



# PHISHING:

## ¿por qué sigue funcionando?

Marta Barrio Marcos y Carolina Gómez Uriarte



# ¿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



1. ¿Qué es el phishing?
2. ¿Cómo detectarlo?
  - 2.1 Ejemplos
3. ¿Qué hacer si hemos sido víctimas?



# 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 <cliente@liberbank.es>

Fecha: 3 jun. 2019 8:34 p. m.

Asunto: Notificación

Para:

Cc:

**Liber bank**

Buenos días,

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

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

Para: Instituto Superior de Ciberseguridad

Entrada - Isciberseguridad 3:06



Estimado cliente,

Verifica tu tarjeta de crédito y su paquete est-esperando la entrega. Confirme el pago en el siguiente enlace, la verificaciôn en línea debe hacerse en los prôximos 15 días 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/juliocesarlop/status/1331142405052100609?s=20>

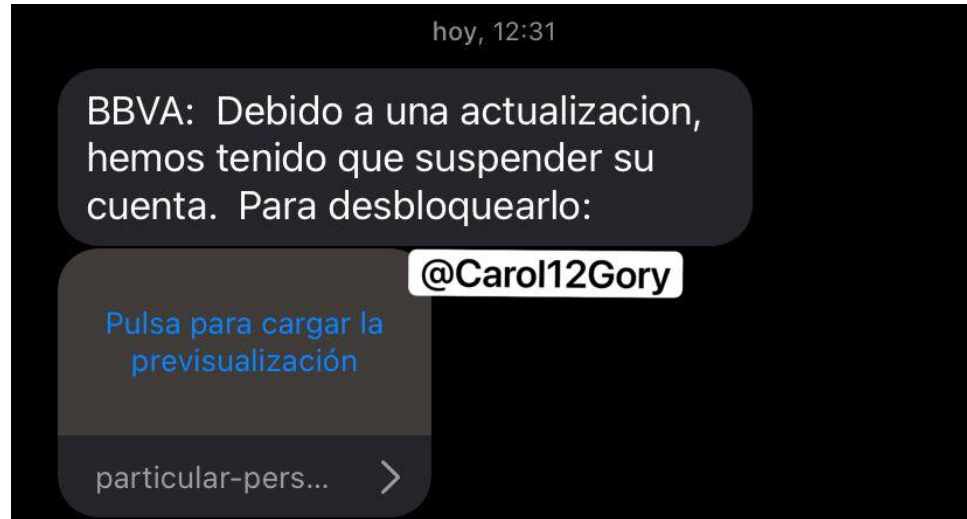


# Ejemplos de phishing



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

# Ejemplos de phishing



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

# Ejemplos de phishing

Compose

Mail

Contacts

Settings

About

Reply

Reply all

Forward

Delete

Print

Spam

Mark

More

Previous

Next

**Mi Vodafone - Cliente de vodafone tu factura esta vencida paga ahora y evita una multa ID- - ( 346441486720 )**

From **MiVodafone88670010@vodafone.es** on 2021-09-01 06:33

From **MiVodafone88670010@vodafone.es**

To **info@sh3llcon.es**

Date 2021-09-01 06:33

All headers...

Details Plain text

Cliente de Vodafone Espana, en esta factura aparecen valores mensuales que corresponden unicamente a los dias de uso real del servicio.

Cliente: info@sh3llcon.es

Fecha de emision: 31/08/2021:21:18:23

Periodo de facturacion: 30/07/2021 - 30/08/2021

Tiempo limite de pago: 03/09/2021

Monto de la deuda directa: EUR 518,30

Elija a continuacion la mejor forma de consultar su Factura

[Ver en formato PDF](#)

[Ver en formato MSI](#)

