



**INVACI**  
INSTITUTO VALENCIANO  
DE CIBERSEGURIDAD Y TELEMÁTICA

## EBOOK GRATUITO

**Aprende a identificar un ataque de phishing**

---

[www.invaci.es](http://www.invaci.es)





# ÍNDICE

## I. INTRODUCCIÓN

<i>Introducción</i>	<b>4</b>
<i>Qué es el phishing</i>	<b>5</b>
<i>En qué se basa el phishing</i>	<b>6</b>
<i>Cómo reconocer el phishing</i>	<b>7</b>
<i>Métodos de propagación</i>	<b>7</b>

## II. EJEMPLOS REALES

<i>Phishing Agencia Tributaria</i>	<b>7</b>
<i>Phishing DGT</i>	<b>9</b>
<i>Phishing BBVA</i>	<b>10</b>
<i>Phishing Correos</i>	<b>11</b>

## III. HERRAMIENTAS

<i>VirusTotal</i>	<b>12</b>
<i>HavelbeenPwned</i>	<b>15</b>
<i>DeHashed</i>	<b>17</b>

## IV. CONCLUSIONES

**18**



# I. INTRODUCCION

Hoy presentamos un ebook que detalla cómo identificar los principales patrones presentes en los ataques de phishing.

Además, aprenderás herramientas fundamentales para verificar la legitimidad de los sitios web donde introduces tus datos, asegurando la protección de tu información personal y/o corporativa.





## ¿Qué es el phishing?

Técnica utilizada para obtener datos valiosos del usuario que los atacantes pueden vender o utilizar indebidamente con fines nefastos como:

- Extorsión
- Robo monetario
- Suplantación de identidad

La forma más común de phishing consiste en suplantar la identidad de un banco o institución financiera a través de correos electrónicos con el objetivo de inducir a la víctima a completar un formulario fraudulento adjunto al mensaje o a acceder a un sitio web que solicita información confidencial, como datos de la cuenta o credenciales de inicio de sesión.





## ¿En qué se basa el phishing?

El phishing se aprovecha de la curiosidad inherente al ser humano.

Por ejemplo, si una memoria USB aparentemente olvidada se encontrara cerca de la cafetera en la zona de descanso de la empresa o en la entrada de la oficina,

¿cuánto tiempo pasaría antes de que alguien la conectara a su ordenador para ver su contenido?

¿Qué sucedería si el USB contuviera un archivo de Excel titulado "nominafeb2023.xls"?

Muchas personas sucumbirían a la tentación de conocer el salario de un colega y abrirían el archivo. Este escenario ilustra los aspectos psicológicos que los ciberdelincuentes aprovechan mediante técnicas de ingeniería social.

Es importante señalar que los ataques tipo phishing utilizan las técnicas de ingeniería social cada vez más depuradas para aumentar su aparente autenticidad..



## ¿Cómo reconocer el phishing?

Vamos a incluir aquí varios puntos que generalmente cumplen los ataques de phishing y que nos permitirán identificar dichos patrones para detectarlos.

- SALUDOS GENÉRICOS O INFORMALES
- SOLICITUD DE INFORMACIÓN PERSONAL
- SENSACIÓN DE URGENCIA
- GRAMÁTICA POBRE
- CORRESPONDENCIA INESPERADA
- DOMINIO SOSPECHOSO
- OFERTA U OPORTUNIDAD DEMASIADO BUENA



## Método de propagación de phishing

Habitualmente los ataques de phishing utilizan para su propagación el correo electrónico, aunque también es habitual, sobre todo en campañas tipo, la declaración de la renta, el blackfriday, etc. utilizar mensajes de SMS para su propagación.

## II. EJEMPLOS REALES

### Phishing Agencia Tributaria

Como hemos comentado anteriormente, los ciberdelincuentes suelen utilizar las épocas en las que existen campañas tipo la declaración de la renta, blackfriday, navidades, etc. para asegurarse un público potencial mucho mayor en sus estafas.

Como vemos en los dos próximos ejemplos, en ambos se cumplen varios de los patrones indicados anteriormente.



## Agencia Tributaria NOTIFICACION POSTAL



Agencia Tributaria <agencia-tributaria-es@e-sochog.cl>  
Para oscar@oscarpadial.com

Responder

Responder a todos

Reenviar



Wed 7/19/2023 4:04 PM

### ESTE EMAIL SE CORRESPONDE CON UN AVISO DE UNA NOTIFICACIÓN POSTAL.

Le informamos que está disponible una nueva notificación para Titular con los siguientes datos:

- Titular [oscar@oscarpadial.com](mailto:oscar@oscarpadial.com)
- Organismo emisor: Agencia Estatal de Administración Tributaria, con DIR3: EA0028512
- Identificador: 2294032215794
- Concepto: Notificación administrativa
- Vínculo: Titular

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

Le facilitamos un enlace directo a la [notificación](#).

