

# ENTENDIENDO LA MENTE DEL CRIMEN



Campus Tecnológico-Deportivo para  
Jóvenes

Universidad de Oviedo



**JOSÉ MANUEL REDONDO LÓPEZ** PROYECTO "M-31 'SEGURA'" v1.0



Organiza:  
 Escuela de  
Ingeniería  
Informática  
Universidad de Oviedo

Colaboran:

 CITIPA  
Colegio Oficial de Graduados  
en Ingeniería Informática e  
Ingenieros Técnicos en Informática  
Principado de Asturias

 COITPA  
Colegio Oficial de  
Ingenieros en Informática  
Principado de Asturias

 CÁTEDRA CAPGEMINI  
PARA LA TRANSFORMACIÓN  
DIGITAL SOSTENIBLE

# ¡BIENVENIDO!

- ¿Nunca te has parado a pensar que si hay tantas ciberestafas es por dos motivos?
  - Mucho ciberdelincuente: El culpable siempre es el delincuente
    - Y “empresas del crimen”: organizadas, que hasta cotizan por sus empleados (lógicamente con una buena tapadera)
  - Falta de formación de las personas que las reciben: Como lo primero es inevitable (como Thanos 💀) no nos queda otra que protegernos
- Esta presentación quiere dejarte muy claro lo primero, para que hagas mejor lo segundo 😊



La cantidad de delincuentes que hay en Internet (individuales u organizados) es ENORME. No queda otra que aprender “ciberdefensa”. Y para eso, lo mejor es entender bien cómo piensan



La iniciativa  
“Cobra Kali” por  
José Manuel  
Redondo López



### Investigar Redes Sociales

Técnicas de investigación para RRSS

F-31 “Descubierta”



### Virtualización Básica

Creación y uso de máquinas virtuales

R-11 “Príncipe de Asturias”

Rango 1  
(Marinero)



### Investigación de Webs

Detección de webs problemáticas

S-64 “Narval”



### Entendiendo la Mente del Crimen

Mentes criminales y engaño

M-31 “Segura”



### Ataques contra Personas

Ciberacoso

P-74 “Atalaya”

Rango 2  
(Marinero de Primera)



### Ciberseguridad General

Ciberseguridad general para el día a día

F-74 “Asturias”



### Crime-spotting

Ejemplos de fraudes reales para concienciación

“Nautilus”



### Vigilancia de Redes

Entendiendo cómo funcionan las redes modernas

F-83 “Numancia”

Rango 3  
(Cabo)



Y si el cuerpo te pide marcha... ☺



La iniciativa  
"Cobra Kali" por  
José Manuel Redondo  
López



## Introducción a la Ciberdefensa Personal

Técnicas generales contra ciberataques (Niveles A1, A2)  
Cursos G-9, PDI, Pr. UNIDIGITAL. "BPM P-51 'Asturias'"



## Ciberdefensa Personal Avanzada

Técnicas avanzadas contra ciberataques (Niveles B1, B2)  
Cursos G-9, PDI, Pr. UNIDIGITAL. "BPM P-51 'Asturias'"



## Seguridad de Redes

Threat hunting  
TBA. L-52 "Castilla"

## Administración Segura de SO

Infrastructure as Code  
MUINGWEB, OCW. L-62 "Princesa de Asturias"

## Seguridad de Sistemas Informáticos

Capacitación técnica general en ciberseguridad  
Grado en Ing. del Software, OCW. S-81 "Isaac Peral"



## Liderazgo en Ciberdefensa para Equipos

Herramientas y estrategias de protección (Nivel C1)  
Proyecto UNIDIGITAL. "BPM P-51 'Asturias'"



## Innovación e Investigación en Ciberdefensa

Avances e innovación en ciberdefensa (Nivel C2)  
Proyecto UNIDIGITAL. "BPM P-51 'Asturias'"



## Post-Exploiting e Intrusión en Sistemas

Seguridad ofensiva: Post-Exploitación  
TBA. K-329 "Belgorod"



## Defensa contra el Cibercrimen

Identificación y lucha contra el cibercrimen  
Divulgación pública, cursos. P-45 Audaz"



Rango 1  
(Sargento)



Rango 2  
(Suboficial Mayor)



## Investigación con Fuentes Abiertas (OSINT)

Técnicas de investigación con fuentes abiertas  
OCW (parcialmente). "A-21 Poseidón"



Rango 3  
(Capitán de Fragata)



## Desarrollo Seguro de Software

Platform engineering seguro  
Guías INCIBE. F-113 "Menéndez de Avilés"

Rango 4  
(Almirante)



## Protección de Servidores y Aplicaciones Web

CISOs de perfil técnico  
MUINGWEB, Guías INCIBE, Microcredenciales. D-73 y C-33 "Blas de Lezo"

# ÍNDICE



- [Phishing y ransomware](#)
  - [Malware en general y phishing](#)
  - [El ransomware](#)
- [Mentes criminales](#)
  - [Objetivos de un ciberdelincuente](#)
  - [Psicología de los ciberdelincuentes](#)
- [Formas de engaño](#)
  - [Documentos Maliciosos](#)
    - [Documentos con enlaces maliciosos](#)
    - [Documentos con malware dentro](#)
    - [Documentos falsos](#)
  - [Llamadas y mensajes falsos](#)
  - [Webs falsas](#)
  - [Identidades falsas](#)
- [La IA usada para potenciar el engaño](#)
- [El futuro...](#)

# LA MENSAJERÍA EN LA ACTUALIDAD

- Hoy día tienes dos formas de hablar con alguien

- El email, el clásico “boomer”, pero que aún se usa mucho 🤗
- Las **aplicaciones de mensajería instantánea**
- O la **mensajería integrada** en redes sociales, juegos...

