Campaña de Fraude

"Aviso de notificación de la DEHÚ:

Un phishing bien diseñado

En el mundo hispanohablante históricamente hemos tenido una ventaja a la hora de enfrentarnos a los fraudes online: Muchos de estos fraudes son diseñados para el mercado angloparlante, y/o por grupos de ciberdelincuencia que no hablan nuestro idioma. Por ende, partían con desventaja a la hora de engañarnos, ya que probablemente, a poco que nos fijemos en su legibilidad, algo no funcionaba.Sin embargo, de un tiempo a esta parte la industria del cibercrimen ha crecido tanto que ya es muy habitual encontrarse ante campañas de phishing muy bien elaboradas y localizadas al mercado en cuestión. Este es el caso de la que quería hablar hoy, y que he recibido recientemente: El fraude del aviso de notificación de la DEHÚ.

Primero de todo: ¿ Qué es eso de la DEHU?

DEHÚ es la plataforma de notificación del gobierno de España. Desde hace unos años, y en ese proceso continuo de transformación digital, cada vez más notificaciones se reciben de forma telemática, y para ello, los diferentes ministerios españoles se han ido sumando a la plataforma.

Por tanto, es muy probable que si tienes un requerimiento de Hacienda, o esté esperando alguna subvención, o haya participado en alguna licitación, o simplemente tiene una empresa a su nombre y cuente, por supuesto, con un certificado digital o algún sistema de acceso telemático a servicios gubernamentales, o haya tenido que usar (y pegarte, todo sea dicho) con DEHÚ.

Que no sé usted, pero yo, cada vez que recibo un aviso de notificación de DEHÚ, me pongo nervioso.

En la mayoría de las ocasiones, se trata de una alerta de algún tema relacionado con el ministerio de transformación digital, por eso de que CyberBrainers es una entidad acogida al programa de agente digitalizador del Kit Digital, y este programa, como tantos otros, utiliza DEHÚ como plataforma de notificación.

Pero claro, cuando usted mira el email que te envían, no tiene ni idea de si se trata de algo bueno o malo, siendo esto último lo más habitual.Incluso con el Kit, ya van varias notificaciones que han supuesto tener que volver a enviar más documentación para seguir siendo agentes digitalizadores, por eso de que el gobierno saca programas y luego, con el tiempo, va cambiando a su antojo los requerimientos para estar adscritos, teniendo los digitalizadores que perder nuevamente tiempo documentando otra vez lo que ya habíamos documentado, y nos habían aceptado, previamente.

Y no solo, sino que, como les decía, DEHÚ es la plataforma que también usa la Agencia Estatal de Administración Tributaria. Y ya sabes que siempre que recibe una notificación de Hacienda, es para mal.

A un servidor, por ejemplo, este año le han hecho dos inspecciones: Una a título personal, y otra a título de la empresa. En ambas he podido salir airoso (lo tengo todo regularizado), pero ya sabe cómo va la cosa: Aunque haya hecho todo bien, puede que no se lo acepten, como le pasó a Èlia hace ya un par de años con otra inspección, en la que incluso le echaron para atrás viajes de ida y vuelta para dar conferencias, ya que según el inspector asignado, eso no era por trabajo, es por ocio (claro, te vas un día a la otra punta del mundo, das una conferencia y presentas pruebas de ello, y vuelves al día siguiente, porque te gusta viajar en avión…).

En fin, que sea como fuere, ahora, que estamos en fechas de presentar la Renta, los cibercriminales están lanzando ya campañas de fraude haciéndose pasar por Hacienda.Y la que he recibido yo la semana pasada, perfectamente podría haber pasado por verídica.

¿Cómo funciona el fraude del aviso de notificación de la DEHú?

Echas las presentaciones anteriores, paso a definir cómo fue el ataque, y por qué estuve a puntito de picar.

Pero antes, una matización: Al menos a un servidor siempre que recibo una notificación de la DEHÚ, la suelo recibir por duplicado, supongo que porque tengo dos correos (personal y corporativo) asociados.Por eso, me sorprendió que un día como hoy, a la tarde, recibiera una única notificación de la DEHÚ al correo corporativo.

Sin embargo, daba la casualidad que ese mismo día, a la mañana, había recibido varias, por lo que perfectamente podría tratarse o de un email que se envió más tarde de lo previsto, o de otra nueva notificación.

