3º Correo falso de Hacienda

19/10/2023

Vicerrectorado de empresa, territorio y transformación digital
Servicio Central de Informática
Unidad de Seguridad
seguridadsci@uma.es

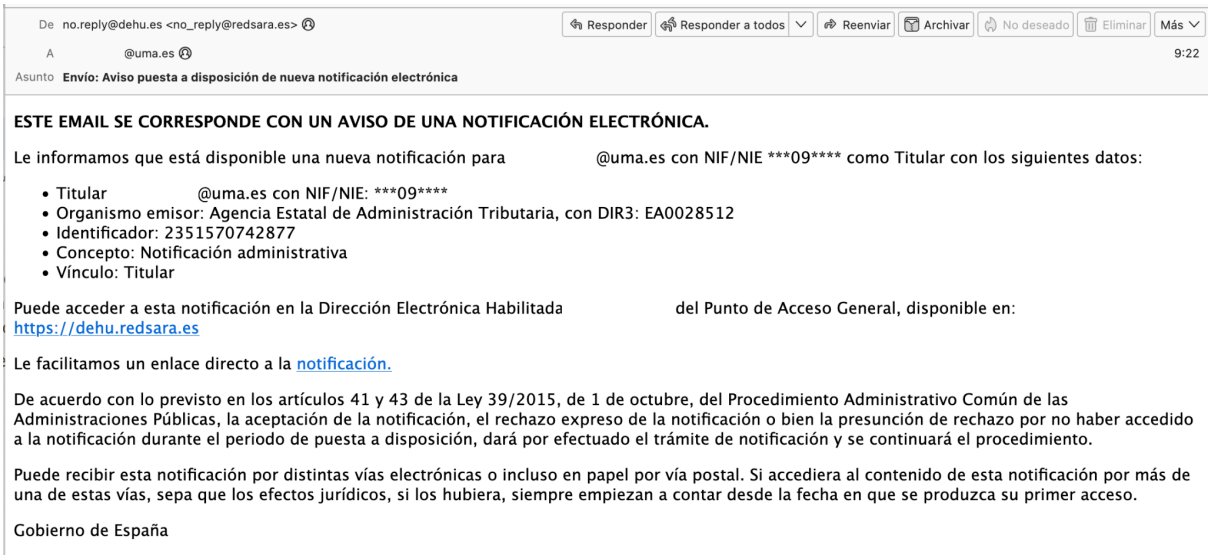
Visión general

Tenemos una nueva evolución del phishing de hacienda. Atentos a los detalles:

En anteriores episodios ….

Aspecto del mail pasado

En meses pasados, en los dos casos de phishing que entraron, el titular que venía era la dirección de correo. Como en esta captura de pantalla:



De no.reply@dehu.es <no_reply@redsara.es>
Responder | Responder a todos | Reenviar | Archivar | No deseado | Eliminar | Más
A @uma.es 9:22
Asunto **Envío: Aviso puesta a disposición de nueva notificación electrónica**

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

Le informamos que está disponible una nueva notificación para @uma.es con NIF/NIE ***09**** como Titular con los siguientes datos:

- Titular @uma.es con NIF/NIE: ***09****
- Organismo emisor: Agencia Estatal de Administración Tributaria, con DIR3: EA0028512
- Identificador: 2351570742877
- Concepto: Notificación administrativa
- Vínculo: Titular

Puede acceder a esta notificación en la Dirección Electrónica Habilitada del Punto de Acceso General, disponible en:
https://dehu.redsara.es

Le facilitamos un enlace directo a la notificación.

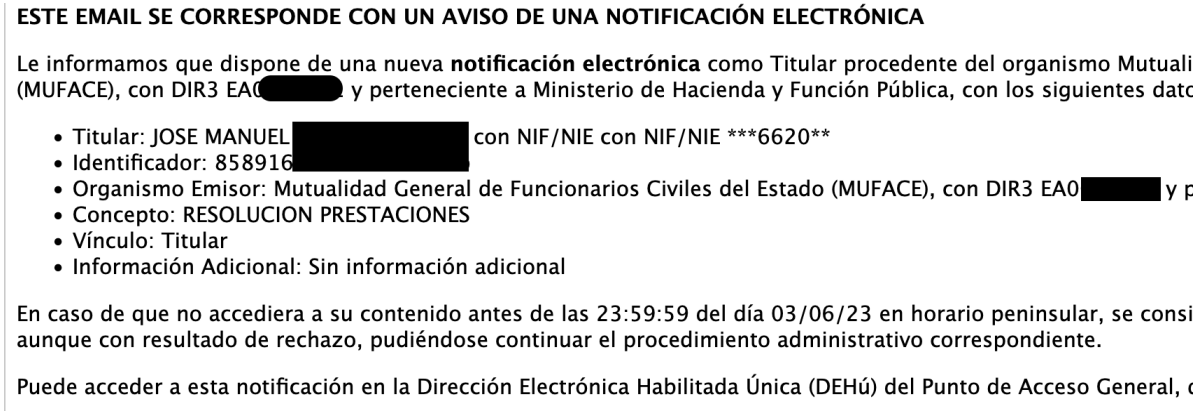
De acuerdo con lo previsto en los artículos 41 y 43 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, la aceptación de la notificación, el rechazo expreso de la notificación o bien la presunción de rechazo por no haber accedido a la notificación 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 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

