COMUNICADO DE SEGURIDAD

[Actualización 07/06/2023]

CAMPAÑA DE PHISHING QUE INTENTA SUPLANTAR A LA AGENCIA TRIBUTARIA PARA OBTENER TU CL@VE PERMANENTE

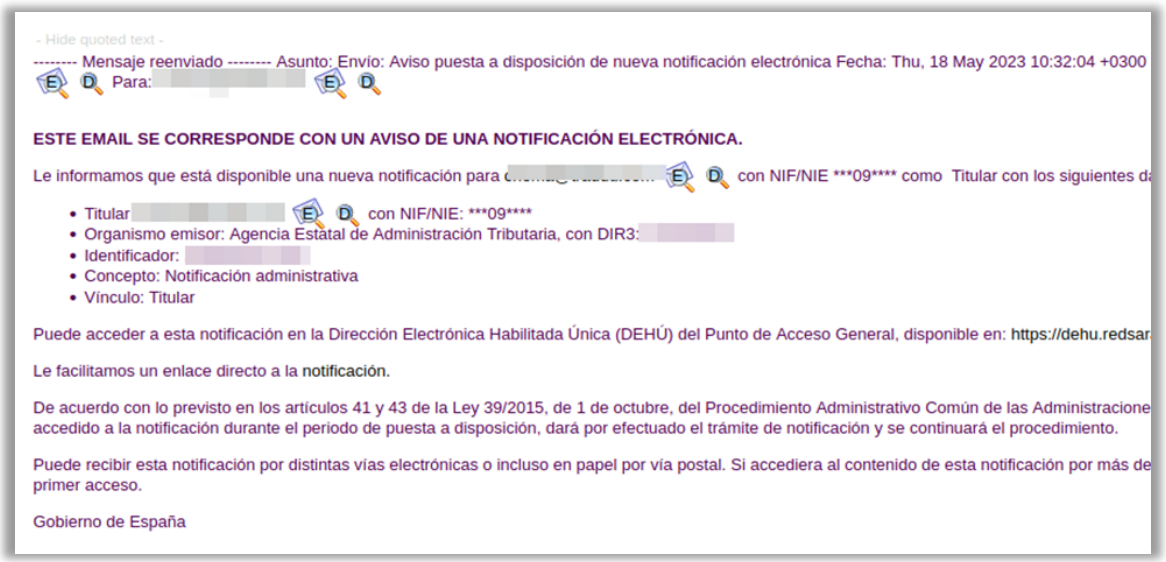
El **INSTITUTO NACIONAL DE CIBERSEGURIDAD** informa sobre la detección de una campaña de correos electrónicos fraudulentos de tipo phishing que trata de suplantar a la Agencia Tributaria para robar la Cl@ve Permanente u otros datos personales.

Es importante recordar que el acceso a Cl@ve Permanente se realiza con el DNI y no con el correo electrónico, lo que confirma que este caso se trata de un fraude.

Detalle

En esta campaña de phishing el asunto de los correos electrónicos detectados se identifica como «**Envío: Aviso puesta a disposición de nueva notificación electrónica».**

Ejemplos:



- Hide quoted text -

-------- Mensaje reenviado -------- Asunto: Envío: Aviso puesta a disposición de nueva notificación electrónica Fecha: Thu, 18 May 2023 10:32:04 +0300

Para:

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

Le informamos que está disponible una nueva notificación para con NIF/NIE ***09**** como Titular con los siguientes d

- Titular con NIF/NIE: ***09****
- Organismo emisor: Agencia Estatal de Administración Tributaria, con DIR3:
- Identificador:
- Concepto: Notificación administrativa
- Vínculo: Titular