Así que, cómo no, corrí a abrirlo, y me encontré

Aviso de notificación de la DEHú contacto@cyberbrainers.com Recibidos ×

DEHú notificaciones@dehu.com a través de rsvehicleimports.com.au jue [redacted] (hace 4 días)
para contacto

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

Le informamos que está disponible una nueva notificación para contacto@cyberbrainers.com como Titular con los siguientes datos:

- Titular contacto@cyberbrainers.com
- Organismo emisor: Agencia Estatal de Administración Tributaria, con DIR3: L02000050
- Identificador: 51[redacted]
- Concepto: Notificación -- Expediente 46[redacted]SIA 2087160, Serie SF0249)
- Vínculo: Titular

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

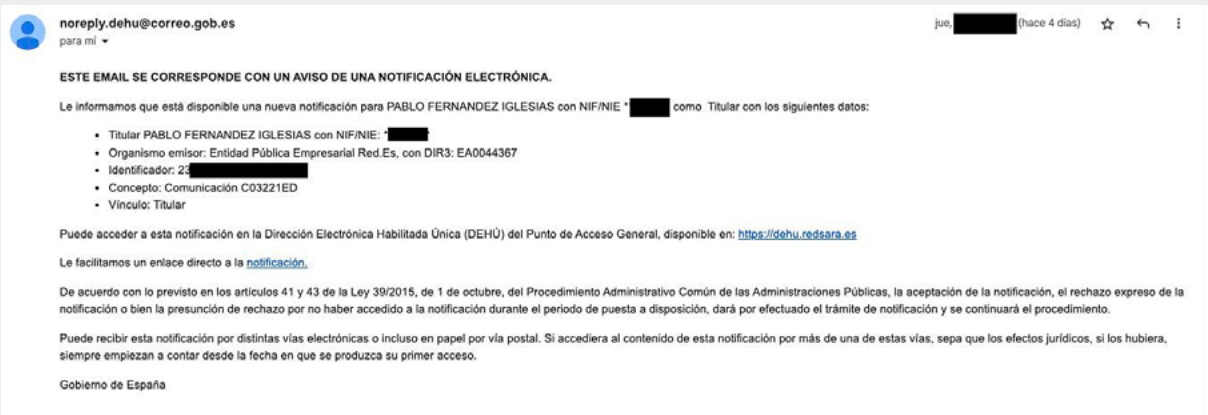
Le facilitamos un enlace directo a la notificación.

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

Ejemplo de campaña de phishing de la DEHÚ bien diseñada



noreply.dehu@correo.gob.es jue [redacted] (hace 4 días)
para mí

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

Le informamos que está disponible una nueva notificación para PABLO FERNANDEZ IGLESIAS con NIF/NIE *[redacted] como Titular con los siguientes datos:

- Titular PABLO FERNANDEZ IGLESIAS con NIF/NIE: *[redacted]
- Organismo emisor: Entidad Pública Empresarial Red.Es, con DIR3: EA0044367
- Identificador: 23[redacted]
- Concepto: Comunicación C03221ED
- Vínculo: Titular

Puede acceder a esta notificación en la Dirección Electrónica Habilitada Única (DEHÚ) 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

Ejemplo de correo real y oficial enviado por la DEHÚ

lo siguiente:

Se trata, a todas luces, de exactamente el mismo copy que tienen todos los envíos de la DEHÚ, y por lo que puedo ver, parece ser una notificación de Hacienda (vamos, algo malo…).

Adjunto otro mail, recibido ese mismo día, y que sí es oficial, para que veas las escasas diferencias que tiene esta campaña de phishing, con un correo real de la DEHÚ.

Como pueden apreciar, teniendo uno delante de otro es fácil darse cuenta de que en el primero no se dirigen a mi como titular, sino al correo electrónico. Por supuesto, si fuera oficial o bien pondrían, como ponen, mis datos fiscales personales (nombre completo y algunos de los números del DNI), o bien iría dirigido a la propia empresa, en cuyo caso aparecerían los datos fiscales de la misma (razón social y algunos de los números del CIF). Pero por lo demás, es un calco exacto de las comunicaciones oficiales.

Hay que decir, eso sí, que lo abrí desde el móvil, y como recomiendo hacer siempre en esos tres puntos que identifican a un phishing, para confirmar su legitimidad, lo primero que hice fue ver quién era el emisor del mail, encontrándome con que, en efecto, parecía ser un mail oficial enviado por notificaciones@dehu.es.

De nuevo, algo que parece legítimo… pero que no existe como tal. Las comunicaciones oficiales de la DEHÚ vienen dadas por el dominio oficial de la DEHÚ, que al tratarse de un dominio corporativo, es correo.gob.es.

Otro matiz que de no tener ambos correos (fraudulento y oficial) delante, se nos puede pasar inadvertido.

A la hora de escribir este artículo, no obstante, y ya desde escritorio, veo que aunque en efecto los metadatos de envío estaban correctamente puestos, GMail sí me chiva que el emisor no es esa cuenta, sino otra con un dominio muy poco confiable, como puedes ver a continuación:

Esta información, en la versión móvil, no me aparecía, pensando que en efecto estaba ante una comunicación oficial

Los oficiales, por supuesto, vienen también firmados por correo.gob.es.

