CIBER WALL ACADEMY

PHISHING:

¿por qué sigue funcionando?

Marta Barrio Marcos y Carolina Gómez Uriarte

GOBIERNO DE ESPAÑA MINISTERIO DEL INTERIOR
VNiVERSiDAD D SALAMANCA
POLICÍA NACIONAL
GRUPO DE INVESTIGACIÓN BISITE .usal.es
CIBER WALL

¿QUIÉN SOY?

Marta Barrio Marcos

Arquitecta de seguridad de aplicaciones en Beam Suntory

> 9 años de experiencia

CISA, CEH, CSX, OSCP, OSCE

Ponente en congresos de ciberseguridad como NN2019, C1b3rWall Academy 2020

Profesora: ISACA, HackBySecurity, docente en UCLM, EIP y UCAM

https://es.linkedin.com/in/martabarriomarcos
@martrudix

¿QUIÉN SOY?

Carolina Gómez Uriarte

Pentester en VASS

> 3 años de experiencia

Directora de Sh3llCON

Ponente en congresos de ciberseguridad como NN2019, C1b3rWall Academy 2020

Escritora en sh3llcon.org

https://es.linkedin.com/in/carolina-gomez-uriarte
@Carol12Gory

ÍNDICE

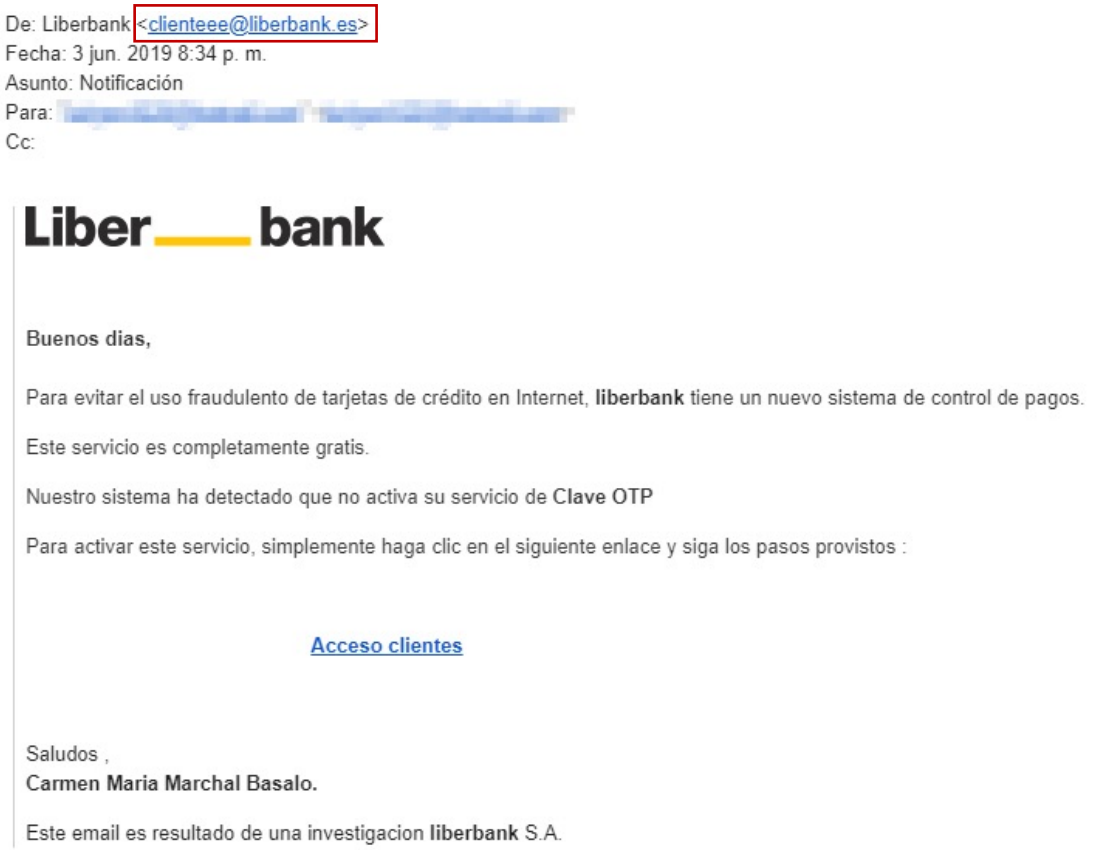
Phishing: ¿Qué es el phishing?

