GOBIERNO DE ESPAÑA
VICEPRESIDENCIA TERCERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

Seminario web 4 "Introducción al phishing"

Ejercicios

017 TU AYUDA EN CIBERSEGURIDAD
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

ÍNDICE

ÍNDICE DE FIGURAS

1. EJERCICIO PRÁCTICO

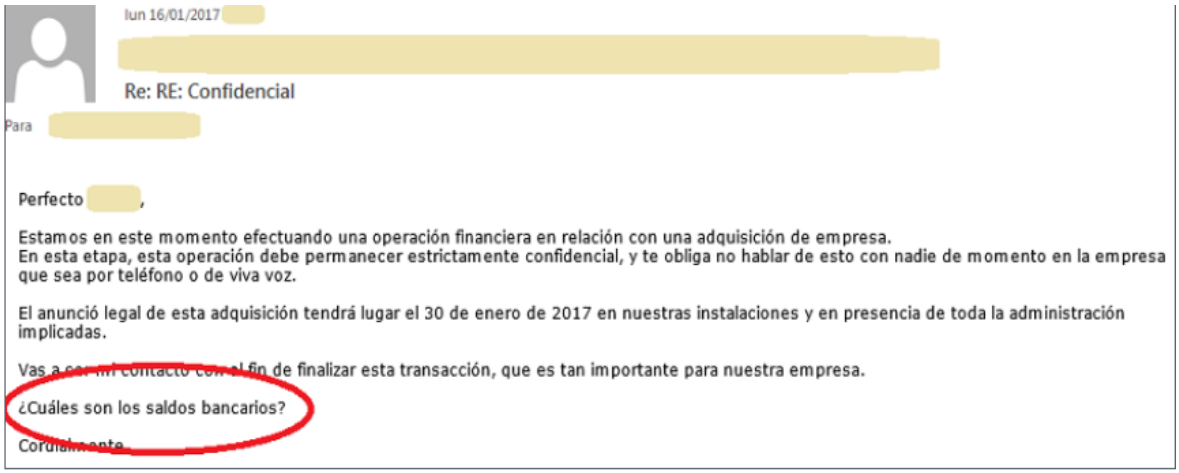
En este ejercicio se trata de discernir entre posibles correos benignos y phishing.

Analiza los distintos elementos del phishing, (pretexto, remitente, URL o adjuntos), en caso de tratarse de una estafa se clasificará entre los distintos tipos de phishing estudiados, es decir:

- Phishing genérico
- Spear phishing
- Whale Phishing
- Cadena de correos
- Smishing
- Spim
- Vishing

En cada caso aparecen distintas imágenes pertenecientes a posibles phishing.

Caso 1


lun 16/01/2017

Re: RE: Confidencial

Para

Perfecto ,

Estamos en este momento efectuando una operación financiera en relación con una adquisición de empresa.
En esta etapa, esta operación debe permanecer estrictamente confidencial, y te obliga no hablar de esto con nadie de momento en la empresa que sea por teléfono o de viva voz.

