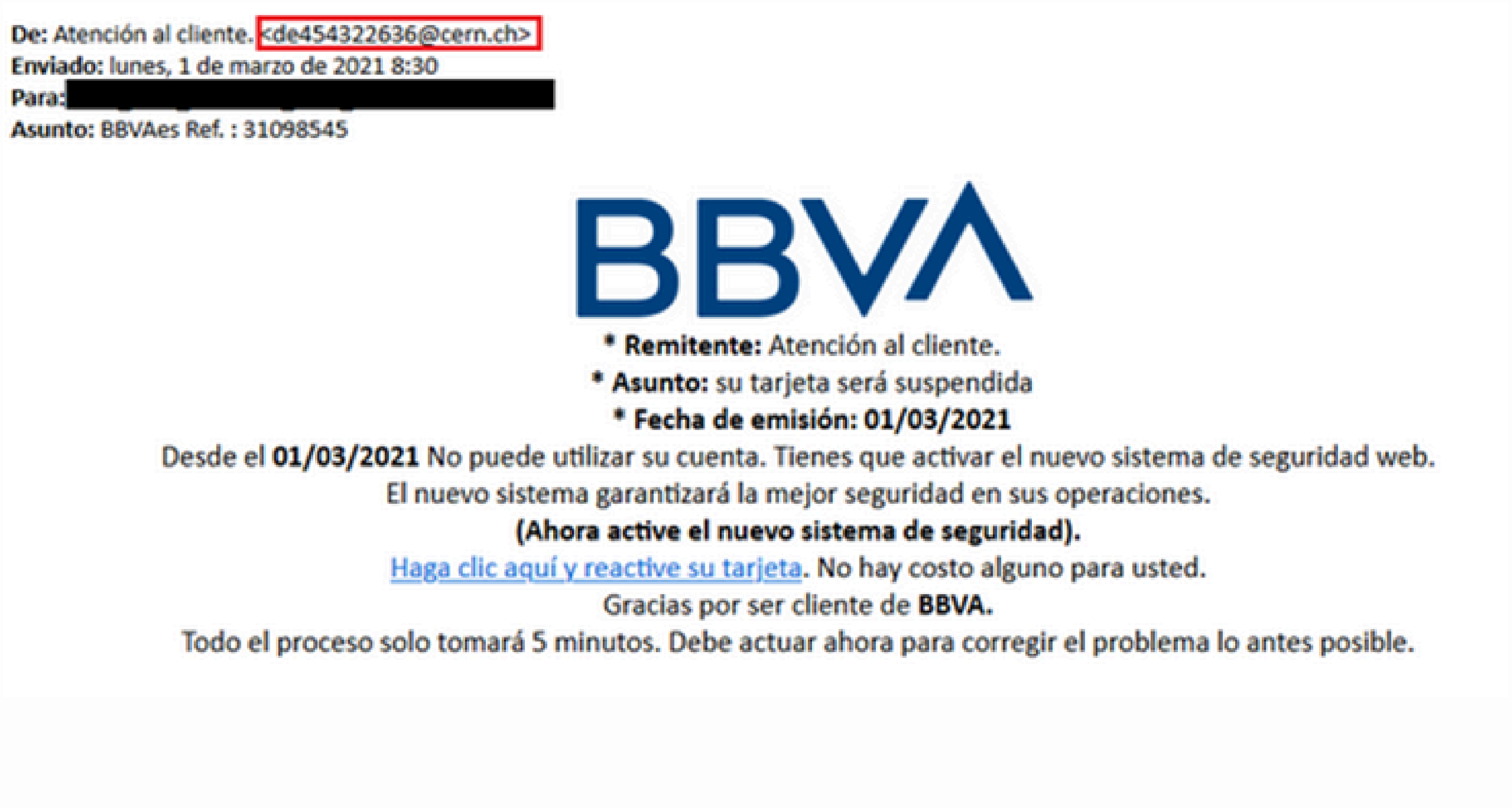
Acceso a mi DGT

Atencion:

Para ver la notificacion, abra en un sistema (Windows).

