COMUNICADO CECOFERSA

Nueva campaña PHISHING fraudulento suplantando Agencia Tributaria DEHÚ

Buenas tardes a tod@s

Una vez más, os informamos que se ha detectado una campaña de correos electrónicos fraudulentos, de tipo phishing, que suplantan la identidad de la **Agencia Tributaria** con el objetivo de robar información personal. El mensaje utiliza como gancho en envío de una supuesta notificación sobre una reclamación, en la que para obtener más información y dar conformidad, es necesario acceder a un enlace.

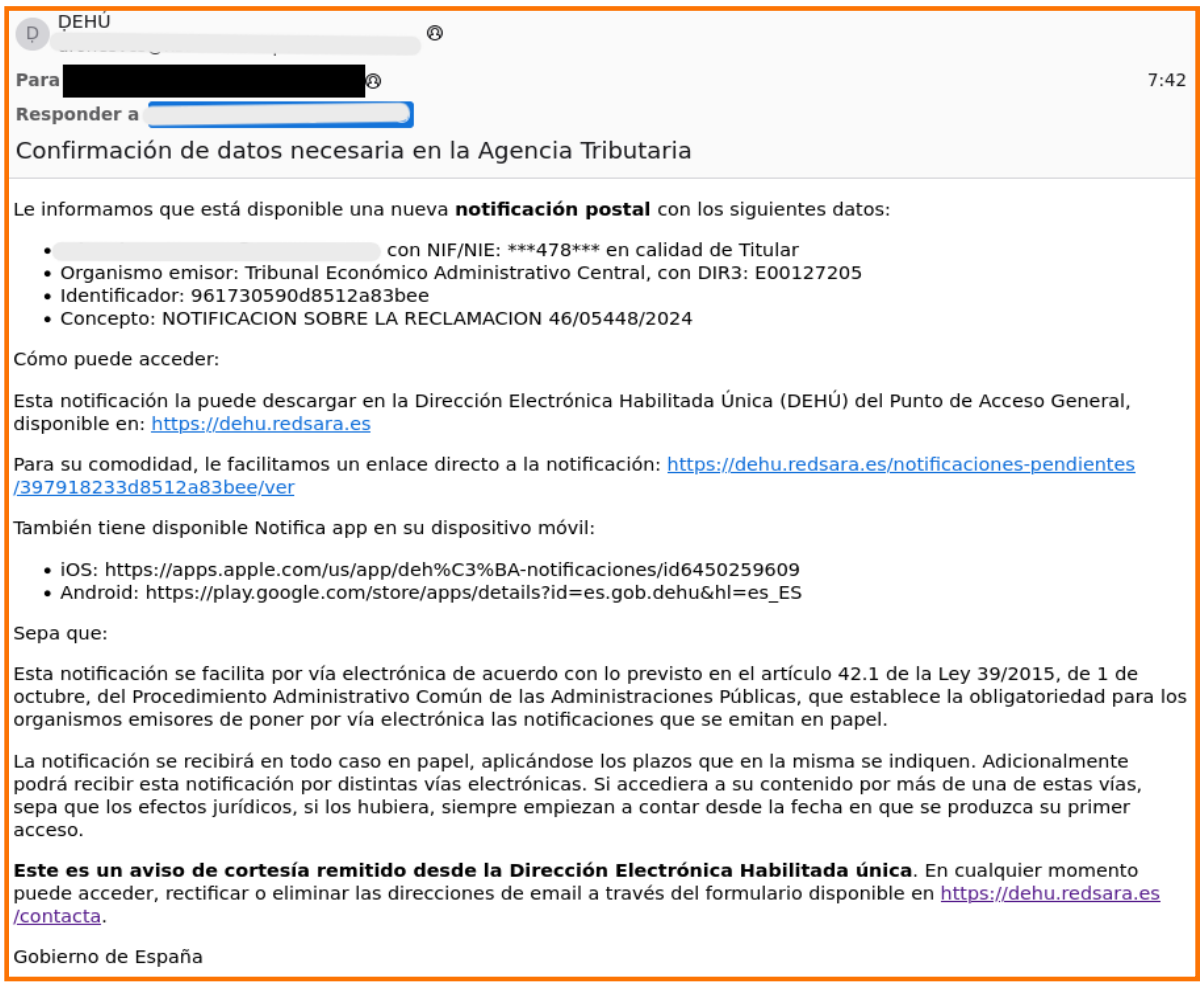
- Los correos electrónicos detectados parecen provenir del remitente **DEHÚ (Dirección Electrónica Habilitada Única),** pero si nos fijamos la dirección de correo electrónico que lo envía, podemos comprobar que resulta sospechosa.

- El asunto del correo, que puede variar, informa de la necesidad de confirmar unos datos en la Agencia Tributaria.