- Pero tenlo claro: el **email** es más **inseguro**

- **El emisor se puede falsificar** con bastante facilidad
- **Los contenidos no van cifrados** normalmente
  - *¿Has enviado algo vergonzoso?* ¡Pues se puede interceptar mucho más fácilmente!
- **Consecuencia:** Hay más **fraudes** que por mensajería

- Pero no te engañes: Por ambos sitios te pueden llegar **estafas** en cualquier momento

- Y, de hecho, **son muy similares**
- Tenemos que saber **cómo piensan** quienes las hacen



Internet está plagado de estafadores/as. Esto son hechos, no es algo que me invente yo. ¿Cómo van a llegar a ti? Mandándote un mensaje con malas intenciones, obviamente 😊

# LA MENSAJERÍA EN LA ACTUALIDAD

- Hoy en día hay grandes proveedores “gratuitos” de
  - Email: Gmail, Outlook, Yahoo...
  - Mensajería: WhatsApp, Telegram...
- Pero no son realmente “gratis”, al igual que las redes sociales y otros servicios
  - Recuerda que lo vimos en la F-31 “Descubierta”
  - **Nuestros datos son el pago por usarlos**
- Y dirás: “Bueno, pero nos protegen de posibles ataques a cambio”
  - Y es verdad, pero como se dice siempre, **la seguridad no es perfecta**
  - Los delincuentes **aprenden a saltarse los sistemas de protección**, que deben evolucionar
  - Pero al final **van a por el más obvio**: Tú 😕
  - Por eso es importante que sepas como operan
    - **Porque tú eres el último sistema de protección contra los ataques de los delincuentes**
  - **¿Preparado para “subir de nivel”?** 💪



# PHISHING Y RANSOMWARE

Siempre que pasa algo, es uno de estos dos



# ¿QUÉ VAMOS A VER EN ESTE BLOQUE?



- Cuáles son las principales fuentes de ataques hoy en día
- Cómo actúa un malware típico
- En qué consiste el **phishing** y los tipos que existen
  - Y consejos generales para prevenirlo
- En qué consiste el **ransomware** y cómo actúa
  - Y el enorme daño que puede hacer...

# ¿POR DÓNDE ME PUEDE VENIR EL SUSTO?

- Ciberataques por mensajería hay muchos

- Como se ve en el “Nautilus”

- Pero hay dos que son las “estrellas”

- Infecciones por **malware** (especialmente **ransomware**)

- Está produciendo **pérdidas económicas masivas** a empresas (y personas)
    - Incluso cierre de negocios (**ruina**), hospitales (**muerte**) y paralización de actividades (**miseria**)
    - Lo más probable es que afecte a tu máquina y a todas las de su misma red, porque **se propagan**
      - Tu casa, el trabajo de todos los que viven en ella

- **Te daña a ti, a tus compañeros, a tu familia** y posiblemente **a su medio de vida**

- Ser víctima de timos / **phishing** (cualquier clase de engaño)

- Las principales consecuencias son el **robo de dinero y de información personal** (privada, comprometedora...)
    - La información robada **se vende en “mercados del crimen”**
    - O se usa como “tapadera” para hacer más timos (**suplantación de la víctima**)



La “pesca” (de víctimas que caigan en un engaño por falta de formación o tener un descuido o mal día) también se practica en Internet, por desgracia ☹



## Malware en general y su relación con el phishing

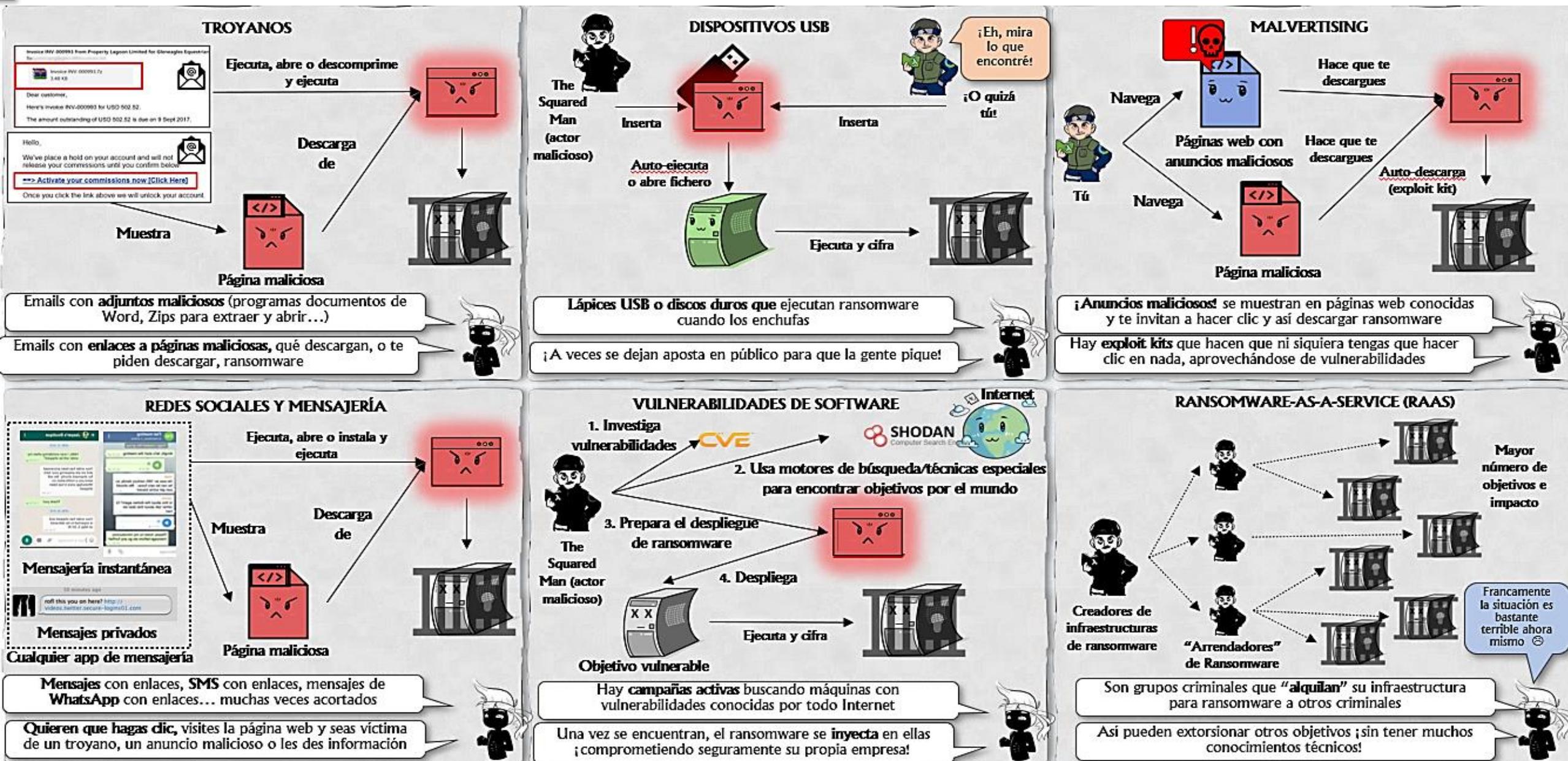
Un malware es software...creado para hacer algún mal