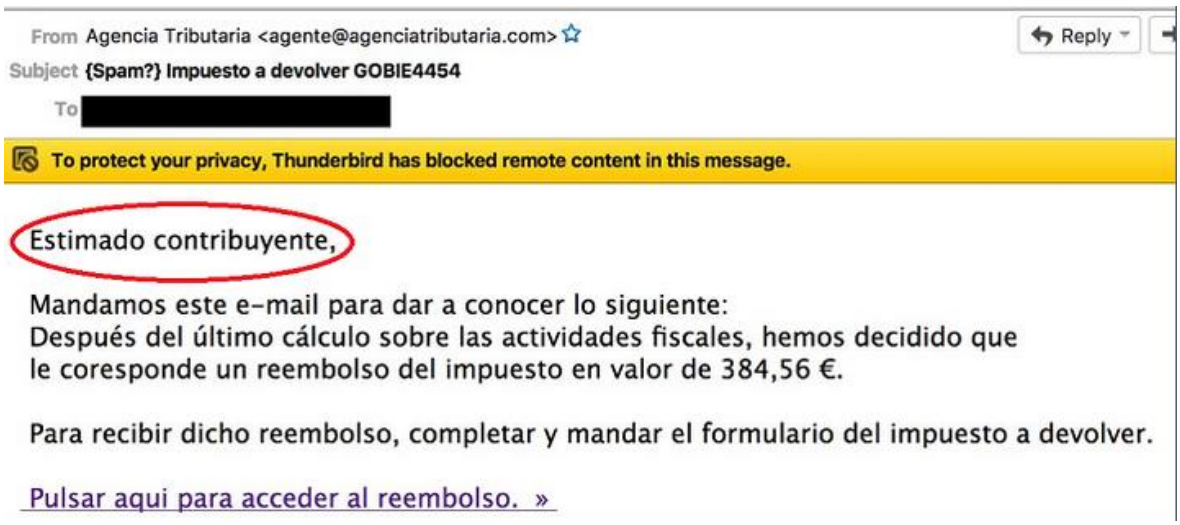
El anunció legal de esta adquisición tendrá lugar el 30 de enero de 2017 en nuestras instalaciones y en presencia de toda la administración implicadas.

Vas a ser mi contacto con el fin de finalizar esta transacción, que es tan importante para nuestra empresa.

¿Cuáles son los saldos bancarios?

Cordialmente

Caso 2


From Agencia Tributaria <agente@agenciatributaria.com>

Reply

Subject {Spam?} Impuesto a devolver GOBIE4454

To [redacted]

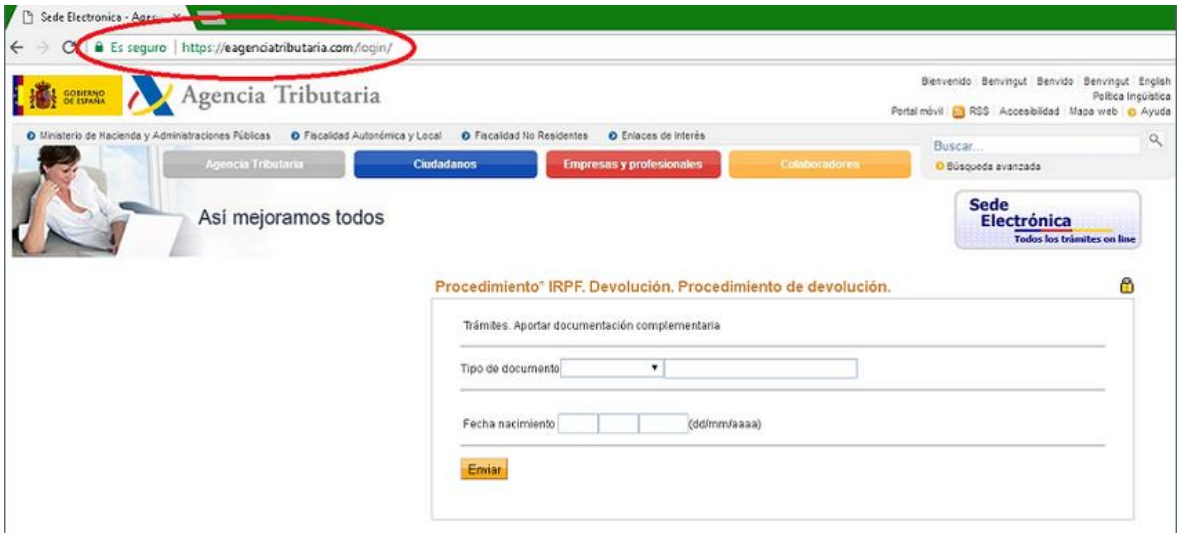
To protect your privacy, Thunderbird has blocked remote content in this message.