En el correo de Hacienda “de verdad”, el titular era sólo el nombre y apellidos, **nunca la dirección de correo electrónico**

Este es el aspecto original de un correo de Hacienda. Fijaros en el **Titular**



ESTE EMAIL SE CORRESPONDE CON UN AVISO DE UNA NOTIFICACIÓN ELECTRÓNICA

Le informamos que dispone de una nueva **notificación electrónica** como Titular procedente del organismo Mutuali
(MUFACE), con DIR3 EA[redacted] y perteneciente a Ministerio de Hacienda y Función Pública, con los siguientes datc

- Titular: JOSE MANUEL [redacted] con NIF/NIE con NIF/NIE ***6620**
- Identificador: 858916[redacted]
- Organismo Emisor: Mutualidad General de Funcionarios Civiles del Estado (MUFACE), con DIR3 EA0[redacted] y p
- Concepto: RESOLUCION PRESTACIONES
- Vínculo: Titular
- Información Adicional: Sin información adicional

En caso de que no accediera a su contenido antes de las 23:59:59 del día 03/06/23 en horario peninsular, se consi
aunque con resultado de rechazo, pudiéndose continuar el procedimiento administrativo correspondiente.

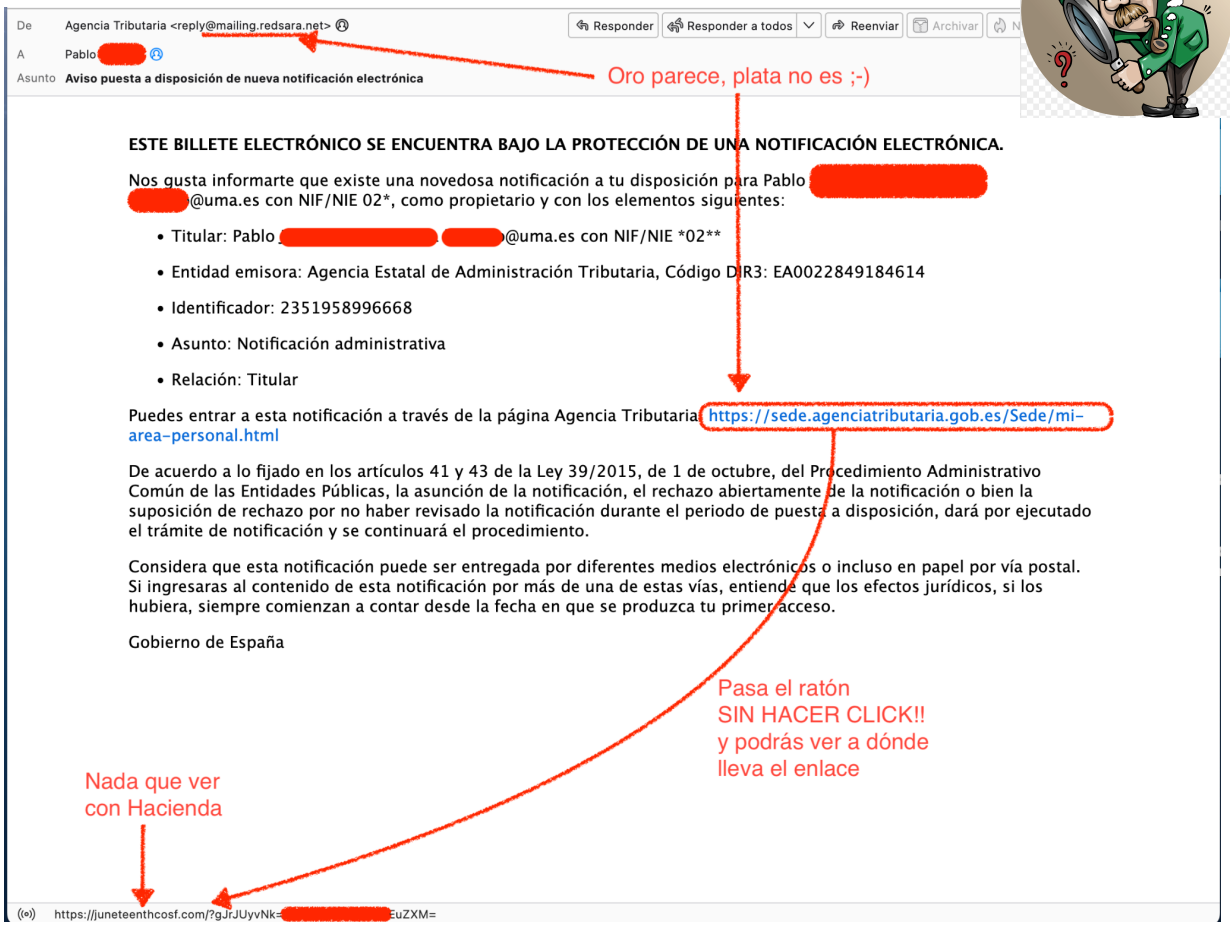
Puede acceder a esta notificación en la Dirección Electrónica Habilitada Única (DEHú) del Punto de Acceso General, c