# MALWARE: FORMAS DE QUE NOS LLEGUE...

José Manuel  
Redondo López



# ¿CÓMO ACTÚA UN MALWARE / RANSOMWARE HABITUALMENTE?

- Abres un fichero que tiene “bicho” que te llega junto con un mensaje que te engaña para que lo abras
  - Al hacerlo, infecta tu PC o móvil, sin que tu antivirus lo detecte

## ● Muchos no solo infectan, buscan vías para propagarse

- Empiezan a **buscar otras máquinas** a tu alrededor (en tu red de casa / las del trabajo de tu gente...)
  - La idea es encontrar una vulnerabilidad en ellas que le permita propagarse
  - Carpetas compartidas, falta de parches, problemas de configuración...
- O leen tu **lista de contactos** de tu cuenta de correo
  - Para enviarse a todo el mundo que esté en tu libreta de direcciones

## ● Ahora imaginemos que ha infectado a otros PCs /móviles

- **El proceso se repite con cada usuario infectado y se sigue propagando...**
- Por tanto, la cantidad de **afectados puede aumentar enormemente** de manera muy rápida ☹ (¡la que has liao por no tener cuidao!)



Los antivirus son necesarios, pero no son 100% infalibles. Es como las vacunas: reduces las posibilidades de enfermar, pero nunca son 0%

# ¿QUÉ RELACIÓN HAY ENTRE MALWARE Y PHISHING?

- **¡Toda!**: Los mensajes de phishing son la vía favorita para hacer llegar malware a las víctimas
  - Se denominan “de phishing” si son engañosos, **sin importar el tipo de engaño** que puedan contener
- Pero normalmente se distinguen tres tipos
  - **Phishing “general”**: Mensajes que se envían en masa a ver si alguien pica
    - Envían **millones a coste mínimo**, por lo que muchas veces, aunque pique el 1%, ya sacan rendimiento
  - **Spear phishing** (“pesca con arpón”): Cuando el mensaje se personaliza (y se envía) a un grupo de personas particular porque hay una forma de que los delincuentes tengan sus direcciones
    - Normalmente, **una filtración de datos de una empresa** (y como últimamente hay pocas...)
    - Alumnos y profesores de X colegio, miembros de un equipo de futbol concreto, etc.
  - **Whaling** (“pesca de ballenas”): Un **spear phishing** que se envía a una sola persona, un “**pez gordo**”
    - Van a por alguien que “maneja” 💰, porque saben que si lo consiguen van a tener un gran beneficio
    - El mensaje está totalmente personalizado para esa víctima concreta
      - Investigándola, mirando sus contactos...
      - Hacen una inversión en investigación para sacar luego un “**rendimiento**” de ella
      - Hasta en esto hay clases...

# PHISHING



José Manuel  
Redondo López

## ● A “los pobres” nos “toca” el general o el spear phishing

- Mensajes imitando a los de la empresa real
- Bancos, compañías de transporte, de tarjetas de crédito, proveedores de email, redes sociales, servicios (Amazon, PayPal, eBay, Netflix...)...
- Con webs asociadas falsas, **clonando / imitando la original**

## ● Además de propagar malware, buscan los datos de la víctima

- Ej.: El usuario que tiene la víctima dado de alta en la empresa suplantada
- A través del **enlace** que contiene el mensaje
- La víctima intenta entrar en su cuenta en la página falsa y... \*

# DECÁLOGO ANTI-PHISHING

**EL PHISHING** es un ataque que se inicia enviando a la víctima una comunicación en la que, suplantando a una entidad conocida, le piden que haga clic en un enlace, descargue un fichero o envíe información sensible.

El objetivo es **robar** cuentas, contraseñas y otros datos, o **infectarle** con malware.

SIGUE ESTE DECÁLOGO PARA HACERLE FRENTE.

**Instala un antivirus con antiphishing para correo y páginas web. Manténlo actualizado, con las firmas al día y activado.**

**Actualiza el software de tus sistemas y de tu web** en cuanto conozcas que hay una actualización, pues se aprovechan de estos fallos para instalar el malware.

Permanece atento para reconocer los ataques de **ingeniería social**. Si tienen prisas, te adulan o te amenazan, ¡desconfía!

Si tienes dudas de la veracidad del mensaje o de su procedencia, **contacta por otro medio con el remitente** y confirma que realmente te ha enviado ese mensaje antes de responder o hacerles caso.

No hagas clic en **una URL** para introducir tus datos sin antes pasar el ratón sobre el enlace para comprobar si es legítimo el sitio a donde te dirige.

Desconfía de las **URL acortadas**, pues no se puede comprobar si el destino es legítimo o no. Los sitios legales no las utilizarán para pedirte datos.

Antes de hacer login en una web, **comprueba su identidad**: consulta los datos de certificado, en el candado de la barra de navegación. Verifica que usa <https://>.

Antes de introducir el email, y otros datos sensibles, en una web o en un formulario **lee y comprende la política de privacidad y el aviso legal** para evitar dar tu consentimiento a que cedan esos datos a terceros y terminen en manos de ciberdelincuentes.

Al descargar un fichero no hagas clic en «habilitar el contenido» salvo que confies en la fuente de dónde procede. Si al descargar un fichero te solicita permiso para **habilitar el contenido**, no te fies, podría iniciarse la descarga del malware.

Ante la menor sospecha: **borra el mensaje o cuelga esa llamada!**

Fuente: INCIBE

# PHISHING Y PRECAUCIÓN

- El problema es **tan grave** que el INCIBE (y muchas otras instituciones) tiene muchísimo material de formación para prevenirlo

- <https://www.incibe.es/ciudadania/tematicas/ingenieria-social-fraudes-online/phishing>
- Voy a enseñarte unos cuantos, **pero te recomiendo que entres y leas todo lo que tienen**

## ¿QUÉ ES EL PHISHING ?

Fraude que consiste en enviar correos electrónicos que suplantan a entidades y empresas conocidas para engañar a los usuarios bajo cualquier excusa y robar así sus datos personales, bancarios, contraseñas, etc.



**¿Cómo actuar ante él?**  
¡No respondas al email sospechoso! En caso de duda, contrasta la información con la empresa que supuestamente te está contactando a través de sus canales oficiales.