Esta notificación se facilita por vía electrónica de acuerdo con lo previsto en el artículo 42.1 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, que establece la obligatoriedad para los organismos emisores de poner por vía electrónica las notificaciones que se emitan en papel.

La notificación se recibirá en todo caso en papel, aplicándose los plazos que en la misma se indiquen. Adicionalmente podrá recibir esta notificación por distintas vías electrónicas. Si accediera a su contenido 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

## BLOQUEO JUDICIAL - Pendiente financiera - [ id 186091682 ]

AT

Administración Tributaria <impuestos@hacienda.gob.es>  
Para oscar@oscarpadial.com



Responder

Responder a todos

Reenviar



lu. 31/08/2020 3:43

Los vínculos y algunas otras funciones se han deshabilitado en este mensaje. Para restaurar la función, mueva este mensaje a la Bandeja de entrada.  
Haga clic aquí para descargar imágenes. Para ayudarle a proteger su confidencialidad, Outlook ha impedido la descarga automática de algunas imágenes en este mensaje.



[Descargar todo como.zip archivos adjuntos \( 128 kb\)](#)

se anexa el siguiente comprobante fiscal digital

Remitente: Servicio de Administración Tributaria.

Hemos identificado que tienes pendiente de presentar, al 01 de agosto de 2020, lo siguiente:  
A quien corresponda

SERIE Y FOLIO:	2158945
FECHA DE EMISION:	01/08/2020
MONTO TOTAL:	9522.20

Servicio de Administración Tributaria,  
+35 1308 808 500 Capitales y Áreas metropolitanas

APRENDE A IDENTIFICAR UN ATAQUE DE PHISHING



# Phishing DGT

La Dirección General de Tráfico es también una de las entidades que utilizan los ciberdelincuentes para suplantar su identidad y “pescar” datos confidenciales. El caso de las multas de la DGT es uno de los casos que también utilizan bastante la propagación mediante SMS.

**De:** Ministerio del Interior <notificaciones@dgt.ggobs.es>

**Enviado el:** miércoles, 18 de mayo de 2022 9:39

**Para:** oscar@oscarpadial.com

**Asunto:** MULTA NO PAGADA - [ id 190743660 ]



SALUDOS CORDIALES

**Tienes una multa pendiente**

Se ha identificado en nuestro sistema una multa de tráfico no pagada dirigida a usted o su vehículo.

Para ver la notificación

Visite:

[Acceso a mi DGT](#)

Atención:

Para ver la notificación, abra en un sistema (Windows).



hoy, 9:05

DGT: Último recordatorio antes del aumento de su multa pendiente de pago. Consulta tú expediente: DGT: [itsssl.com/dgtes\\_servicio](https://itsssl.com/dgtes_servicio)

## Phishing BBVA

De: Atención al cliente. <de454322636@cern.ch>  
Enviado: lunes, 1 de marzo de 2021 8:30  
Para: [REDACTED]  
Asunto: BBVAes Ref. : 31098545



- \* Remitente: Atención al cliente.
- \* Asunto: su tarjeta será suspendida
- \* Fecha de emisión: 01/03/2021

Desde el 01/03/2021 No puede utilizar su cuenta. Tienes que activar el nuevo sistema de seguridad web. El nuevo sistema garantizará la mejor seguridad en sus operaciones.

**(Ahora active el nuevo sistema de seguridad).**

[Haga clic aquí y reactive su tarjeta.](#) No hay costo alguno para usted.

Gracias por ser cliente de BBVA.

Todo el proceso solo tomará 5 minutos. Debe actuar ahora para corregir el problema lo antes posible.