  A continuación, os detallamos algunos de los asuntos identificados en estos mensajes para que os ayude a identificarlos:

  - Agencia Tributaria: actualice ahora para garantizar un servicio continuo
  - Agencia Tributaria: valide sus datos para un acceso estable
  - Acción requerida: valide su información en la Agencia Tributaria
  - Actualice sus datos en la Agencia Tributaria para un servicio ininterrumpido
  - Actualización importante: confirme su información en la Agencia Tributaria
  - Actualización necesaria: verifique su cuenta de la Agencia Tributaria
  - Agencia Tributaria le informa: actualice su cuenta ahora
  - Agencia Tributaria: confirme su información para seguir utilizando los servicios
  - Confirmación de datos necesaria en la Agencia Tributaria
  - La Agencia Tributaria le informa: valide sus datos de cuenta ahora
  - Verificación de cuenta requerida por la Agencia Tributaria
  - Acción necesaria: actualice sus datos en la Agencia Tributaria
  - Actualización de la Agencia Tributaria: su atención es necesaria
  - Agencia Tributaria: confirme sus datos para mantener los servicios activos
  - Agencia Tributaria: verifique su cuenta para continuar utilizando los servicios
  - Aviso importante: confirme su información en la Agencia Tributaria
  - Confirme su información en la Agencia Tributaria para evitar interrupciones
  - Mantenga su acceso a la Agencia Tributaria: actualice su cuenta
  - Verifique ahora: la Agencia Tributaria necesita confirmar sus datos
  - Agencia Tributaria le recuerda: actualice sus datos de cuenta
  - Agencia Tributaria: complete la verificación de su cuenta
  - Agencia Tributaria: su acción es necesaria para garantizar el acceso continuo
  - Agencia Tributaria: su acción es necesaria para mantener el acceso
  - Confirmación de datos requerida para mantener su acceso a la Agencia Tributaria
  - Confirmación pendiente: actualice su información en la Agencia Tributaria
  - Notificación de la Agencia Tributaria: actualización de datos requerida
  - Notificación urgente de la Agencia Tributaria: confirme sus datos

A continuación, en el cuerpo del mensaje, se exponen una serie de datos que, a excepción del correo electrónico del destinatario, parecen ser completamente aleatorios:



DEHÚ

Para [redacted] 7:42

Responder a [redacted]

Confirmación de datos necesaria en la Agencia Tributaria

Le informamos que está disponible una nueva **notificación postal** con los siguientes datos:

- [redacted] con NIF/NIE: ***478*** en calidad de Titular
- Organismo emisor: Tribunal Económico Administrativo Central, con DIR3: E00127205
- Identificador: 961730590d8512a83bee
- Concepto: NOTIFICACION SOBRE LA RECLAMACION 46/05448/2024

Cómo puede acceder:

Esta notificación la puede descargar en la Dirección Electrónica Habilitada Única (DEHÚ) del Punto de Acceso General, disponible en: https://dehu.redsara.es

Para su comodidad, le facilitamos un enlace directo a la notificación: https://dehu.redsara.es/notificaciones-pendientes/397918233d8512a83bee/ver

También tiene disponible Notifica app en su dispositivo móvil:

- iOS: https://apps.apple.com/us/app/deh%C3%BA-notificaciones/id6450259609
- Android: https://play.google.com/store/apps/details?id=es.gob.dehu&hl=es_ES

Sepa que:

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.

Este es un aviso de cortesía remitido desde la Dirección Electrónica Habilitada única. En cualquier momento puede acceder, rectificar o eliminar las direcciones de email a través del formulario disponible en https://dehu.redsara.es/contacta.

Gobierno de España

Para terminar el mail que os envían, e intentando dar más credibilidad al mensaje, se hace referencia una ley y se firma el mensaje como si del Gobierno de España se tratase.

Como en otras campañas de este tipo, se incita a la víctima a hacer clic en un **enlace** que le redirigirá a una página web maliciosa, muy similar a la legítima, en la que, de introducir sus datos, **estos quedarán en manos de los ciberdelincuentes**.

En el caso de hacer clic en un **enlace:**

Los ciberdelincuentes solicitan el DNI de la víctima o incluso el certificado electrónico para poder acceder a dicha notificación. Si los ciberdelincuentes se hacen con dicha información, podrían usarla para futuros fraudes suplantando la identidad de la víctima.

En caso de haber recibido un correo electrónico como el que se describe en este aviso, se recomienda eliminarlo directamente y ponerlo en conocimiento de la Dirección de la empresa para que puedan realizar las gestiones de bloqueo e información interna pertinentes.

Si se ha accedido al enlace e introducido los datos:

- Mantente alerta ante posibles contactos posteriores. Al haber facilitado nombre y DNI, es posible que los ciberdelincuentes pretendan obtener otros datos.
- Si es necesario, considera revocar y obtener un nuevo certificado digital.
- Analiza el equipo utilizando un antivirus actualizado.
- Pon en cualquier buscador **el nombre de tu empresa entre comillas**, verás lo que aparece de tu empresa en la red y asegúrate de que tus datos no están siendo utilizados con fines no deseados.

También puedes comprobar la fiabilidad de los enlaces recibidos en virustotal.com

Recuerda que, ante cualquier sospecha, es preferible no acceder a ningún enlace sospechoso ni descargar archivos de fuentes no fiables.

JAVIER HERRERA
Director General