1 La dirección del remitente no coincide con el nombre de la empresa o entidad que dice ser.

2 El mensaje contiene errores gramaticales o de ortografía.

3 Apela a tus emociones para que accedas a las peticiones de manera urgente.

4 Facilita un enlace para realizar la gestión en cuestión.

5 Lleva adjunto un archivo que supuestamente es un documento oficial.

Has caído en el engaño? Sigue estos consejos:

- 1 Cambia tu contraseña lo antes posible si la has facilitado. Y actualiza la de otros servicios online en los que utilizarás la misma.
- 2 Contacta con tu entidad bancaria si has proporcionado datos bancarios.
- 3 Realiza búsquedas en Internet de tus datos personales para comprobar que no se estén usando.
- 4 Reenvia el correo fraudulento a INCIBE (incidencias@incibe-cert.es)
- 5 Denuncia ante las Fuerzas y Cuerpos de Seguridad del Estado proporcionando las evidencias.
- 6 Y si aún tienes dudas, contacta con 'Tu Ayuda en Ciberseguridad' de INCIBE, llamando al 017, o a través de WhatsApp (900 116 117) o Telegram (@017INCIBE).




Financiado por la Unión Europea NextGenerationEU

Gobierno de España  
Ministerio de Asuntos Económicos y Transformación Digital

SECRETARÍA DE ESTADO DE INVESTIGACIONES Y PROTECCIÓN DE DATOS

Plan de Recuperación, Transformación y Resiliencia

España | digital

incibe\_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

OSI Oficina de Seguridad del Internauta



# PHISHING Y PRECAUCIÓN

## Cómo identificar un correo electrónico malicioso

Cientos de emails fraudulentos llegan a nuestras bandejas de correo y, aunque muchos son eliminados, otros consiguen su objetivo, ser leídos. Dependiendo de nosotros saber cómo identificar un correo electrónico malicioso:

### 3 OBJETIVO DEL MENSAJE

¿Cuál es el objetivo del correo?

Una entidad de servicios como el banco, suministros del hogar (agua, gas) u otros nunca te pedirá tus datos personales por correo. Además, si es de carácter urgente, amenazante o con ofertas y promociones muy atractivas, es muy posible que sea un fraude.

### 5 ENLACES

¿Los enlaces llevan a una página legítima?

Sitúa el cursor encima del enlace, o mantén presionado el enlace en dispositivos móviles, podrás ver la URL real a la que redirige. Si no coincide o es una web sin certificado de seguridad (<https://>), no hagas clic.

### 1 REMITENTE

¿Esperabas un email de esta persona/entidad?

Comprueba que el email coincida con la persona o entidad remitente que dice ser o si está suplantando a alguien.

1

SocialNet <info@socialneet.es>  
para mí ▾

2

Espacio de almacenamiento extra  
SocialNet <info@socialneet.es>  
para mí ▾

### 3

Estimado usuario de SocialNet

Le notificamos que debido al hecho de haber superado el espacio de almacenamiento estandar de tu red social hemos procedido a cargar en su cuenta un cobro por este servicio de almacenamiento extra y le enviamos la factura que podra descargar desde este email o accediendo a su área cliente:

Gracias por confiar en nosotros

Un cordial Saludo

SocialNet

<http://social.net/do/trkln.php?>

5

W Factura.doc

6

W Factura.doc

### 2 ASUNTO

¿Capta tu atención el asunto del correo?

La mayoría de correos fraudulentos utilizan asuntos llamativos e impactantes para captar tu atención. Ten en cuenta esta consideración.

### 4 REDACCIÓN

¿Tiene errores ortográficos o parece una mala traducción de otro idioma?

Revisa la redacción en busca de errores de ortografía o gramaticales. Además, si no está personalizado o parece una traducción automática, sospecha.

### 6 ADJUNTOS

¿Contiene un archivo adjunto que no estabas esperando o es sospechoso?

Analiza los adjuntos antes de abrirlos, puede tratarse de un malware.

Los antivirus y analizadores de ficheros te ayudarán a identificar si están infectados.



Finalmente, no olvides utilizar el sentido común y aplicar todos los contenidos que se encuentran en la OSI para convertirte en un usuario ciberseguro.

¡Sigue estas pautas y disfruta de un correo electrónico libre de riesgos!

# PHISHING Y PRECAUCIÓN

## CAMPAÑAS DE PHISHING



### ¡¡ESTATE ATENTO!!

Es habitual que cada cierto tiempo se lancen ataques de Phishing suplantando la identidad de Organizaciones y Bancos.

Estos correos contienen mensajes fraudulentos para los ciudadanos requiriendo sus datos personales o credenciales de accesos a través de enlaces falsos.

### RECUERDA

- Si recibes un correo de estas características **déjalo**.
- **No facilites datos personales** o corporativos en páginas web de dudoso origen.
- Si recibes un correo electrónico de un remitente desconocido **no accedas a sus enlaces** ni descargas sus ficheros adjuntos.
- **Las Organizaciones Legítimas no suelen mandar enlaces.**
- El phishing es una técnica consistente en la **suplantación de identidad** de un organismo o entidad cuya **finalidad es robar tus datos** personales o credenciales de acceso.
- Puedes informarte de este y otros tipos de ataque en las siguientes páginas:



Oficina de Seguridad del Internauta

<https://www.osi.es/es>



Instituto Nacional de Ciberseguridad

<https://www.incibe.es/>



## IDENTIFICA UN CORREO DE PHISHING

- De: Banco <jose ramos@cochesymotos.es> → Remitente desconocido, no coincide con la entidad
- Asunto: Tu cuenta ha sido bloqueada
- BANCO**
- Hola cliente,  
Tu cuenta ha sido bloqueada  
Motivo: alta de información.
- Ingeniería social, genera situación de alarma
- Detalles
- Falta informacion personal.  
Falta informacion de facturacion.  
Falta informacion de la tarjeta de crédito.
- Haga clic en el enlace y siga los pasos para desbloquear su cuenta.
- ENLACE**
- Este mensaje vadirigido, de manera exclusiva, a su destinatario y puede contener información confidencial y sujeta al secreto profesional, cuya divulgación no está permitida por Ley.
- Enlace. Una entidad legítima no pone enlaces
- Firma de correo distinta a la habitual



José Manuel  
Redondo López

# PHISHING Y PRECAUCIÓN: SPEAR PHISHING CON BANCOS

## 'SMISHING' BANCARIO POR SMS

El 'smishing' (combinación de las palabras SMS y 'phishing') es el intento de fraude para obtener información personal, financiera o de seguridad a través de un mensaje de texto.

## ¿CÓMO LO HACEN?

El mensaje de texto normalmente te pedirá que hagas clic en un enlace o que llames a un teléfono para "verificar", "actualizar" o "reactivar" tu cuenta. Pero... el enlace te lleva a una página web falsa, y el número de teléfono es el de un estafador que suplanta a una empresa.