# Phishing Correos

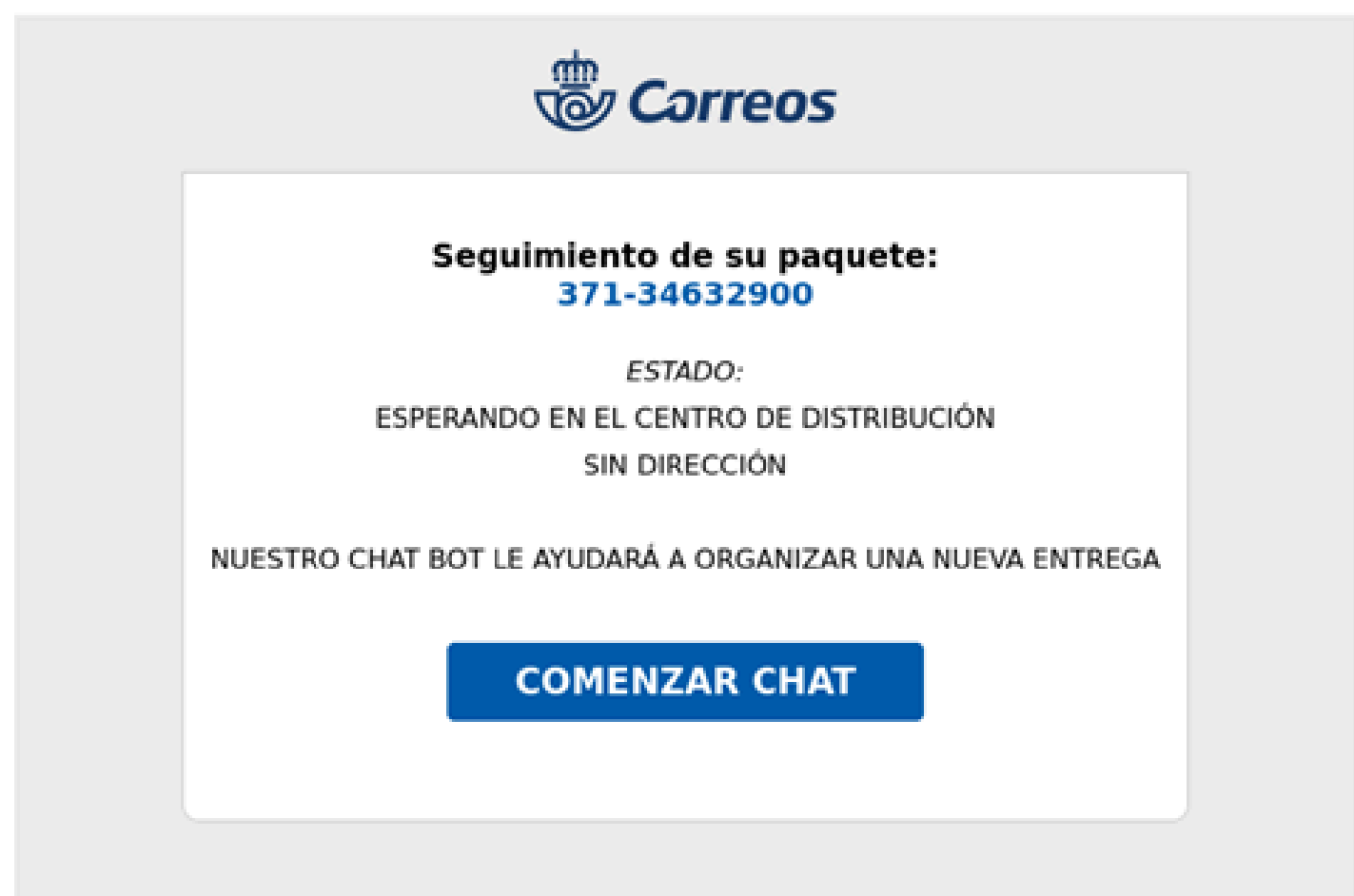
ospadia.....Tu-paquete-ha\_llegado!

Envio-garantizado! <admin.snviypecp3jjcy3s4v@rowbowe.space>  
Para ospadial@gmail.com

178.249.68.206

ospadia

No se han pagado los gastos de transporte de 4,95 €.



## III. HERRAMIENTAS

Después de ver varios ejemplos y las pautas para identificarlos vamos a hablar ahora de las herramientas que nos ayudarán a asegurarnos en caso de duda de si el enlace al que accedemos es correcto o por el contrario es una web ilícita que pretende robar nuestros datos.



# VirusTotal

La primera herramienta de la que hablaremos es VirusTotal que nos ayudará de una manera muy sencilla a comprobar que un enlace es o no legítimo.

Para ilustrar su funcionamiento con un ejemplo real, vamos a utilizar el que hemos visto anteriormente de la DGT (aunque serviría cualquiera de ellos):

**De:** Ministerio del Interior <notificaciones@dgt.ggobs.es>

**Enviado el:** miércoles, 18 de mayo de 2022 9:39

**Para:** oscar@oscarpadial.com

**Asunto:** MULTA NO PAGADA - [ id 190743660 ]



**SALUDOS CORDIALES**

**Tienes una multa pendiente**

Se ha identificado en nuestro sistema una multa de tráfico no pagada dirigida a usted o su vehículo.