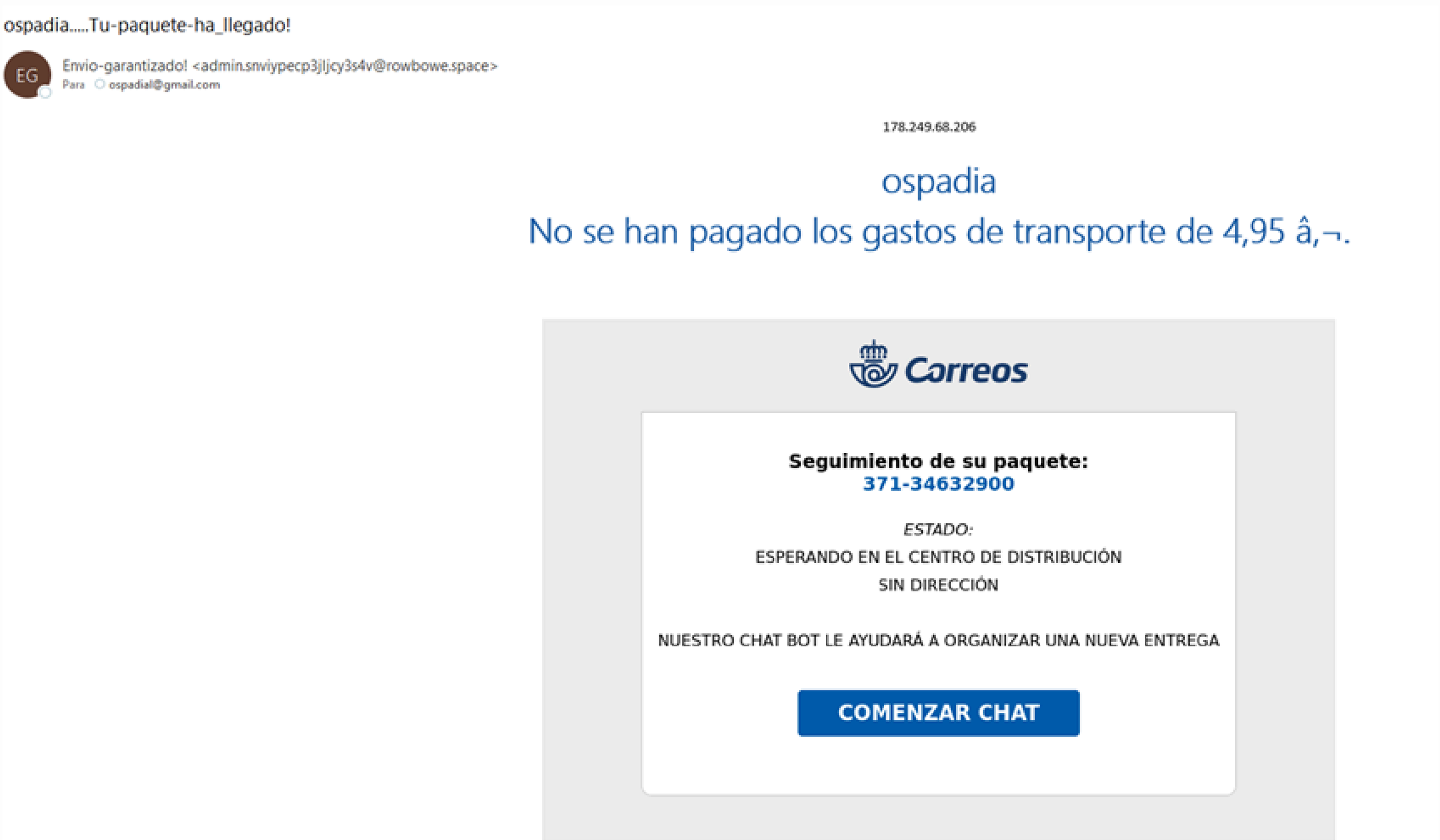
APRENDE A IDENTIFICAR UN ATAQUE DE PHISHING

Phishing BBVA



APRENDE A IDENTIFICAR UN ATAQUE DE PHISHING

Phishing Correos



III. HERRAMIENTAS

Después de ver varios ejemplos y las pautas para identificarlos vamos a hablar ahora de las herramientas que nos ayudarán a asegurarnos en caso de duda de si el enlace al que accedemos es correcto o por el contrario es una web ilícita que pretende robar nuestros datos.

VirusTotal

La primera herramienta de la que hablaremos es VirusTotal que nos ayudará de una manera muy sencilla a comprobar que un enlace es o no legítimo.