## ¿QUÉ PUEDES HACER?

- No hagas clic en enlaces, adjuntos o imágenes que recibas en mensajes de texto no solicitados sin antes verificar el remitente.
- No te apresures. Tómate tu tiempo y haz las comprobaciones necesarias antes de responder.
- Nunca respondas a un mensaje de texto que te solicite tu PIN o la contraseña de tu banco, o cualquier otra credencial de seguridad.
- Si crees haber respondido a un 'smishing' y proporcionado tus datos bancarios, contacta con tu banco de inmediato.

## BANCA ELECTRÓNICA FRAUDULENTA

Los 'phishing' bancarios vía correo electrónico suelen incluir enlaces que te redirigen a una página web fraudulenta, donde te solicitan tus datos personales y financieros.

## ¿QUÉ SEÑALES TE ALERTARÁN?

Las páginas web bancarias fraudulentas son casi idénticas a su equivalente legítimo. Estas páginas utilizan ventanas emergentes solicitando tus credenciales bancarias. Un banco real nunca las utilizaría.

Estas páginas web muestran habitualmente:

**Urgencia:** no encontrarás este tipo de mensajes en páginas web legítimas.

**Diseño poco cuidado:** ten cuidado con las páginas web que tienen fallos en el diseño o faltas de ortografía.

**Ventanas emergentes:** se utilizan para obtener información delicada sobre ti. No hagas clic ni introduzcas en ellas información personal.

## ¿QUÉ PUEDES HACER?

Nunca hagas clic en enlaces de correo electrónico que te redirijan a la web de tu banco.

Escribe siempre la dirección en el navegador o utiliza un enlace almacenado en tu lista de "favoritos".

Utiliza un navegador con bloqueo de ventanas emergentes.

Si hay algo importante que requiere tu atención, tu banco te alertará de ello cuando accedas a tu banca electrónica.

Los ciberdelincuentes asumen que las personas están ocupadas; a simple vista, estos correos electrónicos falsos parecen ser legítimos.

Ten cuidado cuando uses un dispositivo móvil. Puede ser más difícil detectar un intento de 'phishing' desde tu tableta o móvil.

#Ciberestafa

EUROPOL  
EC3

EF

RG

AEIB

ASOCIACIÓN  
ESPAÑOLA  
DE BANCA

DSN

#Ciberestafa

#Ciberestafa

## 'PHISHING' BANCARIO POR CORREO ELECTRÓNICO

'Phishing' se refiere a correos electrónicos fraudulentos que engañan a los destinatarios para que comparten su información personal, financiera o de seguridad.

## ¿CÓMO LO HACEN?

Estos correos electrónicos:

Pueden **parecer** idénticos al tipo de correspondencia que envían los bancos reales.

## ¿QUÉ PUEDES HACER?

Mantén tus aplicaciones actualizadas, incluyendo navegador, antivirus y sistema operativo.

Presta especial atención si un correo electrónico de tu 'banco' te solicita información confidencial (p. ej. la contraseña de tu cuenta bancaria).

Revisa el correo con cuidado: compara la dirección con los mensajes auténticos de tu banco. Comprueba si existen errores de ortografía o de gramática.

No respondas a un correo electrónico sospechoso, reenvíalo a tu banco escribiendo tú la dirección real.

No hagas clic en el enlace o descargas el archivo adjunto, escribe la dirección real de tu banco en el navegador.

En caso de duda, comprueba la información entrando en la página web de tu banco o por teléfono.

# Aprende a reconocer fraudes en redes sociales y WhatsApp

En nuestras redes sociales y aplicaciones de mensajería instantánea, como WhatsApp, son comunes los fraudes y estafas. Por eso, debemos aprender a reconocerlos y evitarlos:

## 1 Concursos y promociones falsos:

¡He ganado un premio sin haber participado!

Si para recibirlo debo:

- Compartirlo con mis contactos.
- Rellenar un formulario con mis datos personales.
- Efectuar un pago o suscripción a un servicio de pago.
- Aceptar unas bases legales confusas o que se contradicen.



## 2 Secuestro de WhatsApp:

Me han robado mi cuenta de WhatsApp.

Inesperadamente:

- He recibido un código de verificación de la app por SMS para configurar la cuenta en un nuevo dispositivo.
- Un usuario me ha solicitado el código bajo alguna excusa.



## 3 Cuentas falsas:

¿Perfiles de empresas o famosos demasiado parecidos en una red social?

Analizo si:

- Existen dos o más cuentas con un nombre similar y la misma descripción e imágenes.
- El perfil no cuenta con la insignia de verificación de la cuenta (check).
- Comparte enlaces a webs desconocidas o que no tienen nada que ver con la empresa.
- Manda mensajes genéricos solicitando apoyo económico a sus seguidores.



Más información en "Suplantación de identidad y secuestro de cuentas: ¿cómo actuar?".

## 4 Sextorsión y amores en línea:

Buscando pareja encontré un perfil fraudulento.

Se caracteriza por:

- Utilizar perfiles abiertos, con fotografías de personas atractivas.
- Usar fotos robadas de otras cuentas privadas o públicas en Internet.
- Compartir los mismos gustos, aficiones, etc.
- Pedir ayuda económica bajo algún pretexto.
- Solicitar imágenes íntimas o vídeos explícitos.

Más información en "Amor online: ¡Que no te den sapo por príncipe azul!".

## 5 Anuncios de tiendas fraudulentas:

He visto un anuncio que es un chollo.

Pistas:

- Se difunden en redes sociales con promociones muy atractivas.
- Promocionan productos de marcas muy conocidas.
- La URL y estética de la tienda anunciada no tiene nada que ver con la original.
- Las imágenes y descripciones de los productos están poco cuidadas (poca calidad y mala redacción).
- Proporcionan escasa información, o es inexistente, sobre quién es la empresa y cómo contactar con ella.
- No aceptan **métodos de pago seguros**, facilitan un formulario para introducir todos los datos de tu tarjeta, sin ninguna garantía de seguridad.

Más información en "Tiendas online fraudulentas".

Fraudes hay de muchos tipos, desde falsas ofertas de empleo, préstamos falsos, promociones de viaje que no llevan a ningún lado, anuncios de alquileres o venta de productos y viviendas que acaban en decepción.



En la OSI, canal especializado en ciudadanos de INCIBE, encontrarás más información sobre todos ellos, además de recursos para ayudarte a identificarlos y prevenirlos.