Aspecto del nuevo

Pero ahora nos hemos encontrado una nueva versión “mejorada”

No desesperéis, ya tenemos el conocimiento para poder detectarlos.

Atentos a los detalles. Primero los más directos



Como siempre, parece que lo manda algún organismo oficial, según ponen desde **redsara**, a nosotros **@uma.es**, con un enlace que parece que también es de la Agencia, peroooo……

Si pasamos el ratón por encima del enlace **sin hacer click**, ya podemos ver que saltará a un sitio que nada tiene que ver con la Agencia **juneteenthcosf**

```
Aquí ya sabemos que este mail es un engaño
```

Pero nosotros, que ya hemos asistido al curso de cibersec queremos dar un paso más.

Vamos a poner en práctica lo aprendido sobre las cabeceras.

Análisis de la cabera

Saco los apuntes, me pongo mi sudadera con capucha y ya soy Hacker!!

Como hemos visto en el taller, me fijo en el **to**, el **from** y el primer servidor que recepciona el correo **Received**.

```
Received: from jubipk by webserver97.turnkeywebspace.com with
local (Exim 4.96.2)
      (envelope-from <jubipk@webserver97.turnkeywebspace.com>)
      id 1qtQGH-0005ot-0c
      for h******@uma.es;
      Thu, 19 Oct 2023 06:28:17 -0400
To: h*******@uma.es
Subject:
=?UTF-8?B?QXZpc28gcHVlc3RhIGEgZGlzcG9zaWNpw7NuIGRlIG51ZXZhIG5vdGlm
aWNhY2nDs24gZWxlY3Ryw7NuaWNh?=
X-PHP-Script:
jubi.pk/wp-content/themes/astra/inc/builder/type/header/site-ident
ity/library.php for 185.76.11.24
X-PHP-Originating-Script: 2872:phphxIsYr
From: =?UTF-8?B?QWdlbmNpYSBUcmlidXRhcmlh?=
<reply@mailing.redsara.net>
Reply-To: reply@mailing.redsara.net
```

Ya sabemos que **to** y **from**, como los pone el que manda el correo, es la parte más fácil de falsificar. No voy a volver a caer en este punto!!

En el **to** aparecerá nuestra dirección y en el **from** la dirección del que lo manda. En este caso viene codificada (lo he puesto en verde) en base64

```
QWdlbmNpYSBUcmlidXRhcmlh?=
```

Pero cualquier conversor on-line, nos podrá decir que han querido poner ahí. Uno que nos puede servir para este ejemplo está en este enlace:

https://www.base64decode.org/es/

Y si copiamos y pegamos en esa web esa cadena de texto, nos lo traducirá a...

```
Agencia Tributaria
```

Pero podría poner cualquier cosa, todo es mentira.

El primer received, que es el primer servidor que recepciona el mensaje, nos va a dar más pistas. Lo he puesto en celeste y dice que lo está mandando desde un servidor que se llama

```
webserver97.turnkeywebspace.com
```

y un usuario, probablemente al que han vulnerado su cuenta que es

```
jubipk
```

En cualquier caso, nada que ver con Hacienda.

One more thing

Hemos cortado el acceso a ese enlace y puesto en lista negra a esa dirección, pero pueden vulnerar otra cuenta y el mismo correo vendrá de otro usuario y podrán poner otros enlaces, por eso si has entendido el proceso, a vosotros os dará igual porque sabréis distinguir si es falso o no.

Y para el que no esté seguro...

lo espero en las próximas ediciones del curso de ciberseguridad 🤣

Como siempre os digo, tenéis las direcciones seguridadsci@uma.es e incidentes@uma.es a vuestra disposición.

¡Espero que os sirva de ayuda!