- Suplantación de páginas web, correos electrónicos, etc.
- Uso de logos, textos, imágenes conocidas por el usuario para engañarle y hacerle caer en el engaño.
- Objetivo: credenciales, distribución de malware, suscripciones a listas de spam...

Phishing: ¿Cómo detectarlo?

- Comprobar el remitente
- Comprobar la gramática del correo
- ¿Dónde va el enlace?
- Otras comprobaciones como las cabeceras del correo: IPs, dominios, etc.

Ejemplos de phishing



De: Liberbank <clienteee@liberbank.es>
Fecha: 3 jun. 2019 8:34 p. m.
Asunto: Notificación
Para: [redacted]
Cc:

Liber bank

Buenos dias,

Para evitar el uso fraudulento de tarjetas de crédito en Internet, **liberbank** tiene un nuevo sistema de control de pagos.

Este servicio es completamente gratis.

Nuestro sistema ha detectado que no activa su servicio de **Clave OTP**

Para activar este servicio, simplemente haga clic en el siguiente enlace y siga los pasos provistos :

Acceso clientes

Saludos ,
Carmen Maria Marchal Basalo.

Este email es resultado de una investigacion **liberbank** S.A.

http://nuevadigital.co.vu/?ref=9809C51RO2M5BB3908H8SY1HXTFRLW3D0998D7H897

Ejemplos de phishing

Correos

Entrada - Isciberseguridad 3:06

El equipo de correos: Su paquete est·esperando la entrega.

Para: Instituto Superior de Ciberseguridad

Correos

Estimado cliente,

Verifica tu tarjeta de crédito y su paquete est·esperando la entrega. Confirme el pago en el siguiente enlace, la verificaciôn en lÌnea debe hacerse en los prôximos 15 dÌas antes de que caduque, Siga las instrucciones :

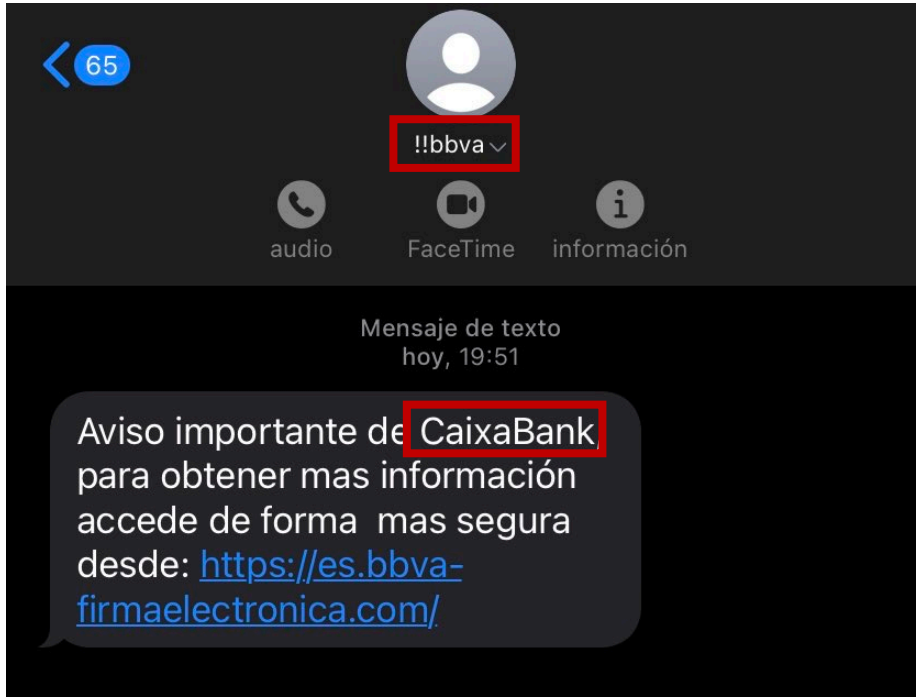
Haga clic aqui:

saludos,
El equipo de correos,

COPYRIGHT TODOS LOS DERECHOS RESERVADOS
Sociedad Estatal Correos y Telégrafos

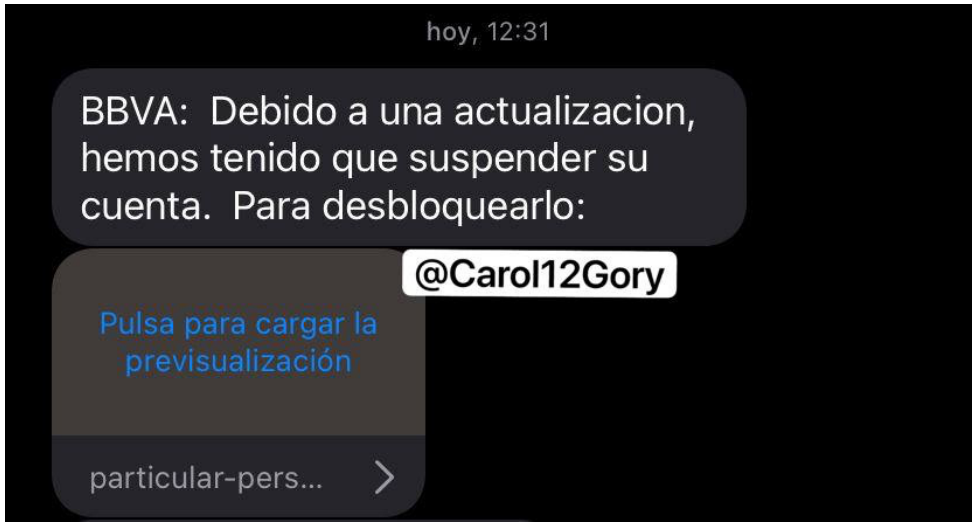
https://twitter.com/juliocesarlopd/status/1331142405052100609?s=20