Para ilustrar su funcionamiento con un ejemplo real, vamos a utilizar el que hemos visto anteriormente de la DGT (aunque serviría cualquiera de ellos):

De: Ministerio del Interior <notificaciones@dgt.ggobs.es>
Enviado el: miércoles, 18 de mayo de 2022 9:39
Para: oscar@oscarpadial.com
Asunto: MULTA NO PAGADA - [id 190743660]

DGT Dirección General de Tráfico | GOBIERNO DE ESPAÑA | MINISTERIO DEL INTERIOR

SALUDOS CORDIALES

Tienes una multa pendiente

Se ha identificado en nuestro sistema una multa de trafico no pagada dirigida a usted o su vehiculo.

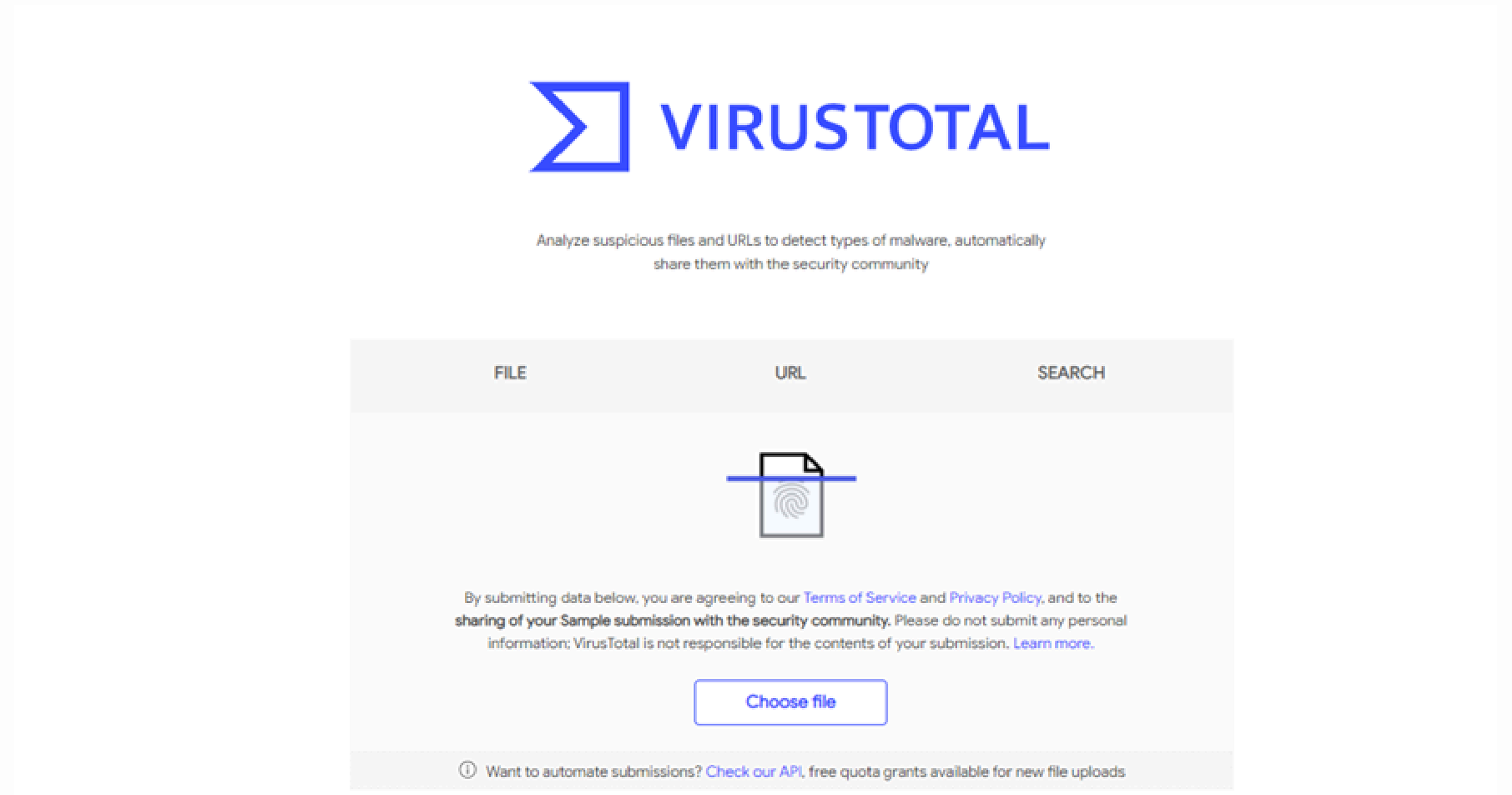
Para ver la notificacion
Visite:

Acceso a mi DGT

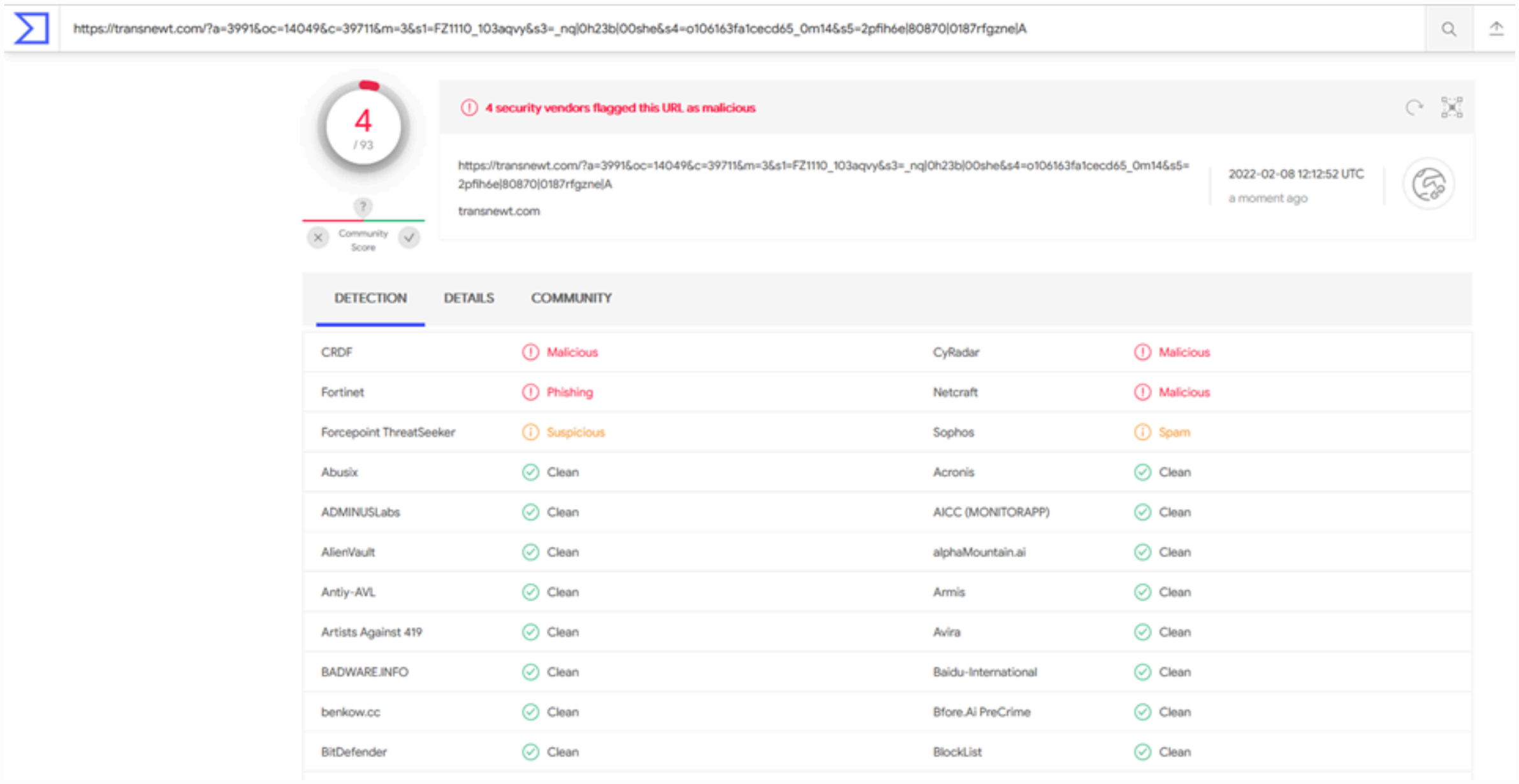
Atencion:

Para ver la notificacion, abra en un sistema (Windows).