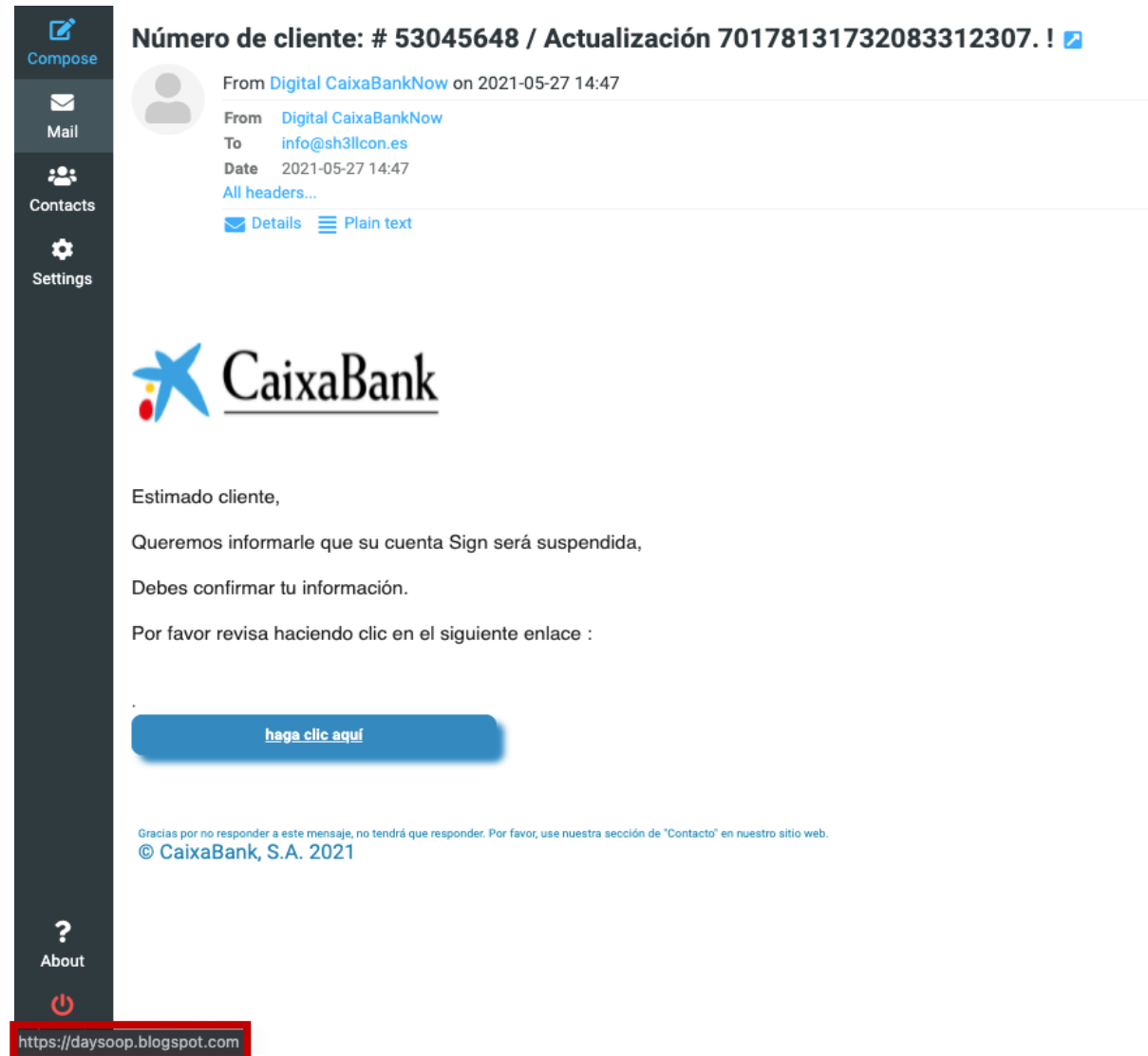
\* Este correo electronico fue enviado automaticamente por Vodafone Espana. Por favor no responda.

