Guía para la prevención contra los ataques de suplantación de identidad

Comisión de Nuevas Tecnologías del Consejo General de Graduados Sociales

CONSEJO GENERAL DE COLEGIOS OFICIALES
DE GRADUADOS SOCIALES DE ESPAÑA

"Expertos en Relaciones Laborales y Recursos Humanos"

Introduccion:

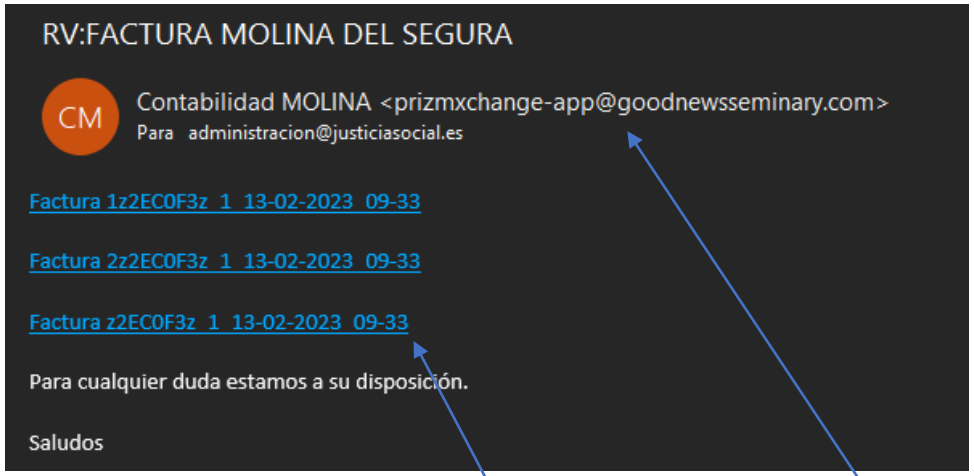
Guía básica, elaborada por el Consejo General de Graduados Sociales de Colegios Oficiales de España, dirigida a todos los colegios oficiales de Graduados Sociales, especialmente para aquellos sin departamento de informática.

Disponible también para todos los colegiados que quieran implementar unos conceptos básicos de ciberseguridad contra el phishing.

Fecha 23/02/2023

Versión 1.0

¿Qué es el Phishing?



- Son ataques informáticos que buscan la obtención de datos o acceso a sistemas que proporciona el usuario sin su conocimiento y consiguen a través de engaños.
- Por ejemplo, un truco que utilizan de forma común es la suplantación de identidad, de compañías energéticas, bancos …
- Aquí podemos ver un ejemplo de un intento de phishing, en este caso un correo haciéndose pasar por una factura.

Como se puede ver, la dirección es sospechosa

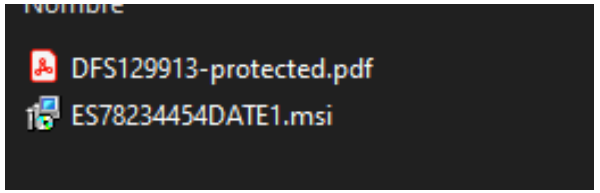
No son archivos adjuntos, sino enlaces

Puntos clave a identificar

La dirección

Descarga archivos automáticamente

Que se descarga



- Como vemos, la dirección es extraña, ya que no coincide con el email y no tiene relación ninguna.
- Si un enlace descarga automáticamente archivos sin avisar, es muy probable que sea un virus. También la extensión .zip (comprimidos) no es algo común.
- Cuando descomprimimos el .zip podemos ver 2 archivos, un .pdf y un .msi. El archivo .msi es un virus, pero para dar mayor confianza incluye el .pdf, así habrá mas posibilidades que lo enmascare.

Pautas generales de prevención para evitar ser víctima de fraudes de este tipo:

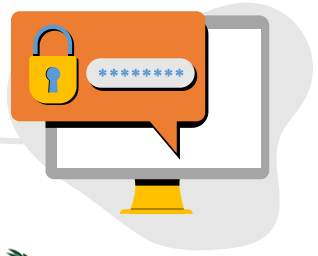
Contiene mensajes genéricos, como “Estimado cliente”, u datos incompletos que no te identifiquen

Revisa la dirección donde recibes el correo y el cuerpo del mensaje

El correo que proceda de una entidad bancaria legítima, nunca contendrá enlaces a su página de inicio de sesión o documentos adjuntos.