Como vemos en este caso el enlace es el botón de “Acceso a mi DGT”.
Lo que debemos hacer es pulsar sobre el botón (o enlace) con el botón derecho del ratón, le damos a copiar hipervínculo y luego lo pegaremos en la web de VirusTotal para analizarlo:



Como vemos en VirusTotal podemos analizar tanto un fichero como una URL o dirección web.
En este caso pegamos la dirección obtenida anteriormente en el apartado URL y le damos a “enter” para que lo analice.



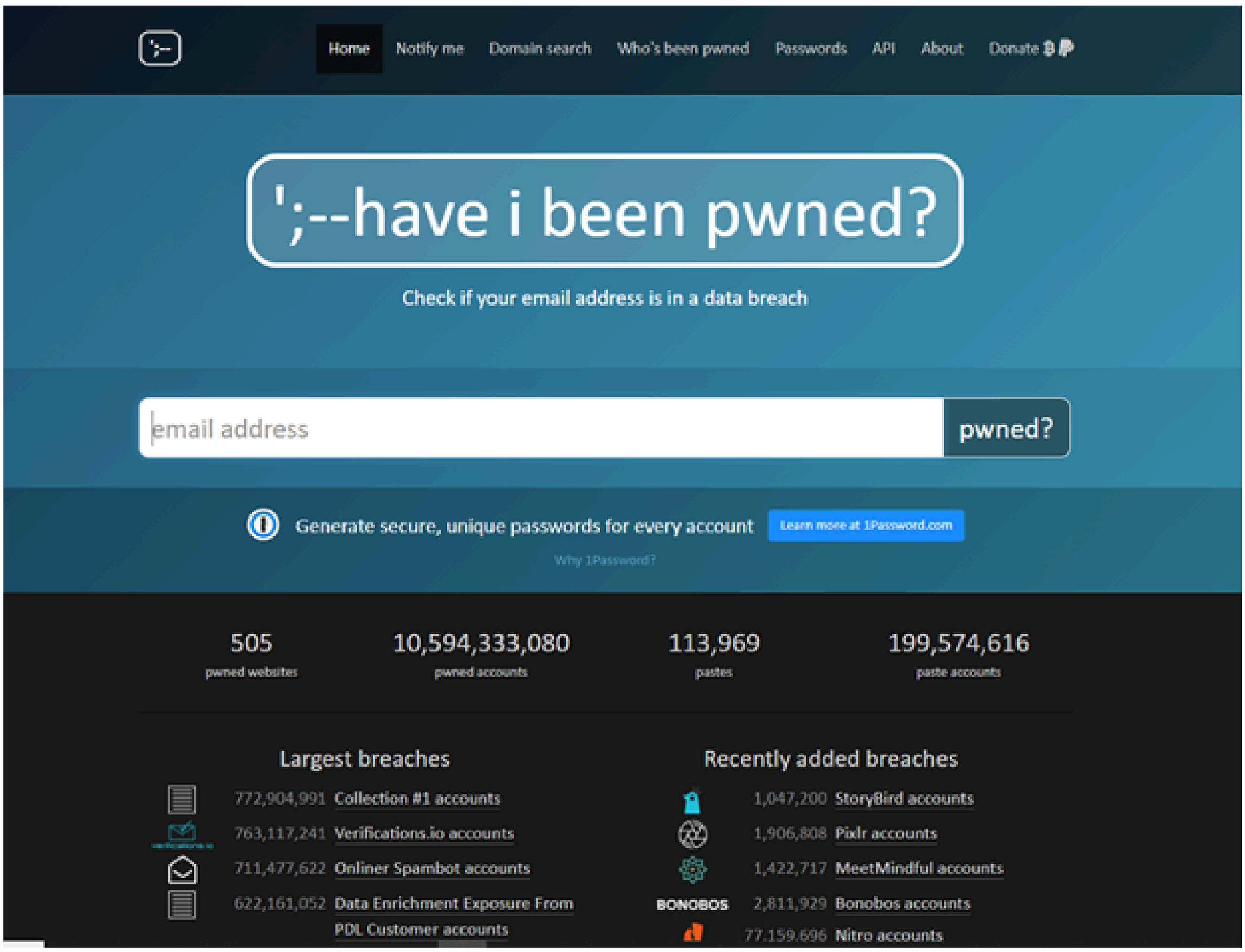
Como podemos ver en la imagen anterior con el resultado del análisis de VirusTotal, el enlace ya ha sido catalogado como Malicios o Phishing por empresas como CyRadar o Fortinet.