Estimado contribuyente,

Mandamos este e-mail para dar a conocer lo siguiente:
Después del último cálculo sobre las actividades fiscales, hemos decidido que le coresponde un reembolso del impuesto en valor de 384,56 €.

Para recibir dicho reembolso, completar y mandar el formulario del impuesto a devolver.

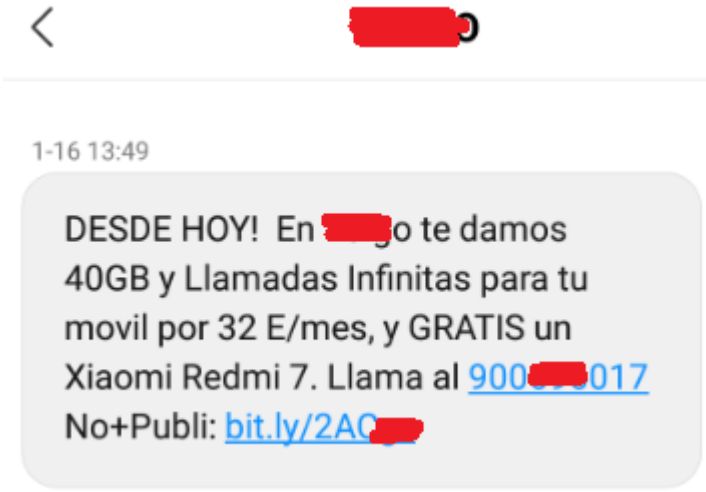
Pulsar aqui para acceder al reembolso. »



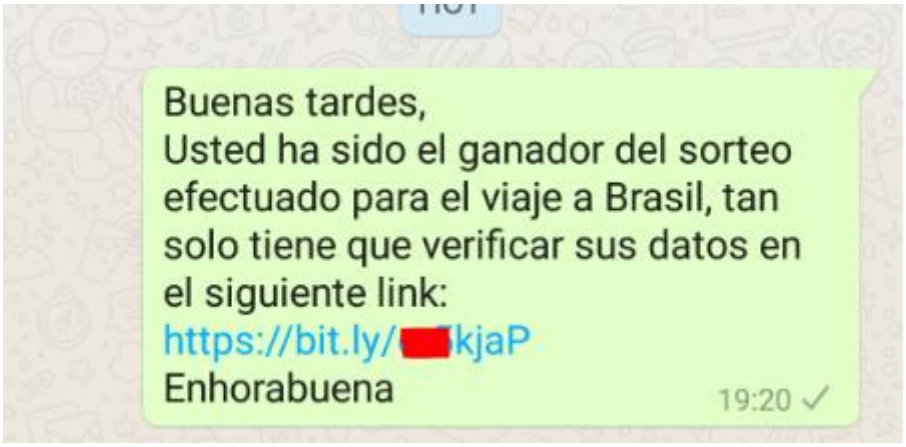
Caso 3

De: **ING** <ing@ing.es>
Date: mié., 29 ene. 2020 8:30
Subject: Ahora invertir a lo grande es para todos
To: <[redacted]@gmail.com>

Caso 4


1-16 13:49
DESDE HOY! En [redacted]o te damos 40GB y Llamadas Infinitas para tu movil por 32 E/mes, y GRATIS un Xiaomi Redmi 7. Llama al 900[redacted]017
No+Publi: bit.ly/2A[redacted]