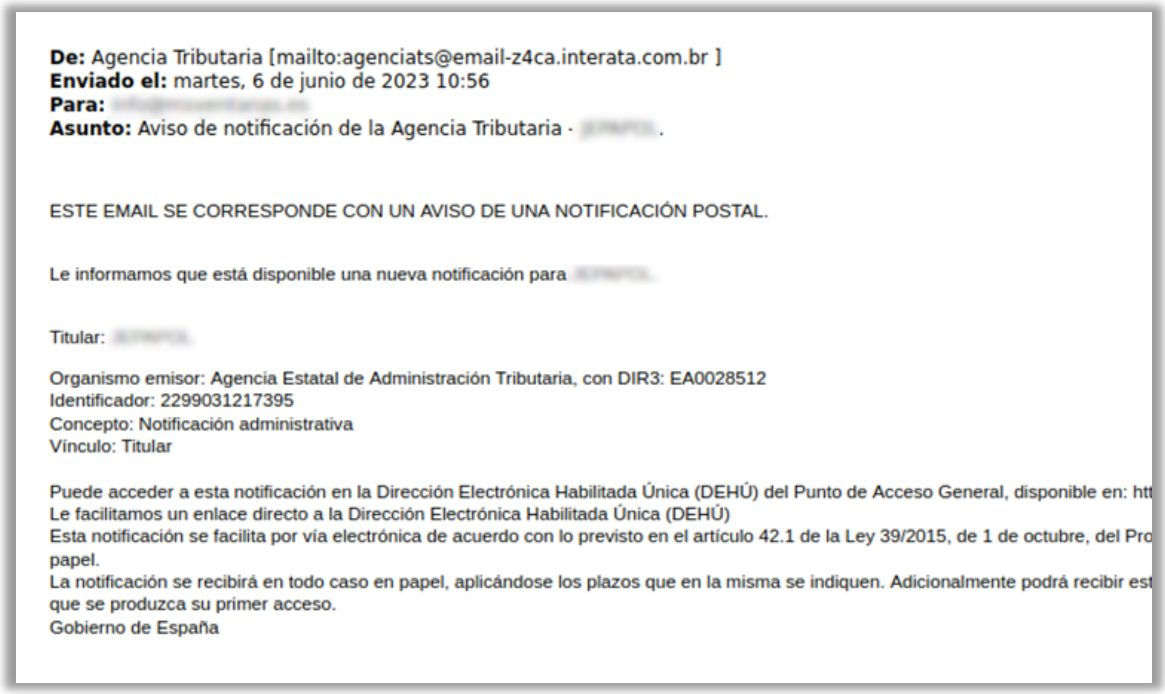
Puede acceder a esta notificación en la Dirección Electrónica Habilitada Única (DEHÚ) del Punto de Acceso General, disponible en: https://dehu.redsar

Le facilitamos un enlace directo a la notificación.

De acuerdo con lo previsto en los artículos 41 y 43 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administracione accedido a la notificación durante el periodo de puesta a disposición, dará por efectuado el trámite de notificación y se continuará el procedimiento.

Puede recibir esta notificación por distintas vías electrónicas o incluso en papel por vía postal. Si accediera al contenido de esta notificación por más de primer acceso.

Gobierno de España



De: Agencia Tributaria [mailto:agenciats@email-z4ca.interata.com.br]
Enviado el: martes, 6 de junio de 2023 10:56
Para:
Asunto: Aviso de notificación de la Agencia Tributaria -

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

Le informamos que está disponible una nueva notificación para

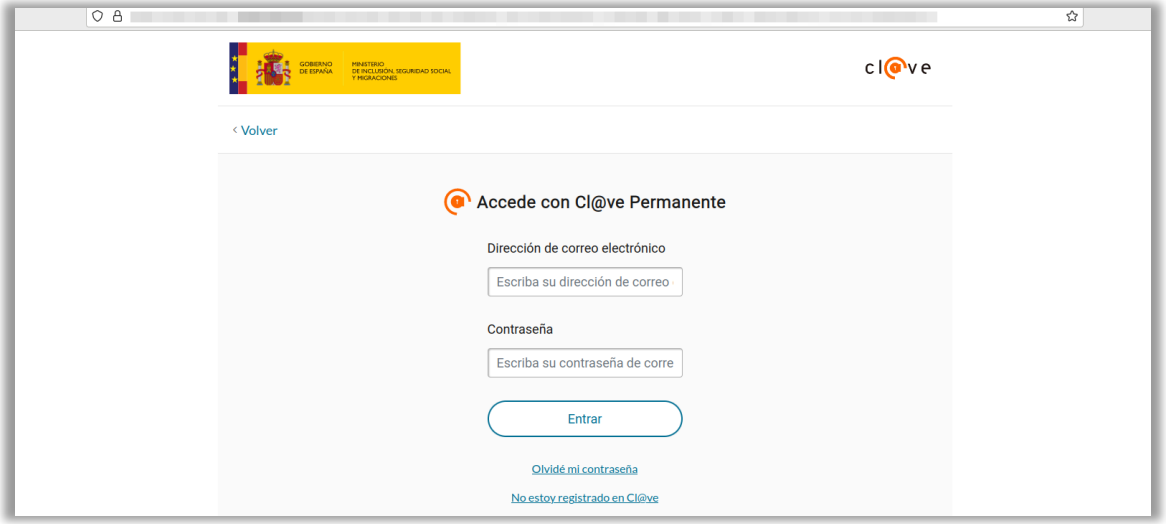
Titular:

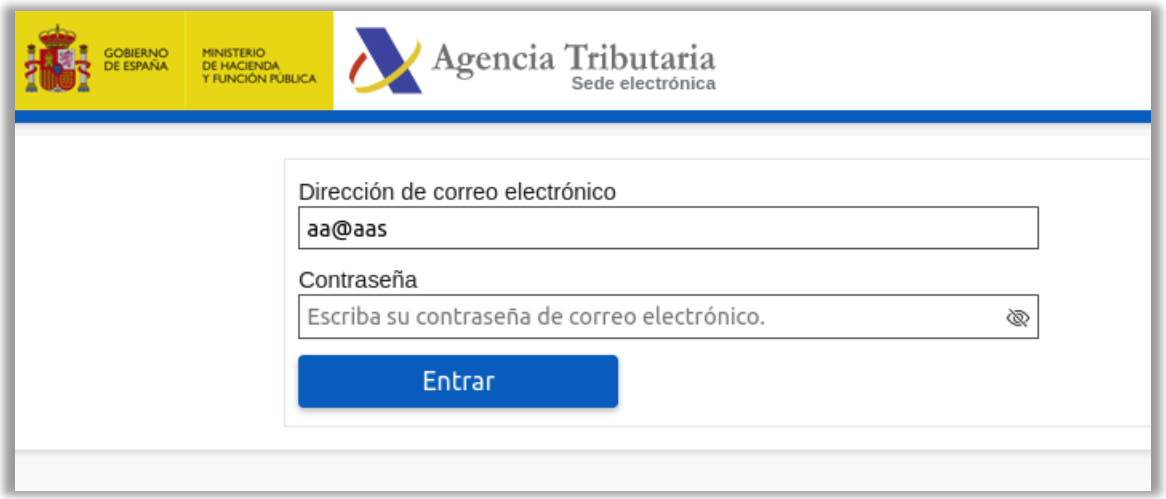
Organismo emisor: Agencia Estatal de Administración Tributaria, con DIR3: EA0028512
Identificador: 2299031217395
Concepto: Notificación administrativa
Vínculo: Titular

Puede acceder a esta notificación en la Dirección Electrónica Habilitada Única (DEHÚ) del Punto de Acceso General, disponible en: htt
Le facilitamos un enlace directo a la Dirección Electrónica Habilitada Única (DEHÚ)
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 Pro
papel.
La notificación se recibirá en todo caso en papel, aplicándose los plazos que en la misma se indiquen. Adicionalmente podrá recibir est
que se produzca su primer acceso.
Gobierno de España

Cabe destacar que en ningún momento se menciona el nombre o apellidos del destinatario, ya que lo desconocen, solo se hace referencia al correo electrónico, lo que debería hacer sospechar al usuario de la veracidad del correo. Además, incluye parte del DNI y un identificador que probablemente sean números aleatorios.

A continuación, se incita al usuario a acceder a un enlace malicioso que le redirigirá a la página web fraudulenta, similar a la legítima, donde se le solicitarán las credenciales de acceso, como un correo electrónico y una contraseña.





El mensaje termina advirtiendo al destinatario de las posibles consecuencias legales de no atender la notificación, añadiendo tono de urgencia, pretendiendo que la víctima actúe de forma precipitada.

Si el usuario introduce sus datos bancarios, estos pasarán a manos de los ciberdelincuentes.

Solución:

Desde INCIBE, se recomienda eliminar directamente el correo electrónico fraudulento y poner en preaviso al resto del personal para evitar posibles víctimas.

En caso de haber facilitado las credenciales, bien de tu Cl@ve Permanente o cualquier otro servicio, como el correo electrónico, será necesario cambiarlas inmediatamente. Además, se recomienda activar un doble factor de autenticación siempre que sea posible para que, en caso de que los ciberdelincuentes se hagan con las credenciales, no puedan acceder al servicio.

Ten en cuenta que por defecto al establecer tu Cl@ve Permanente ya dispone de un segundo factor de autenticación, ya que, al hacer uso de ella, el sistema te enviará un SMS con un código numérico de un solo uso.

Puedes informar a la Agencia Tributaria sobre este y otro tipo de fraudes a través de su página de ayuda: https://sede.agenciatributaria.gob.es/Sede/ayuda/Phishing.html

Si has recibido una notificación por parte de la AEAT y te surgen dudas, puedes visitar su web https://sede.agenciatributaria.gob.es/Sede/ayuda/Phishing.html y ver ejemplos de fraudes que se han elaborado suplantándoles e incluso reportárselos

https://www2.agenciatributaria.gob.es/soporteaeat/Formularios.nsf/Seguridad si has recibido uno. También puedes ponerte en contacto con la Agencia Tributaria para contrastar la información de los SMS o correos recibidos, y te ayudarán a solventar dicho problema a través de su chat . https://www2.agenciatributaria.gob.es/soporteaeat/Arcadia20.nsf

PRESTAR ATENCION A LA CIBERSEGURIDAD ES COSA DE TODOS.

info@incibe.es