Para facilitar la comprensión de los pasos anteriores, hemos realizado un vídeo con un ejemplo actual de una phishing utilizando el SMS donde también utilizamos desde el mismo terminal móvil la herramienta VirusTotal para analizar el enlace:

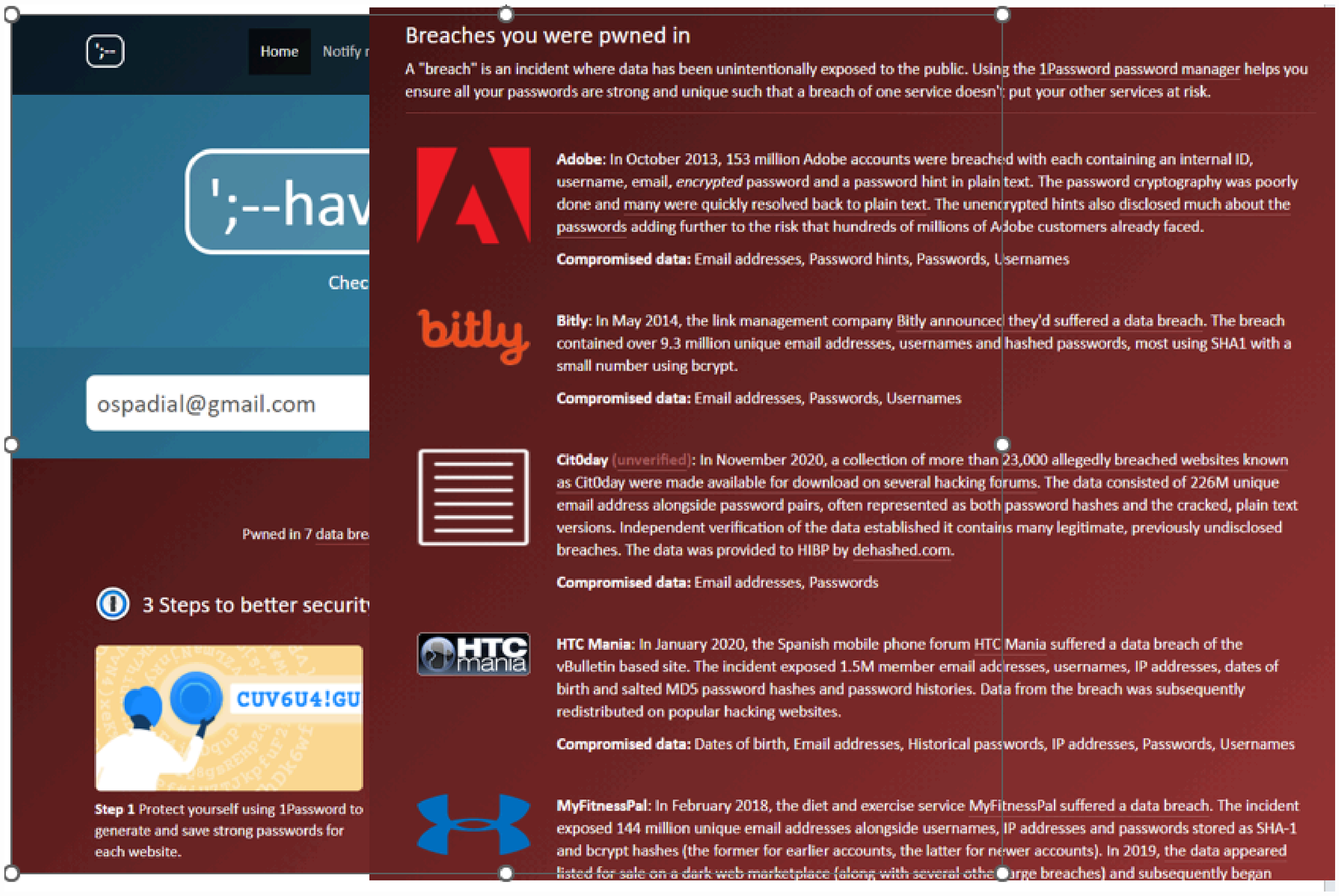
https://youtube.com/shorts/i_c40TuUMMM?feature=share

Have I been pwned?