Para ver la notificación

Visite:

[Acceso a mi DGT](#)

Atencion:

Para ver la notificación, abra en un sistema (Windows).




Como vemos en este caso el enlace es el botón de “Acceso a mi DGT”.

Lo que debemos hacer es pulsar sobre el botón (o enlace) con el botón derecho del ratón, le damos a copiar hipervínculo y luego lo pegaremos en la web de VirusTotal para analizarlo:



Analyze suspicious files and URLs to detect types of malware, automatically share them with the security community

FILE	URL	SEARCH
		
<p>By submitting data below, you are agreeing to our <a href="#">Terms of Service</a> and <a href="#">Privacy Policy</a>, and to the sharing of your Sample submission with the security community. Please do not submit any personal information: VirusTotal is not responsible for the contents of your submission. <a href="#">Learn more.</a></p>		
<input type="button" value="Choose file"/>		
<small>📄 Want to automate submissions? <a href="#">Check our API</a>, free quota grants available for new file uploads</small>		

Como vemos en VirusTotal podemos analizar tanto un fichero como una URL o dirección web.

En este caso pegamos la dirección obtenida anteriormente en el apartado URL y le damos a “enter” para que lo analice.



4 / 93

4 security vendors flagged this URL as malicious

https://transnewt.com/?a=39915oc=140496c=397115m=35s1=FZ1110\_103aqvy6s3=\_nqj0h23b|00she6s4=o106163fa1cecd65\_0m14&s5=2pfi6e|80870|0187rfgzne|A  
transnewt.com

2022-02-08 12:12:52 UTC  
a moment ago

DETECTION	DETAILS	COMMUNITY
CRDF	Malicious	CyRadar Malicious
Fortinet	Phishing	Netcraft Malicious
Forcepoint ThreatSeeker	Suspicious	Sophos Spam
Abusix	Clean	Acronis Clean
ADMINUSLabs	Clean	AICC (MONITORAPP) Clean
AlienVault	Clean	alphaMountain.ai Clean
Antiy-AVL	Clean	Armis Clean
Artists Against 419	Clean	Avira Clean
BADWARE.INFO	Clean	Baidu-International Clean
benkow.cc	Clean	Bfore.AI PreCrime Clean
BitDefender	Clean	BlockList Clean

Como podemos ver en la imagen anterior con el resultado del análisis de VirusTotal, el enlace ya ha sido catalogado como Malicioso o Phishing por empresas como CyRadar o Fortinet.

Para facilitar la comprensión de los pasos anteriores, hemos realizado un vídeo con un ejemplo actual de una phishing utilizando el SMS donde también utilizamos desde el mismo terminal móvil la herramienta VirusTotal para analizar el enlace:

[https://youtube.com/shorts/i\\_c40TuUMMM?feature=share](https://youtube.com/shorts/i_c40TuUMMM?feature=share)



# Have I been pwned?

Otra herramienta muy interesante para saber si tu correo electrónico ha sido vulnerado y es posible que tu contraseña aparezca en algunas de las filtraciones de seguridad realizadas a las multiples empresas y/o servicios a las que, consciente o inconscientemente estamos suscritos, es “Have I been pwned?”

Home Notify me Domain search Who's been pwned Passwords API About Donate

## ';--have i been pwned?

Check if your email address is in a data breach

Generate secure, unique passwords for every account [Learn more at 1Password.com](#)

Why 1Password?

505	10,594,333,080	113,969	199,574,616
pwned websites	pwned accounts	pastes	paste accounts

### Largest breaches

	772,904,991 <a href="#">Collection #1 accounts</a>
	763,117,241 <a href="#">Verifications.io accounts</a>
	711,477,622 <a href="#">Onliner Spambot accounts</a>
	622,161,052 <a href="#">Data Enrichment Exposure From PDL Customer accounts</a>

### Recently added breaches

	1,047,200 <a href="#">StoryBird accounts</a>
	1,906,808 <a href="#">Pixlr accounts</a>
	1,422,717 <a href="#">MeetMindful accounts</a>
	2,811,929 <a href="#">Bonobos accounts</a>
	77,159,696 <a href="#">Nitro accounts</a>



**Breaches you were pwned in**

A "breach" is an incident where data has been unintentionally exposed to the public. Using the 1Password password manager helps you ensure all your passwords are strong and unique such that a breach of one service doesn't put your other services at risk.