Caso 5

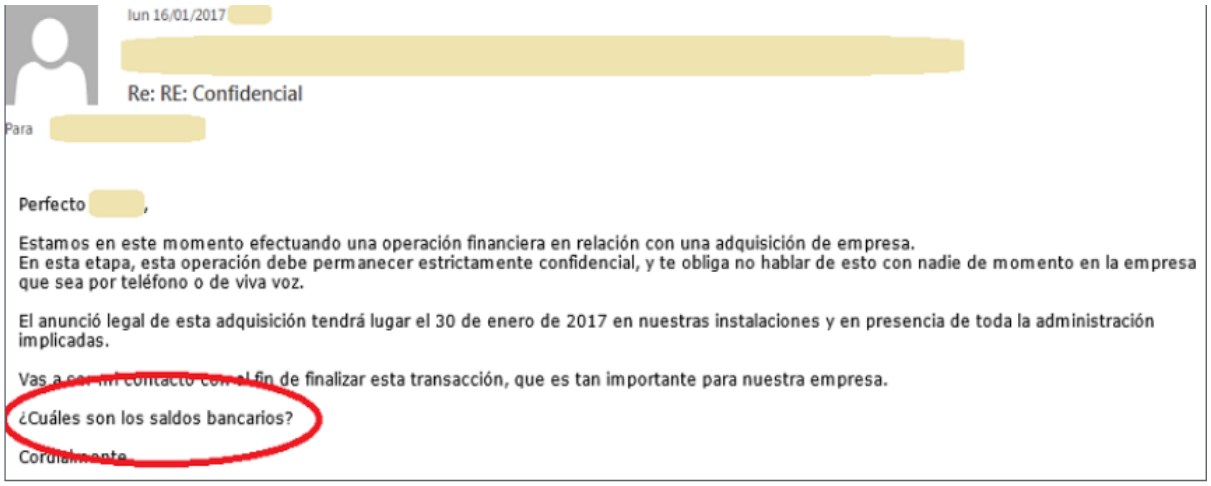

Buenas tardes,
Usted ha sido el ganador del sorteo efectuado para el viaje a Brasil, tan solo tiene que verificar sus datos en el siguiente link:
https://bit.ly/[redacted]kjaP
Enhorabuena
19:20

Solución

Caso 1

Phishing dirigido.

Esto se puede discernir de la elaboración del pretexto y del requerimiento de los datos bancarios para una operación.


lun 16/01/2017

Re: RE: Confidencial

Para

Perfecto ,

Estamos en este momento efectuando una operación financiera en relación con una adquisición de empresa.
En esta etapa, esta operación debe permanecer estrictamente confidencial, y te obliga no hablar de esto con nadie de momento en la empresa que sea por teléfono o de viva voz.

El anunció legal de esta adquisición tendrá lugar el 30 de enero de 2017 en nuestras instalaciones y en presencia de toda la administración implicadas.

Vas a ser mi contacto con el fin de finalizar esta transacción, que es tan importante para nuestra empresa.

¿Cuáles son los saldos bancarios?

Cordialmente

Figura 1 Ejercicio práctico – Phishing dirigido

Caso 2

Phishing genérico

En este caso se trata de un phishing genérico suplantando la identidad de la agencia tributaria.

El phishing es bastante convincente en cuanto al remitente pues el dominio es muy parecido al real.

El pretexto es un buen cebo pues promete a la víctima una cantidad de dinero a devolver.

Este engaño incluye una URL que redirige a una página clonada de la agencia para el robo de datos.