Otra herramienta muy interesante para saber si tu correo electrónico ha sido vulnerado y es posible que tu contraseña aparezca en algunas de las filtraciones de seguridad realizadas a las multiples empresas y/o servicios a las que, consciente o inconscientemente estamos suscritos, es “Have I been pwned?”

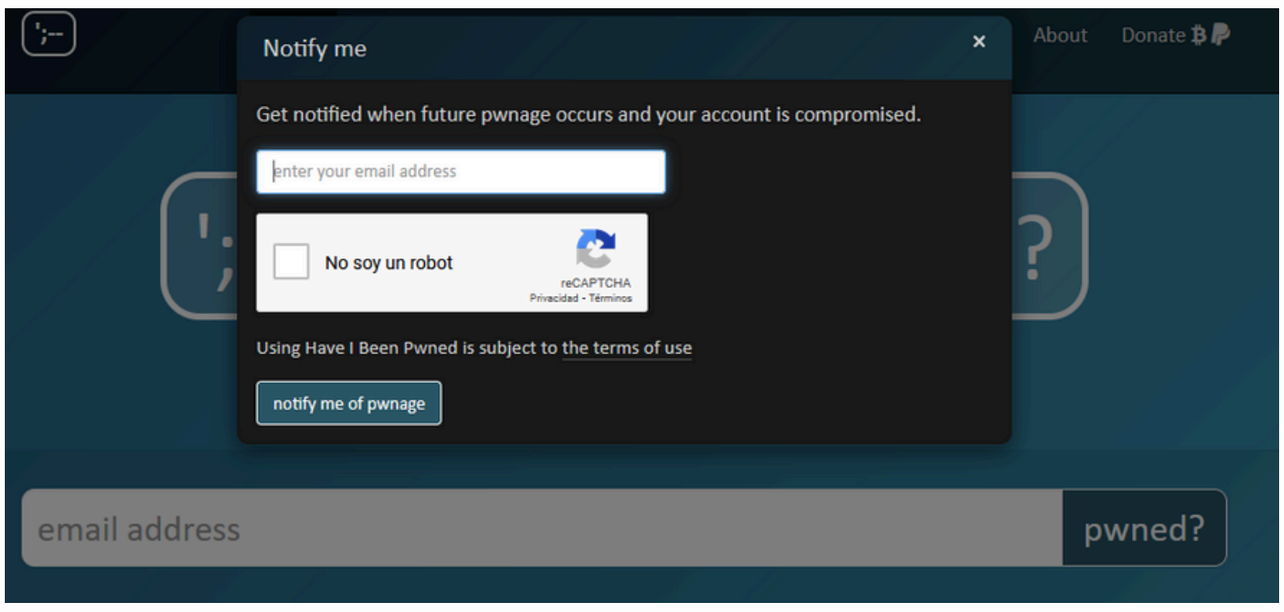


APRENDE A IDENTIFICAR UN ATAQUE DE PHISHING



Si nuestro correo electrónico aparece en alguna de las filtraciones, deberíamos cambiar la contraseña lo antes posible para evitar el acceso a terceros.

Una opción muy interesantes de este servicio es la de suscribirte directamente para que si tu correo aparece en alguna filtración te avisen directamente sin tener que estar comprobandolo cada cierto tiempo:

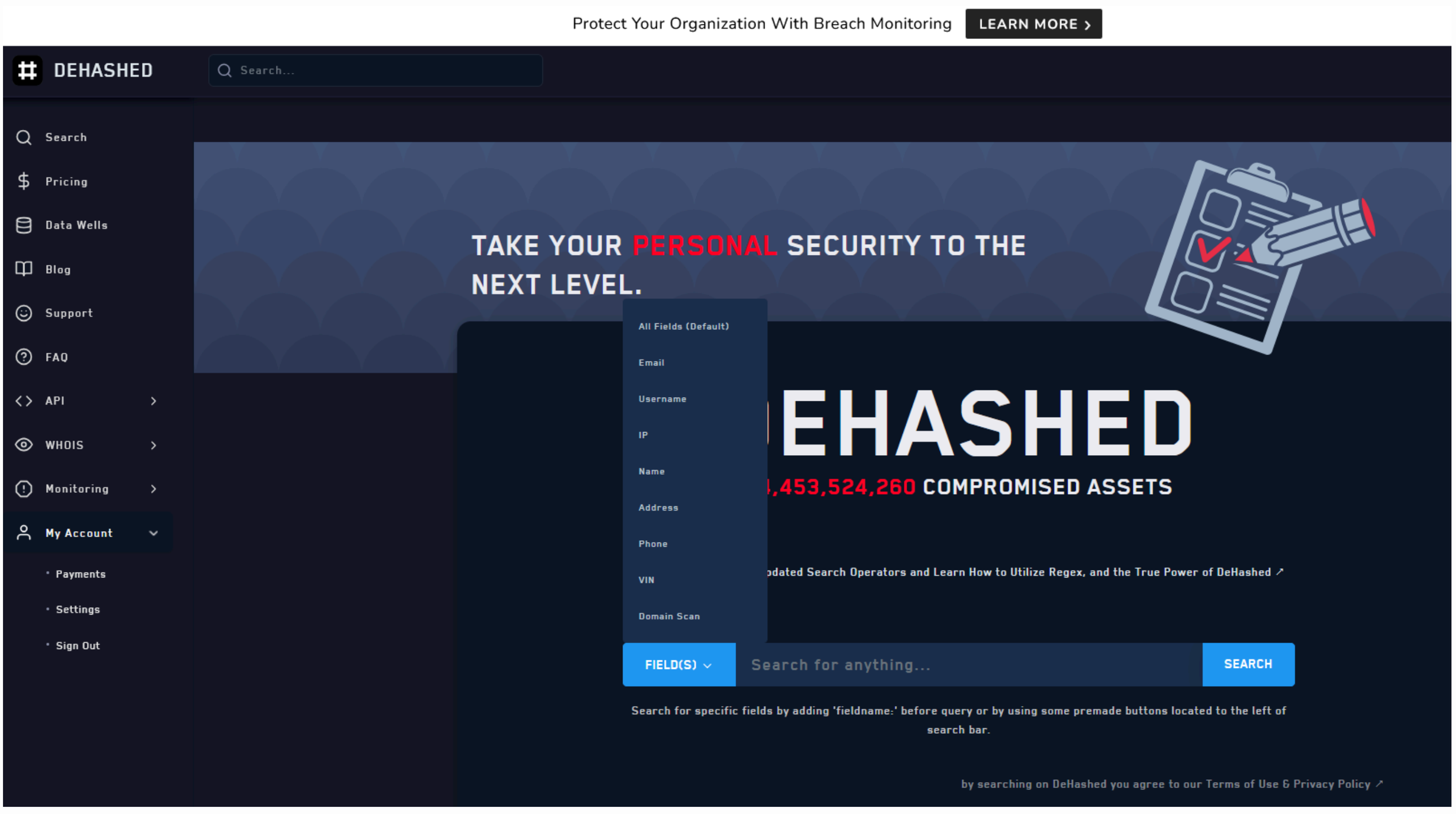


APRENDE A IDENTIFICAR UN ATAQUE DE PHISHING

DeHashed

Otra herramienta muy útil para obtener información sobre si nuestros datos han sido filtrados es DesHashed.

A diferencia de la anterior, DeHashed nos permite realizar búsquedas de más conceptos, como por ejemplo, el usuario, la dirección IP o el número de teléfono:



III. CONCLUSIONES

Para finalizar este ebook queremos dejaros una reflexión que consideramos importante:

“LA CUESTIÓN NO DEBE SER SI VAMOS A SER ATACADOS O NO,

LA CUESTIÓN DEBE SER, CUANDO VAMOS A SER ATACADOS”

Y cuando ese momento llegue que nos coja lo más preparados posible.

Os dejamos aquí un resumen de las pautas para identificar este tipo de ataques de phishing:

- Remitentes desconocidos y/o falseados (suplantación de identidad
- Comunicaciones impersonales (Estimado usuario…)
- Asuntos sospechosos (Urgente, Importante…)
- Mala redacción
- Enlaces falseados
- Firmas y otros elementos en el correo.

SI QUIERES RECIBIR MÁS INFORMACIÓN Y CONTENIDO GRATUITO SUSCRIBETE A NUESTRA NEWSLETER HACIENDO CLICK EN EL LOGO

APRENDE A IDENTIFICAR UN ATAQUE DE PHISHING