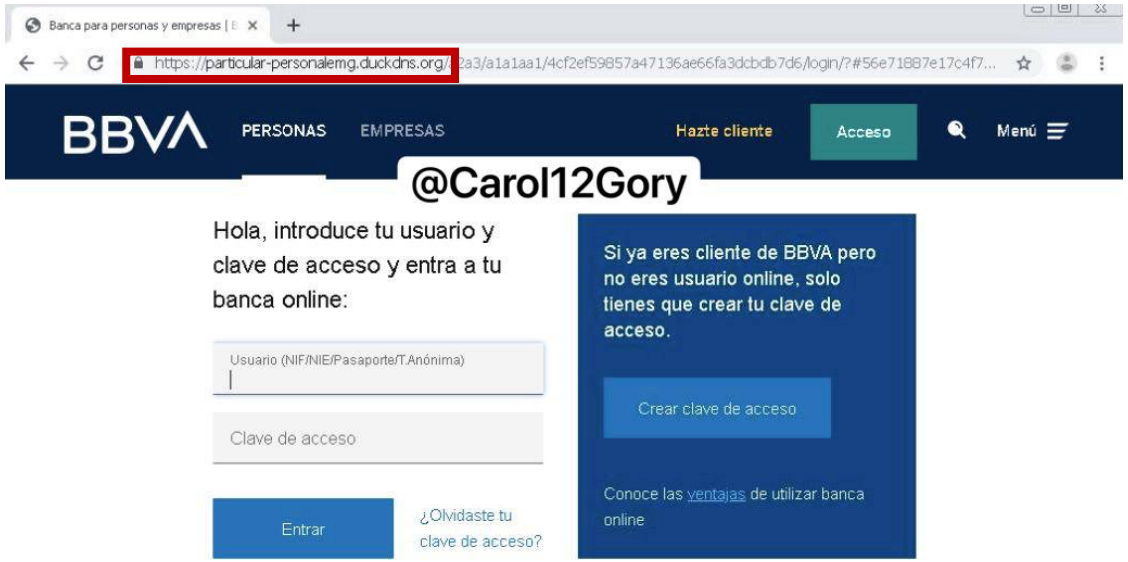
Ejemplos de phishing



https://twitter.com/carol12gory/status/1416094066828267521?s=28

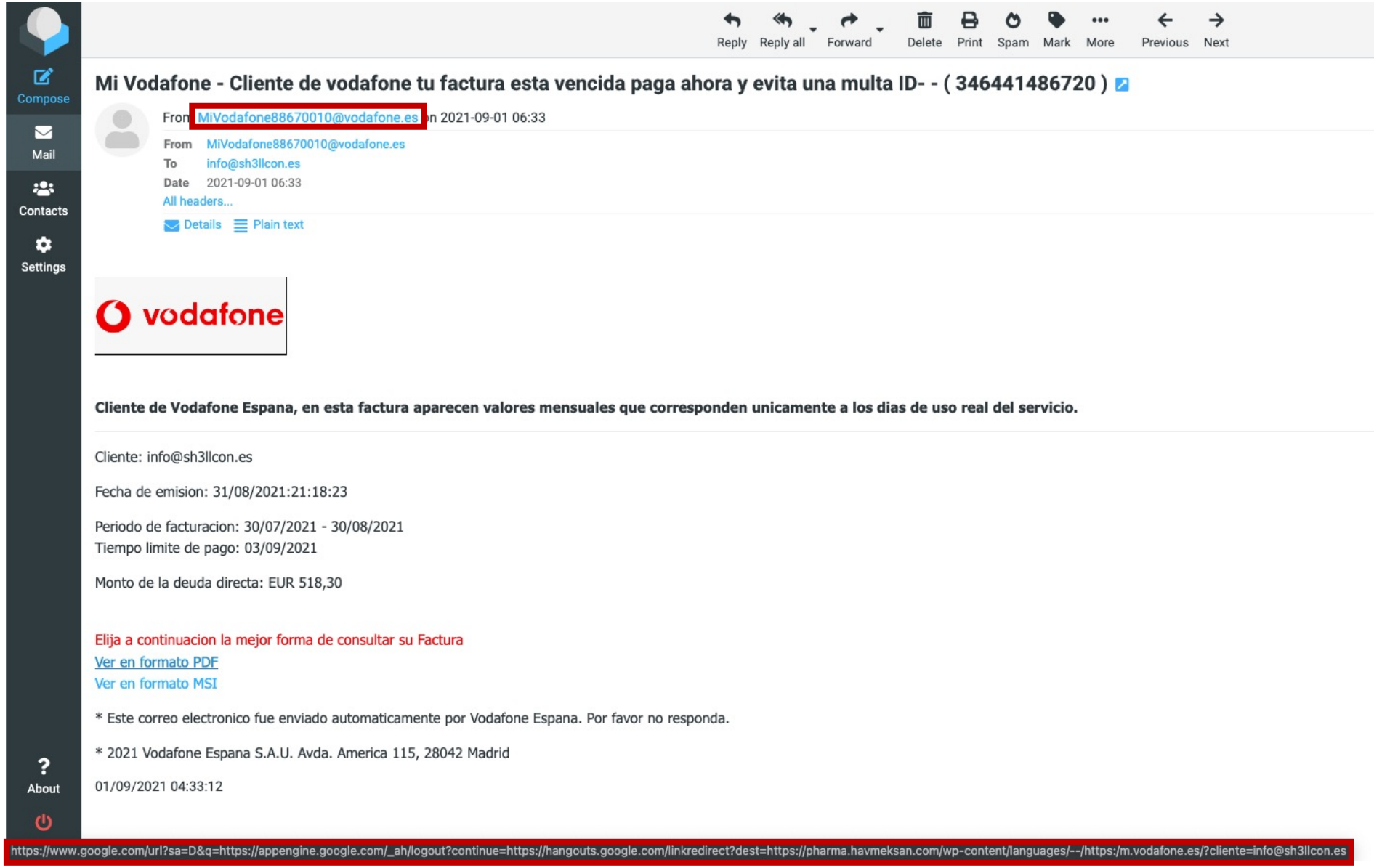