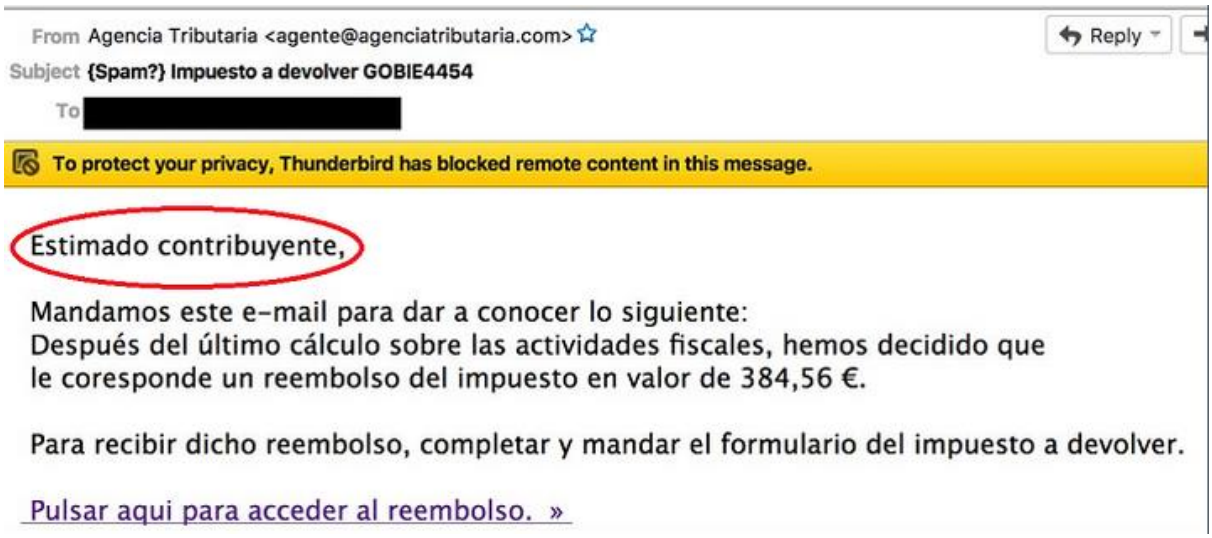


Figura 2 Ejercicio práctico – Correo de phishing

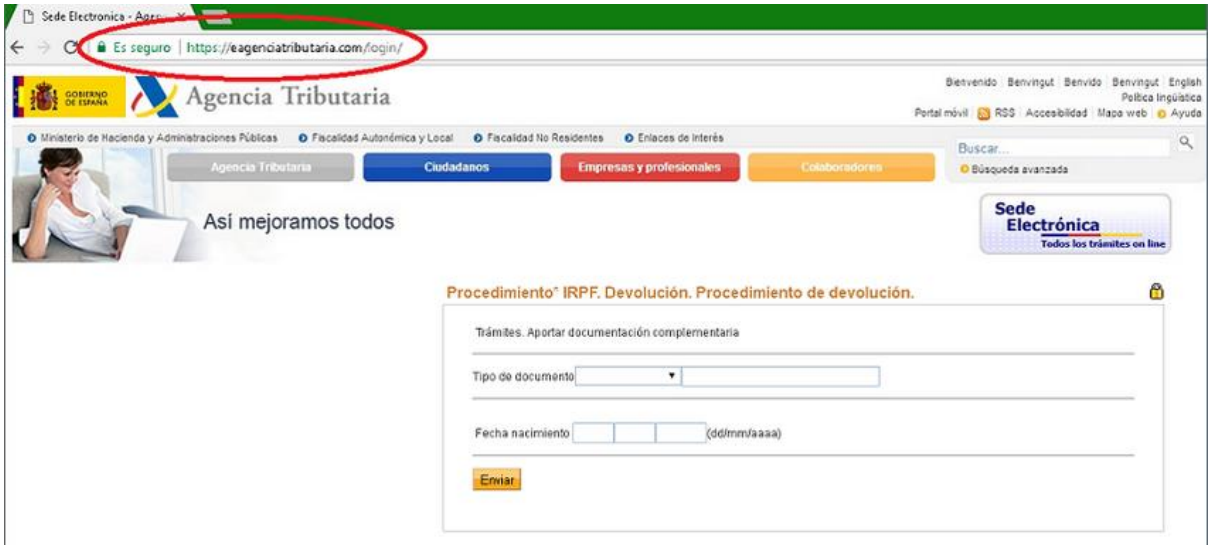


Figura 3 Ejercicio práctico – Portal de phishing

Caso 3

Correo Legítimo

Este correo es totalmente legítimo, el remitente coincide con el dominio de la entidad bancaria, simplemente es un envío de publicidad.

De: **ING** <ing@ing.es>
Date: mié., 29 ene. 2020 8:30
Subject: Ahora invertir a lo grande es para todos
To: <su[redacted]@gmail.com>

Si no ves correctamente este email, haz clic aquí

ING

Publicidad

Ha llegado la simplicidad al mundo de la inversión.