\* 2021 Vodafone Espana S.A.U. Avda. America 115, 28042 Madrid

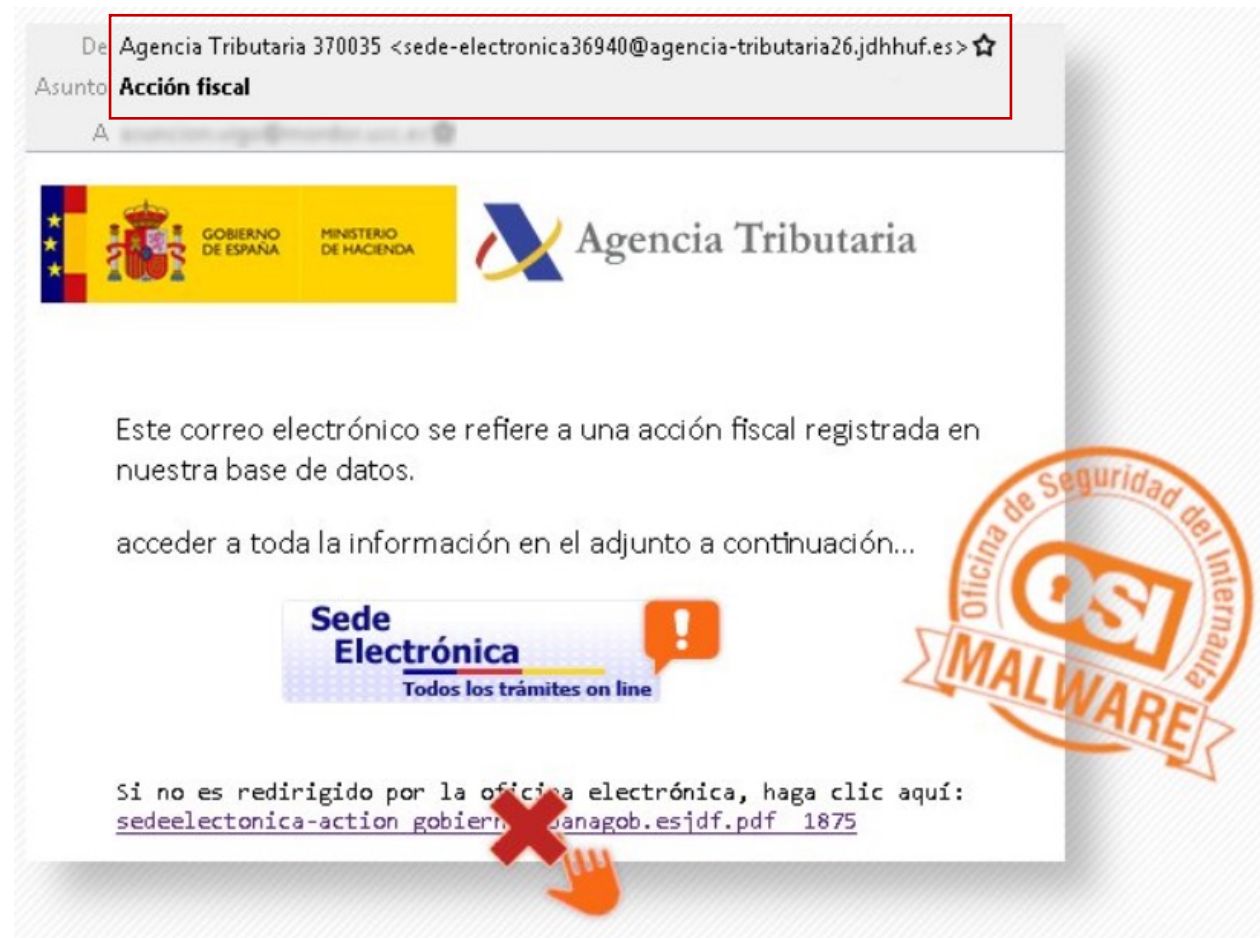
01/09/2021 04:33:12

[https://www.google.com/url?sa=D&q=https://appengine.google.com/\\_ah/logout?continue=https://hangouts.google.com/linkredirect?dest=https://pharma.havmeksan.com/wp-content/languages/--/https://m.vodafone.es/?cliente=info@sh3llcon.es](https://www.google.com/url?sa=D&q=https://appengine.google.com/_ah/logout?continue=https://hangouts.google.com/linkredirect?dest=https://pharma.havmeksan.com/wp-content/languages/--/https://m.vodafone.es/?cliente=info@sh3llcon.es)