Ejemplos de phishing



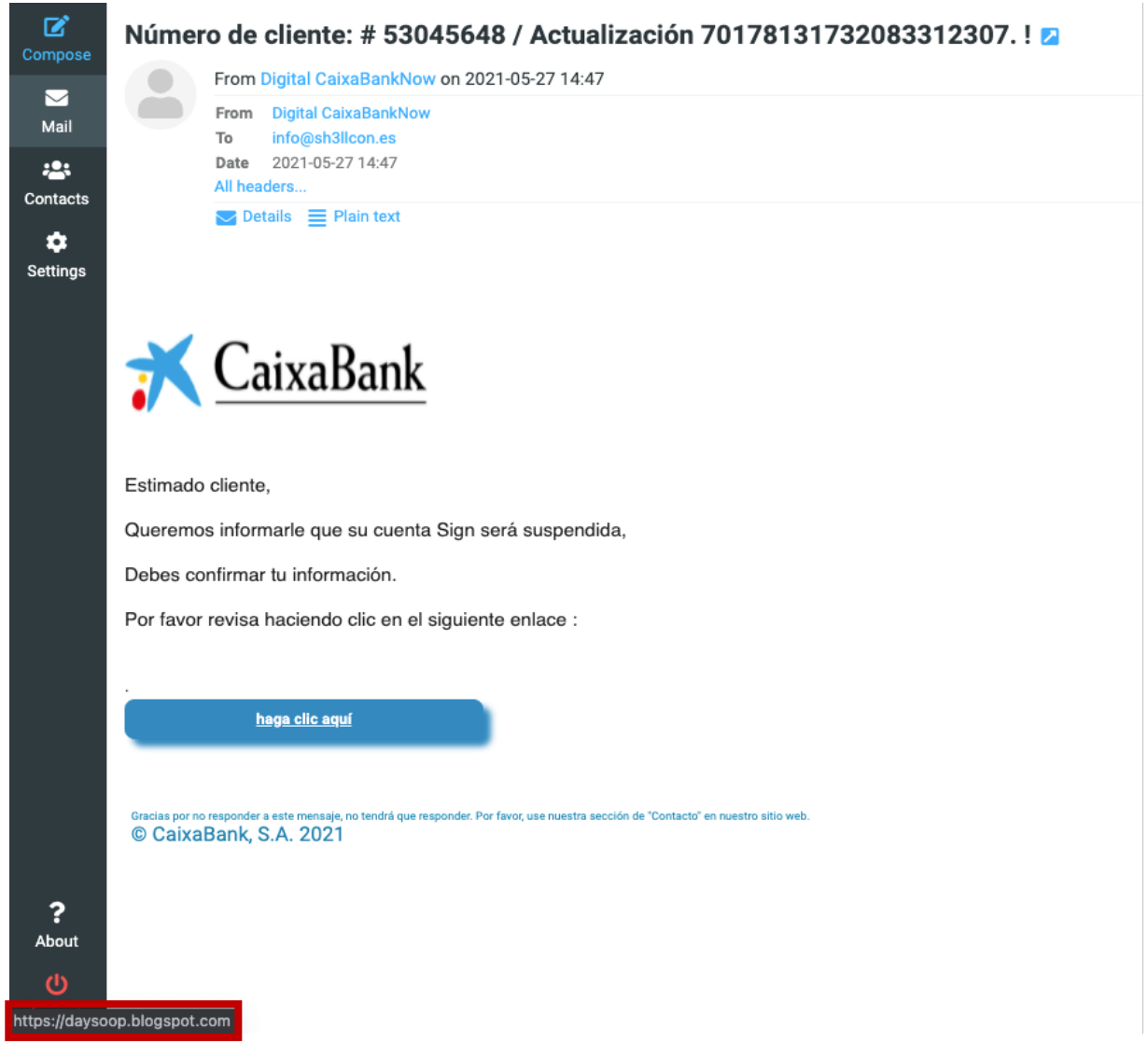


https://twitter.com/Carol12Gory/status/1386635836679131138

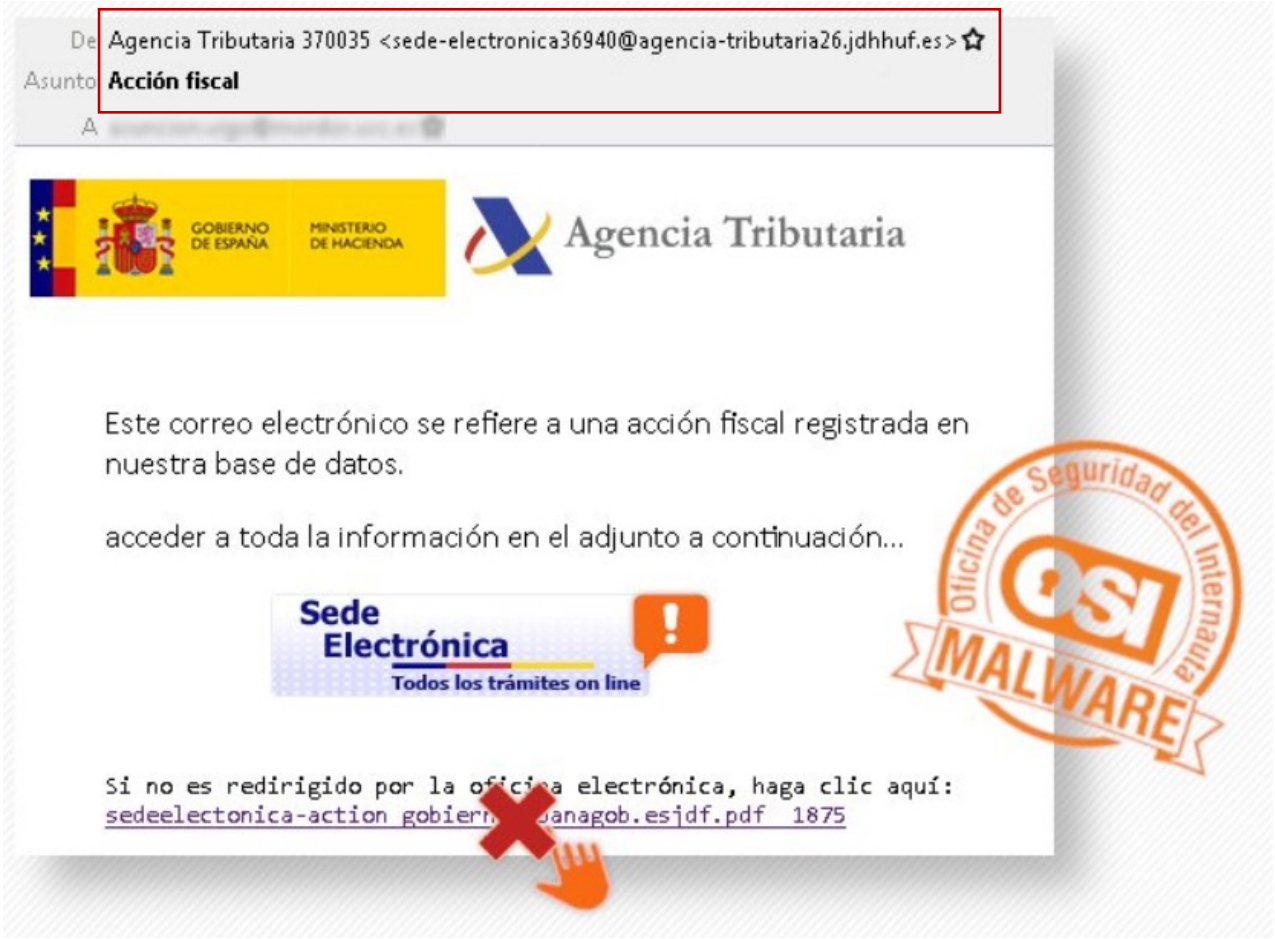