[www.incibe.es](http://www.incibe.es) | [www.osi.es](http://www.osi.es)



incibe  
INSTITUTO NACIONAL DE CIBERSEGURIDAD



osi  
Oficina de Seguridad del Internauta



# PHISHING Y PRECAUCIÓN



José Manuel  
Redondo López

- El mejor material de formación y concienciación desde cero que tiene el INCIBE es “Experiencia senior”

- <https://www.incibe.es/ciudadania/experiencia-senior>
- Totalmente gratuito, adaptado a TODOS y con ejercicios para practicar
- ¡Léetelo para estar mucho más protegido!

Fuente: INCIBE:

<https://www.incibe.es/ciudadania/experiencia-senior/que-hacer-si-eres-victima-de-un-fraude>

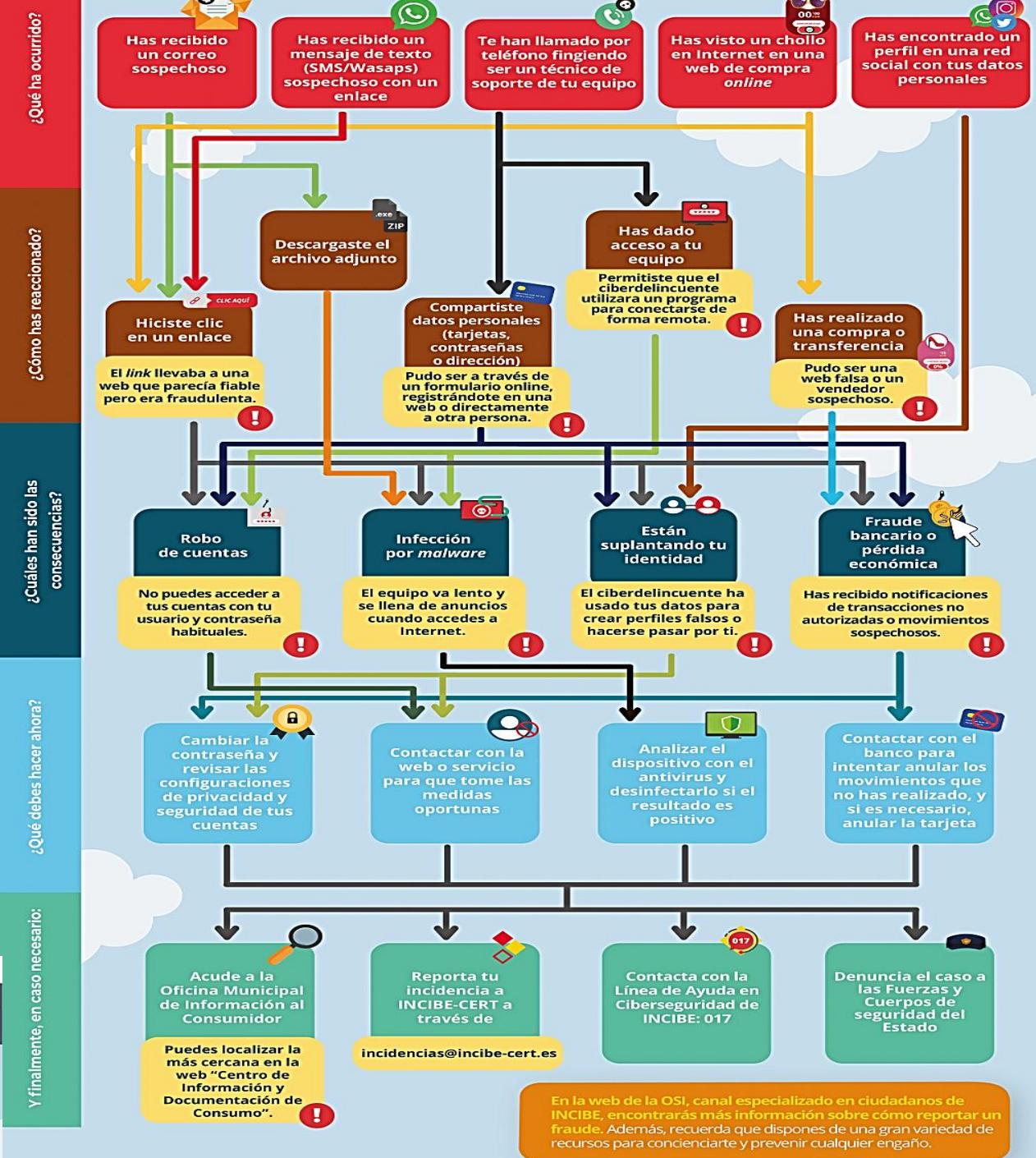
## Qué hacer si eres víctima de un fraude

Experiencia  
SENIOR

Sigue el camino correspondiente y descubre la mejor forma de actuar.



Y finalmente, en caso necesario:





# El ransomware

La mayor “pandemia digital” de la actualidad





# ¿CÓMO ACTÚA UN MALWARE / RANSOMWARE HABITUALMENTE?

José Manuel  
Redondo López

**Panel 1: The Squared Man (Actor malicioso)**

1. Despliega (Deploys) → 2. Ejecuta y cifra (Executes and encrypts) → 3. Paga rescate (Pay ransom) → 4. ¿¿¿ Descifra??? (Decrypt???) → Mwahahaha (Haha)

**Panel 2: Ransomware families**

Ransomware secuestra-equipos (Ransomware that kidnaps equipment) → ¡Ya no puedes usarme! (You can't use me anymore!) → Ransomware secuestra-ficheros (Ransomware that kidnaps files) → ¡Ya no puedo acceder a mis ficheros importantes! (I can't access my important files anymore!).

**Panel 3: Common delivery methods**

- Abrir un adjunto de un correo malicioso (Open a malicious email attachment) → ¡No nos hemos infectado! (aún) (We haven't been infected yet)
- Descargar y ejecutar directamente el malware (Download and execute the malware directly) → ¡Volveré! (I'll be back)
- Abrir un fichero Office malicioso (Open a malicious Microsoft Office file)

**Panel 4: Downloader process**

1. Ejecuta (Execute) → 2. Descarga (Download) → 3. Ejecuta (Execute) → 4. Cifra (Encrypt) → ¡Todas tus ficheras me pertenecen! (All your files belong to me!).

**Panel 5: Propagation**

Máquina infectada inicialmente (Initially infected machine) → Una vez infectada una máquina, ¡el ransomware se propaga a otras máquinas en la misma red rápidamente! (Once a machine is infected, ransomware spreads rapidly to other machines on the same network).

**Panel 6: Prevention and awareness**

Actor malicioso potencial (Potential malicious actor) → Antimalware Entrenamiento Sentido Común (Antimalware Training Common Sense) → ¡No tienes poder aquí! (You have no power here!) → ¡Y ojalá pueda prevenir que te infectes! (And I hope to prevent you from getting infected!).