Pero recalco, lo estaba mirando desde el móvil, y ahí este indicio no lo tenía, así que, y de nuevo por ser precavido, me da por mirar a dónde llevan esos dos enlaces de la notificación (el tercer punto de los que debemos fijarnos a la hora de identificar fraudes de correos legítimos).

Y aquí es cuando veo que estoy ante un fraude más. Eso sí, con sorpresa incluida.

Ambos enlaces, en vez de llevar a la plataforma de la DEHÚ, llevan a una página dentro del dominio registraalbacete[dot]com. Que ya me dirás qué tiene que ver con la DEHÚ (ni tan siquiera vivo en Albacete), por lo que supongo que simplemente es uno de los dominios que tienen bajo el control los cibercriminales.

La sorpresa viene porque al intentar entrar, me encuentro con que el enlace te redirige a una supuesta página de la Agencia Tributaria, que por lo que puedo ver, están cambiando cada poco (cuando entré la primera vez era una agenciatributaria[dot]online, y ahora veo que redirige a agenciatributaria[dot]hk).

La web en cuestión se parece a la de la Agencia Tributaria, pero es aquí donde el fraude cojea, ya que, que yo sepa, hoy en día no hay manera de acceder a trámites administrativos mediante usuario y contraseña.

O bien lo haces mediante certificado digital, bien mediante Cl@ve, o PIN Permanente. Sistemas que

difícilmente veo cómo pueden robárnoslos los cibercriminales.

Pero oye, igual así cazan los datos de algunas víctimas…

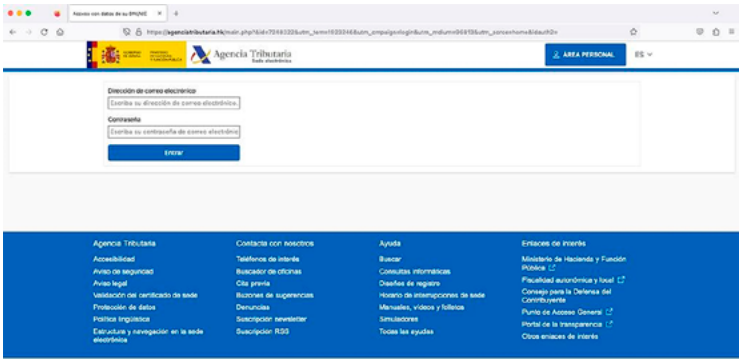
Por cierto, que he probado a poner un usuario y contraseña (inventados, por supuesto), y la web, como era de esperar, me dice que la validación no es correcta y que vuelva a incluirlos.

Ni tan siquiera se han molestado en hacer una redireción a la página oficial…

Y otro apunte:
Desde que me llegó el mail, hasta que he creado este artículo, han pasado 4 días. En estos cuatro días me alegra ver que tanto Chrome como Firefox (los dos navegadores de escritorio que he probado para preparar este tutorial) ya marcaban como potencialmente fraudulento el enlace de Albacete. Y Firefox, además, hacía lo propio con el dominio fake de la AgenciaTributaria (Chrome sí me dejaba entrar a él, sin mostrarme alerta).

Un ejemplo más de los tiempos que manejan estos cibercriminales, que son conscientes de que a las pocas horas de lanzar la campaña, la URL se va a quemar, y tocará volver a lanzar otra campaña.

De hecho, por eso es tan habitual que usen redirecciones que les permitan funcionar durante al menos unas horas más las campañas activas, pudiendo cambiar la URL final del phishing mientras aún no se ha quemado la URL que aparece en el correo, y que redirige al fraude en cuestión.



¿Cómo podemos evitar ser víctimas de este tipo de campañas de phishing?

Como pueden ver, simplemente he aplicado los 3 elementos que delatan a las campañas de phishing o fraude por email.

1. Cerciorarse de quién es quién envía el email realmente
2. Revisar con calma si lo que dice el mail tiene sentido
3. Desconfiar por defecto de los enlaces y de los ficheros adjuntos, estableciendo las medidas de seguridad adecuadas para abrirlos.

Autor: Pablo F. Iglesias

Se describe como un apasionado de la tecnologíaConsultor de Presencia Digital y Reputación Online, presidente de la Consultora de Reputación Online CyberBrainers, y fundador, co-fundador, vocal y vicepresidente de varias startups y asociaciones relacionadas con el mundo de la ciberseguridad, la transformación digital y el marketing.

Con más de una década escribiendo a diario en www.pabloyglesias.com, es uno de los mayores referentes en materia de nuevas tecnologías y seguridad de la información de habla hispana.

Desarrolla labores pedagógicas (online y presencial) sobre Presencia Digital y Seguridad de la Información, intentando concientizar a la sociedad, sobre los riesgos y oportunidades del tercer entorno.

Actualmente asesora a profesionales, PYMES y grandes empresas sobre cómo obtener valor de la información que circula a su alrededor. El punto medio necesario entre marketing, comunicación y seguridad de la información.