Ejemplos de phishing



Ejemplos de phishing



Ejemplos de phishing



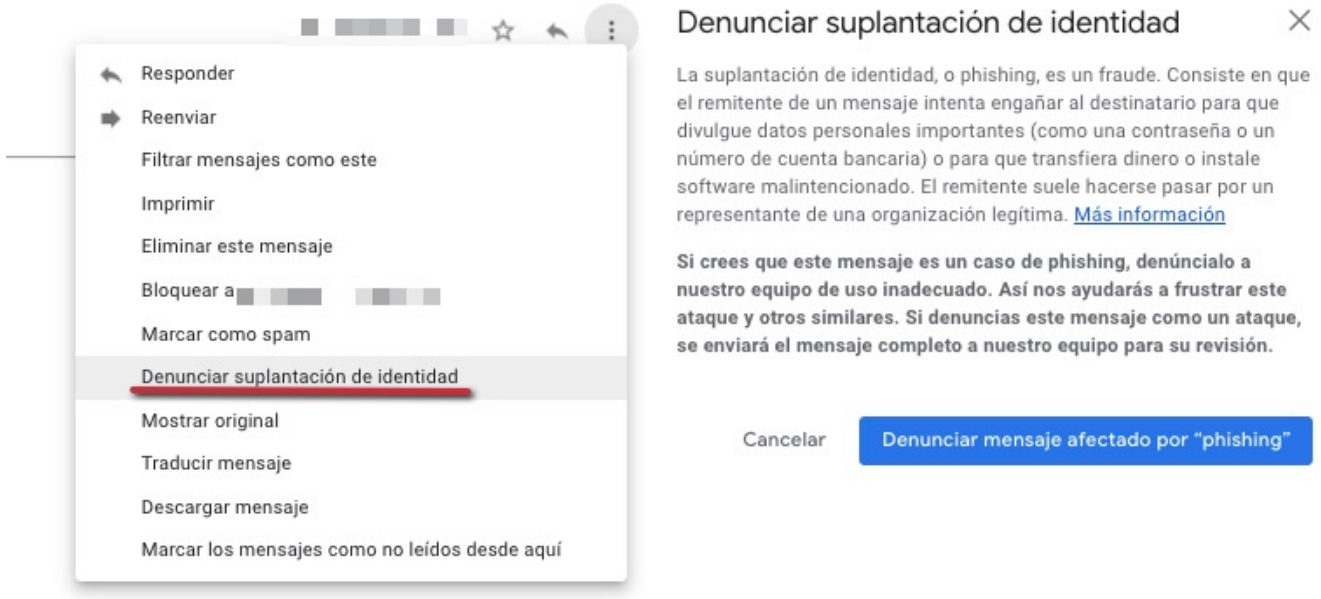
https://twitter.com/osiseguridad/status/1379052098973798400