- Adobe:** In October 2013, 153 million Adobe accounts were breached with each containing an internal ID, username, email, *encrypted* password and a password hint in plain text. The password cryptography was poorly done and many were quickly resolved back to plain text. The unencrypted hints also disclosed much about the passwords adding further to the risk that hundreds of millions of Adobe customers already faced.  
**Compromised data:** Email addresses, Password hints, Passwords, Usernames
- Bitly:** In May 2014, the link management company Bitly announced they'd suffered a data breach. The breach contained over 9.3 million unique email addresses, usernames and hashed passwords, most using SHA1 with a small number using bcrypt.  
**Compromised data:** Email addresses, Passwords, Usernames
- Cit0day (unverified):** In November 2020, a collection of more than 23,000 allegedly breached websites known as Cit0day were made available for download on several hacking forums. The data consisted of 226M unique email address alongside password pairs, often represented as both password hashes and the cracked, plain text versions. Independent verification of the data established it contains many legitimate, previously undisclosed breaches. The data was provided to HIBP by dehashed.com.  
**Compromised data:** Email addresses, Passwords
- HTC Mania:** In January 2020, the Spanish mobile phone forum HTC Mania suffered a data breach of the vBulletin based site. The incident exposed 1.5M member email addresses, usernames, IP addresses, dates of birth and salted MDS password hashes and password histories. Data from the breach was subsequently redistributed on popular hacking websites.  
**Compromised data:** Dates of birth, Email addresses, Historical passwords, IP addresses, Passwords, Usernames
- MyFitnessPal:** In February 2018, the diet and exercise service MyFitnessPal suffered a data breach. The incident exposed 144 million unique email addresses alongside usernames, IP addresses and passwords stored as SHA-1 and bcrypt hashes (the former for earlier accounts, the latter for newer accounts). In 2019, the data appeared listed for sale on a dark web marketplace (along with several other large breaches) and subsequently began

Si nuestro correo electrónico aparece en alguna de las filtraciones, deberíamos cambiar la contraseña lo antes posible para evitar el acceso a terceros.

Una opción muy interesantes de este servicio es la de suscribirte directamente para que si tu correo aparece en alguna filtración te avisen directamente sin tener que estar comprobandolo cada cierto tiempo:

**Notify me**

Get notified when future pwnage occurs and your account is compromised.

Enter your email address

No soy un robot

reCAPTCHA

Using Have I Been Pwned is subject to the terms of use

notify me of pwnage

email address pwned?



# DeHashed

Otra herramienta muy útil para obtener información sobre si nuestros datos han sido filtrados es DesHashed.

A diferencia de la anterior, DeHashed nos permite realizar búsquedas de más conceptos, como por ejemplo, el usuario, la dirección IP o el número de teléfono:

Protect Your Organization With Breach Monitoring [LEARN MORE >](#)

# DEHASHED

Search

Pricing

Data Wells

Blog

Support

FAQ

API >

WHOIS >

Monitoring >

My Account >

Payments

Settings

Sign Out

TAKE YOUR **PERSONAL** SECURITY TO THE NEXT LEVEL.

**DEHASHED**

**1,453,524,260** COMPROMISED ASSETS

Updated Search Operators and Learn How to Utilize Regex, and the True Power of DeHashed ↗

FIELD(S) Search for anything... SEARCH

Search for specific fields by adding 'fieldname:' before query or by using some premade buttons located to the left of search bar.

by searching on DeHashed you agree to our [Terms of Use](#) & [Privacy Policy](#) ↗



## III. CONCLUSIONES

Para finalizar este ebook queremos dejaros una reflexión que consideramos importante:

***“LA CUESTIÓN NO DEBE SER SI VAMOS A SER ATACADOS O NO,***

***LA CUESTIÓN DEBE SER, CUANDO VAMOS A SER ATACADOS”***

Y cuando ese momento llegue que nos coja lo más preparados posible.

Os dejamos aquí un resumen de las pautas para identificar este tipo de ataques de phishing:

- Remitentes desconocidos y/o falseados (suplantación de identidad)
- Comunicaciones impersonales (Estimado usuario...)
- Asuntos sospechosos (Urgente, Importante...)
- Mala redacción
- Enlaces falseados
- Firmas y otros elementos en el correo.



SI QUIERES RECIBIR MÁS INFORMACIÓN Y  
CONTENIDO GRATUITO SUSCRIBETE A  
NUESTRA NEWSLETER HACIENDO CLICK EN  
EL LOGO



APRENDE A IDENTIFICAR UN ATAQUE DE PHISHING