# Ejemplos de phishing



# Ejemplos de phishing



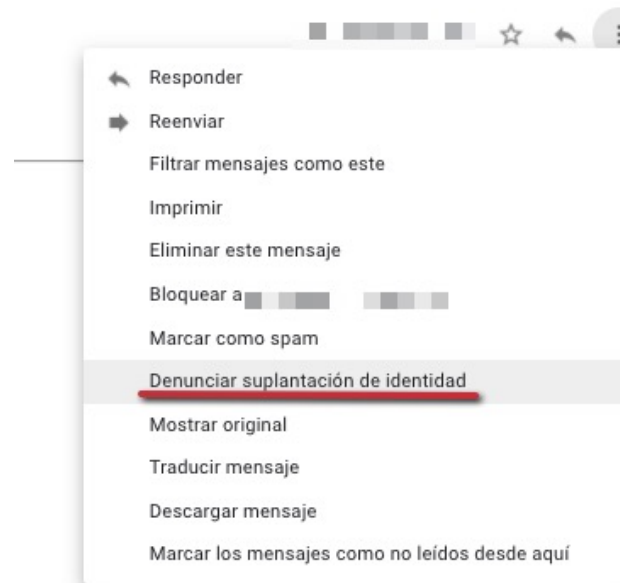
# Phishing: ¿Qué hacer si hemos sido víctimas?

- **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:



## Denunciar suplantación de identidad

La suplantación de identidad, o phishing, es un fraude. Consiste en que el remitente de un mensaje intenta engañar al destinatario para que divulgue datos personales importantes (como una contraseña o un número de cuenta bancaria) o para que transfiera dinero o instale software malintencionado. El remitente suele hacerse pasar por un representante de una organización legítima. [Más información](#)

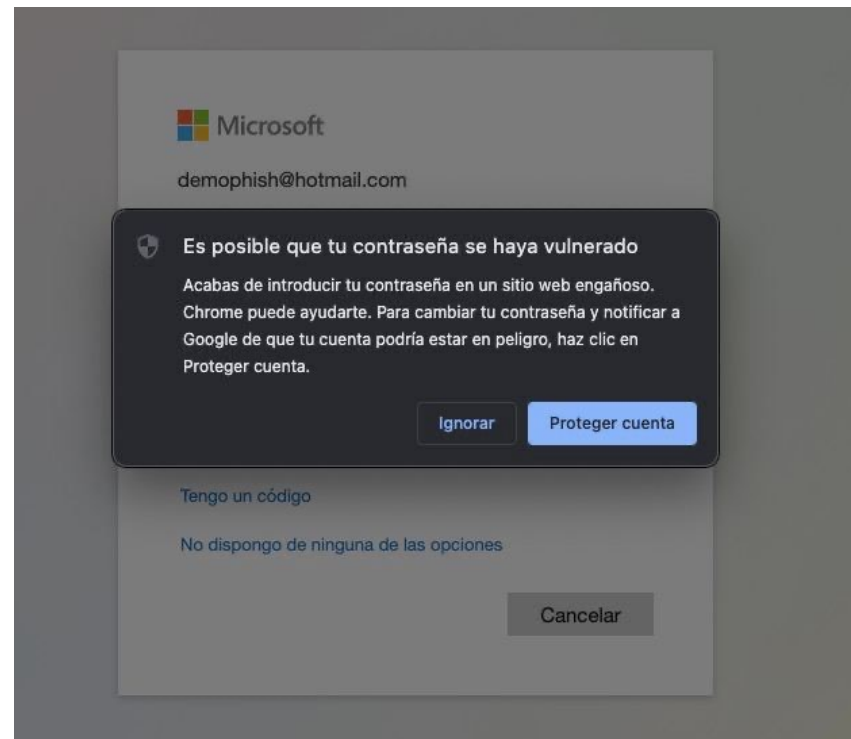
Si crees que este mensaje es un caso de phishing, denúncialo a nuestro equipo de uso inadecuado. Así nos ayudarás a frustrar este ataque y otros similares. Si denuncias este mensaje como un ataque, se enviará el mensaje completo a nuestro equipo para su revisión.

Cancelar

Denunciar mensaje afectado por "phishing"

# Phishing: ¿Qué hacer si hemos sido víctimas?

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





C183R

WALL

— ACADEMY —

GRACIAS

@martrudix

@Carol12Gory