Phishing: ¿Qué hacer si hemos sido víctimas?

- **Recopilar toda la información posible**: *correos electrónicos, capturas de conversaciones vía email, documentos enviados, etc*.
- Phishing bancario: contactar con la oficina del banco para informarles de lo sucedido
- Modificar la contraseña de todos los servicios en los que se utiliza la misma contraseña (pero no utilizamos la misma contraseña para diferentes servicios, **¿verdad?**)
- Denuncia

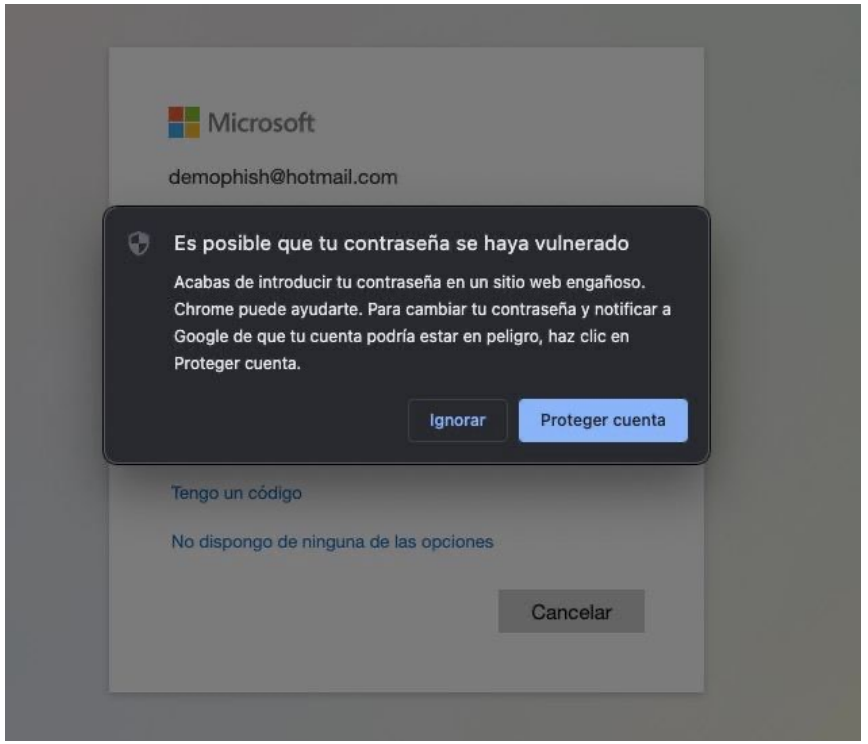
Phishing: ¿Qué hacer si hemos sido víctimas?

- Podemos contactar con:
  - **Servicio** o **empresa implicada**
  - En España: **Oficina Municipal de Información al Consumidor** (OMIC)
  - Denunciar a las **Fuerzas de Seguridad del Estado** (FCSE)
- Reportar a servicios online como Google:



Phishing: ¿Qué hacer si hemos sido víctimas?

- Extra tip: **¿Nuestra contraseña es segura?** ¿Se encuentra en algún leak publicado?
  - HaveIBeenPwned: https://haveibeenpwned.com/
  - Chrome:




C1B3R
WALL
ACADEMY
GRACIAS
@martrudix
@Carol12Gory