Hola [redacted]

Puede que hasta ahora pensaras que la forma de acceder a determinados productos de inversión, por su complejidad, estaba reservada a unos pocos.

En ING, simplificamos la fórmula para acercar la inversión a todos.
Con **Inversión NARANJA+** ponemos a tu alcance la forma de invertir de los que más saben, desde la cantidad que quieras, con la que podrías sacar partido a tus ahorros.

Los principales mercados del mundo en un solo producto.

A través de **Inversión NARANJA+** inviertes en empresas y gobiernos

Figura 4 Ejercicio práctico – Correo legítimo

Caso 4.

SMS Legítimo

Se trata de un SMS de publicidad de una compañía de telecomunicaciones, si se verifica la URL para desvincularse del servicio o se llama al número proporcionado se podría confirmar.

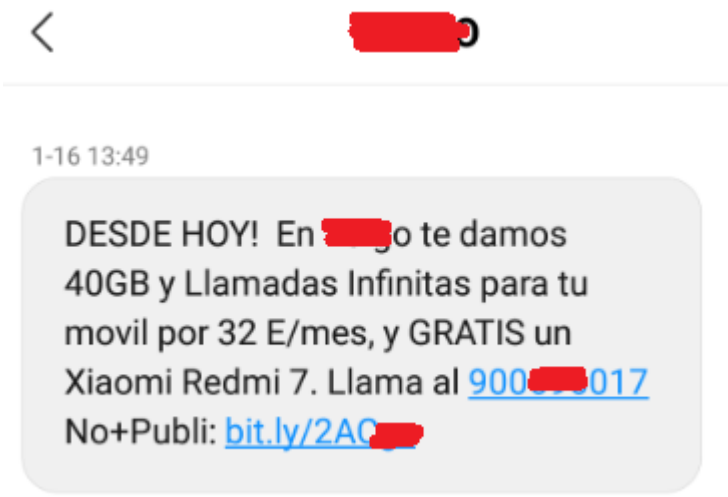


Figura 5 Ejercicio práctico – SMS Legítimo

Caso 5
Spim – WhatsApp

Se trata de un phishing vía WhatsApp. Aún sin verificar la URL, es bastante claro, seguramente ésta lleva al usuario a la descarga de un software malicioso para Android, ya sea para obtener los datos de la víctima, realizar la instalación de software malicioso o algún tipo de estafa.

El pretexto intenta hacer creer a la víctima que ha ganado un premio y que tan solo debe introducir sus datos.

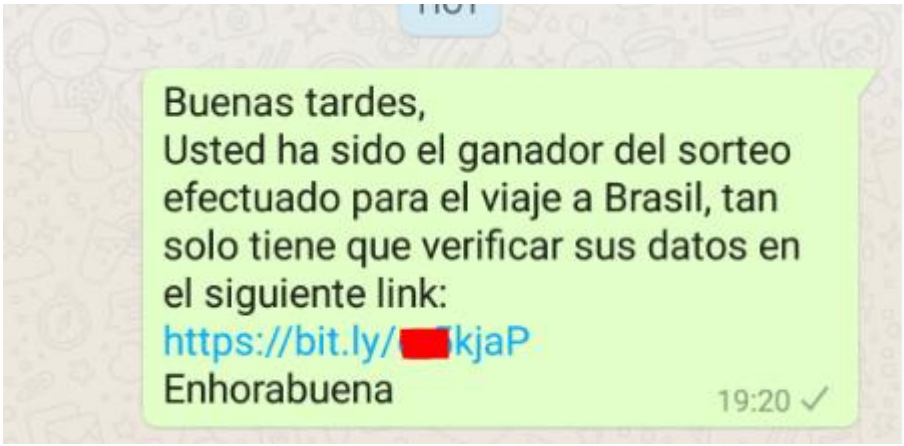


Figura 6 Ejercicio práctico – Spim