**Textual notes:**

- "Es un tipo de malware que **secuestra** un equipo o sus contenidos para que no puedas volver a acceder a ellos" (It's a type of malware that **kidnaps** a computer or its contents so you can't get back to them)
- "Normalmente, pide un **rescate** para recuperarlos" (Normally, it asks for a **ransom** to recover them)
- "¡Y es **MUY COMÚN** hoy día!" (And it's **very common** today!)
- "¡Soy 'inocente'!" (I'm 'innocent'!)
- "(muchas más formas)" (many more ways)
- "Hay dos familias: los que **secuestran equipos** y los que **secuestran ficheros**" (There are two families: those that **kidnap equipment** and those that **kidnap files**)
- "¡Los que secuestran ficheros son los más comunes!" (The ones that kidnap files are the most common!)
- "Hay **varias formas** de ser secuestrado y ¡hay que estar atento a ellas!" (There are **several ways** to be kidnapped and you have to be alert to them!)
- "Normalmente ejecutamos primero un programa inofensivo antes de la infección" (Normally we run a non-infectious program first before the infection)
- "Se llama **downloader**: ¡Se descarga el malware real!" (It's called a **downloader**: It downloads the real malware!)
- "Esta serie de zines te enseñará las cosas más importantes para lidiar con este tipo de malware" (This series of zines will teach you the most important things to deal with this type of malware)
- "¡Y ojalá pueda prevenir que te infectes!" (And I hope to prevent you from getting infected!)

# ¿CÓMO ACTÚA UN RANSOMWARE HABITUALMENTE?



José Manuel  
Redondo López

- De entre todos los malware, el ransomware es probablemente el peor

- ¿Qué hace cuando entra en un equipo?

- **Inspecciona cada PC/móvil “infectado” en busca de datos privados que valgan dinero para la víctima**
  - O conecta con su “operador”, que los busca “a mano”
  - ¡Sin que tú te enteres!
- **Paulatinamente roba estos datos**
  - Haciéndose una copia y destruyendo tus copias
- Y, en la mayoría de los casos, **cuando ha terminado de robar todo lo importante...**
  - Cifra el disco duro y **ya no puedes leer tu propia información**
  - Aparece el típico aviso que vemos en las noticias
  - Salvo que **pagues o tengas una copia no infectada**, perderás esos datos



**WARNING!**

Your personal files are encrypted!

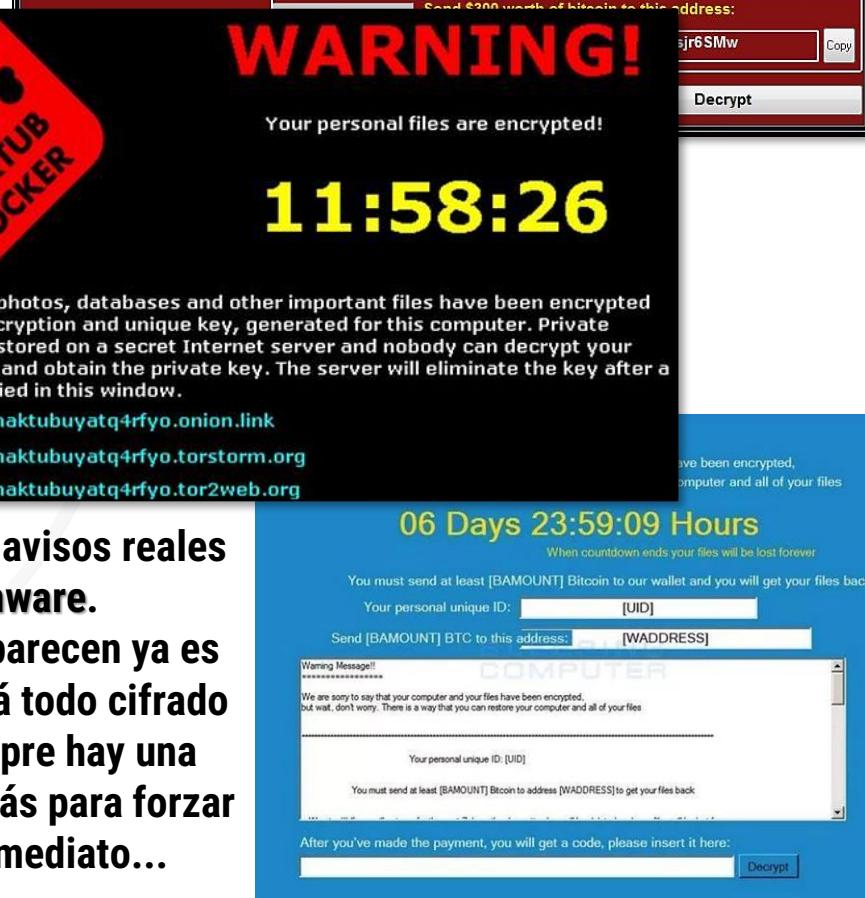
**11:58:26**

Your documents, photos, databases and other important files have been encrypted with strongest encryption and unique key, generated for this computer. Private decryption key is stored on a secret Internet server and nobody can decrypt your files until you pay and obtain the private key. The server will eliminate the key after a time period specified in this window.

Open <http://maktubuyatq4rfyo.onion.link>  
or <http://maktubuyatq4rfyo.torstorm.org>  
or <http://maktubuyatq4rfyo.tor2web.org>