¡Fíjate en el remitente!

¡No te fíes de los adjuntos!

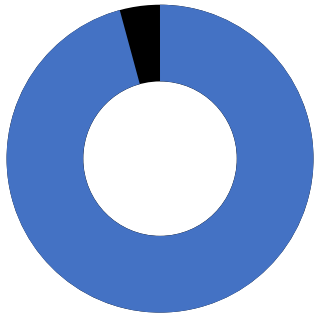


No contestar en ningún caso a estos correos

Ingeniería Social, que es y porque se usa:

La ingeniería social, es la rama que busca métodos que hay en la sociedad, en este caso explota las vulnerabilidades tales como:

- Respeto a la autoridad
- Voluntad de ayudar
- Temor a perder un servicio
- Respeto social
- Servicios Gratuitos

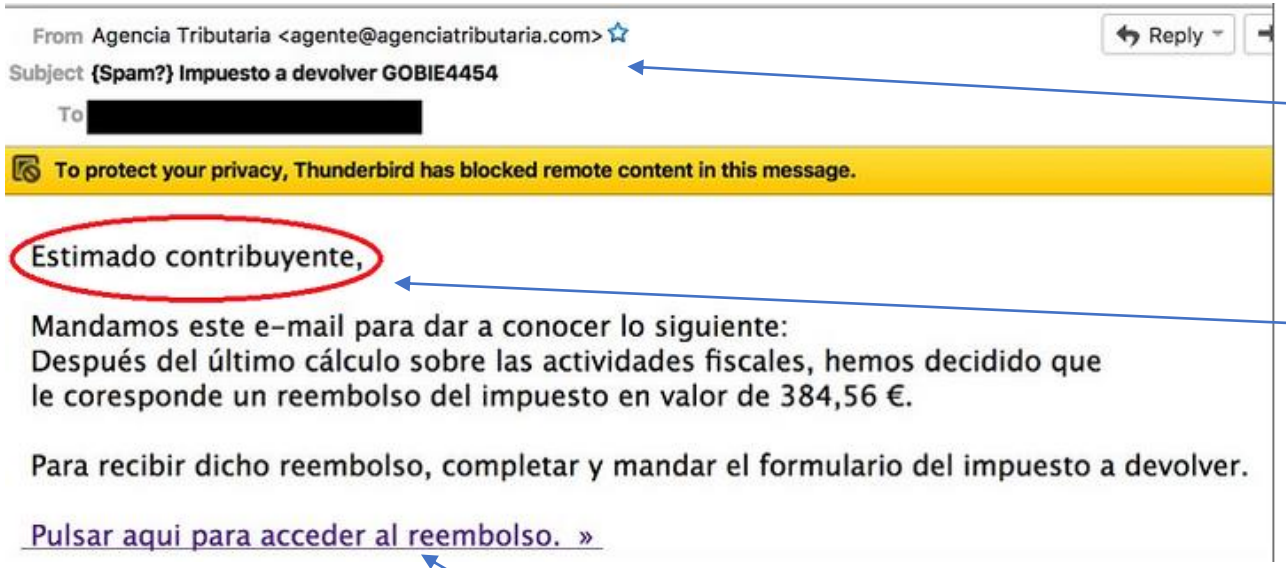


98%

De los ataques utilizan Ingenieria Social

Suplantación de Identidad

Suelen valerse como hemos visto, de la suplantación de identidad a un banco o institución, para dar sensación de seguridad, como veremos en este ejemplo:

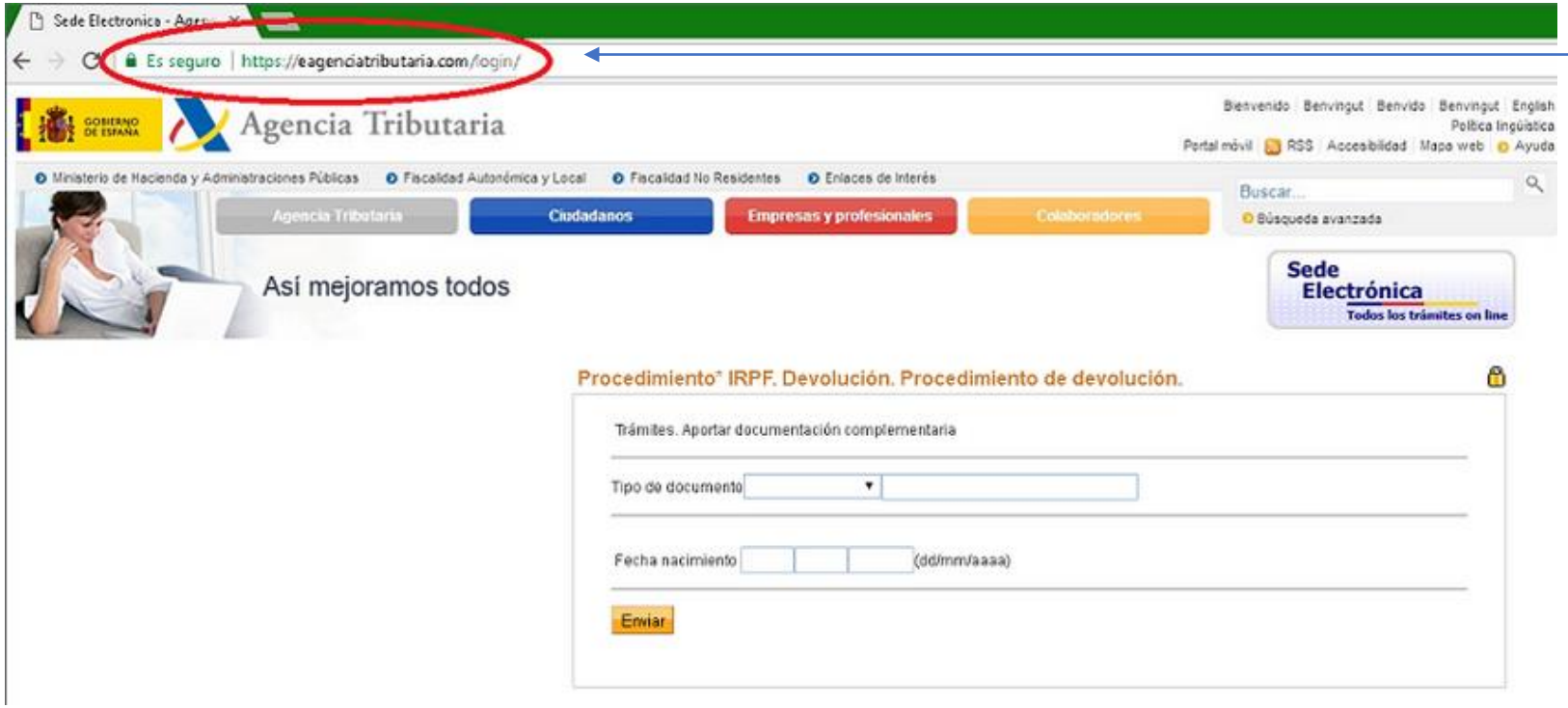


En este caso, se hacen pasar por la agencia tributaria, usando el dominio @agenciatributaria.com. El oficial es @hacienda.gob.es.

Mensaje genérico, sin nombre ni datos adicionales. El ofrecer dinero gratis suele ser un incentivo muy grande.

Los enlaces que no muestran la dirección suelen ser falsos, es decir, no corresponden con el de la institución a suplantar

Puntos a tener en cuenta



La dirección es lo mas similar posible, para que sea mas fácil pasarlo por alto.

Como se puede observar, la pagina es idéntica a la oficial. Lo que diferencia de quien es la pagina y donde nos estamos conectando es la dirección web, y como hemos visto no es la oficial de Hacienda, la oficial seria https://sede.agenciatributaria.gob.es/

Puntos Clave

La mayoría de ataques de este estilo se pueden evitar si sabemos donde observar para poder identificar si son falsos.

- Comprobar las direcciones para asegurar que sean correctas.
- No actuar por prisa, como hemos visto, evita el poder revisar a fondo el mensaje.
- A ser posible, cuando haya dudas, llamar por teléfono al numero oficial de la institución para comprobar los datos.
- Ante cualquier duda, lo mejor no es hacer nada precipitadamente.
- Siempre que sea posible, ponerse en contacto con el responsable informático para que nos solucione las dudas.
- Mantenerse al día sobre este tipo de ataques, ya que si el usuario sabe identificarlos, no crearan problemas.