**Estos son avisos reales de ransomware.**

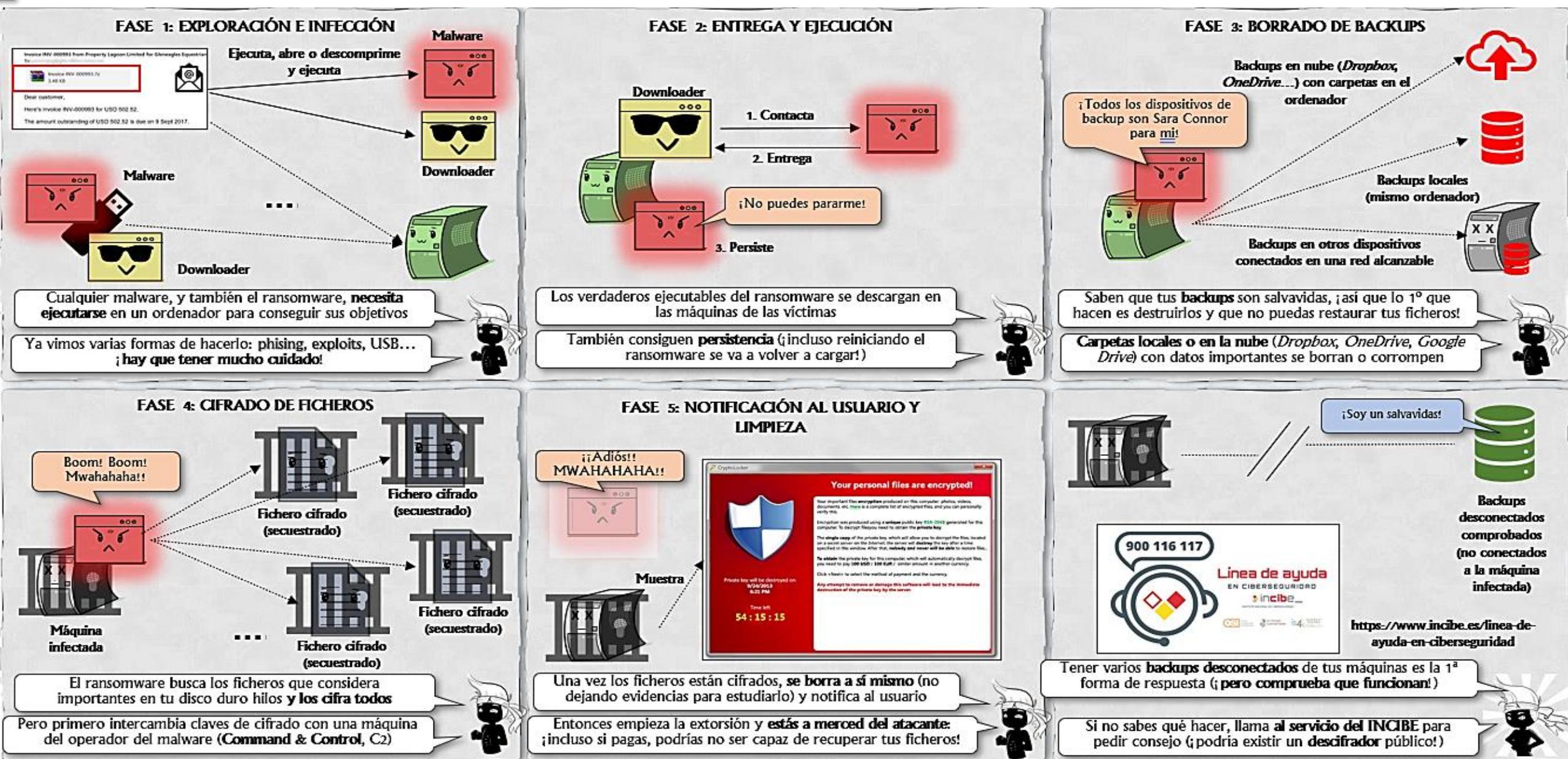
**Cuando aparecen ya es tarde (está todo cifrado ya) y siempre hay una cuenta atrás para forzar al pago inmediato...**





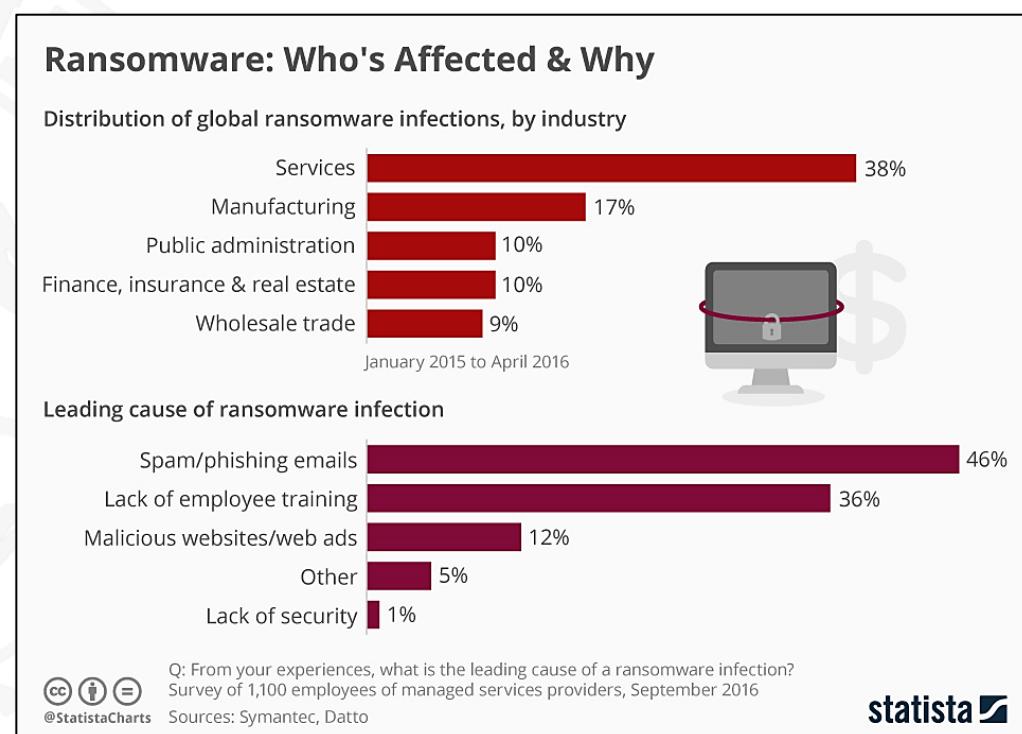
José Manuel  
Redondo López

# ¿CÓMO ACTÚA UN RANSOMWARE HABITUALMENTE?



# ¿CÓMO ACTÚA UN RANSOMWARE HABITUALMENTE?

- Entonces ¿Cuándo me sale el aviso es demasiado tarde ya? **Sí**
- Entonces comienza la **extorsión**
  - Pagar por la clave para descifrar tus archivos
- Pero nadie te da ninguna garantía de recuperarlos: ¡son criminales!
  - Podrías no recuperar una parte (**datos corruptos**)
  - Podrían extorsionarte más veces
    - Te suben el precio, no te dan la clave de todo, te vuelven a atacar...son delincuentes
  - **Podrían filtrar los datos**, aunque hayas pagado (¡son delincuentes!)
    - Pérdida de reputación, clientes, problemas legales...
  - Es decir, **es demasiado tarde**
    - ¡Mejor pon barreras antes no abriendo lo que no debes!



No se libra ningún sector, y el 94% de los casos son por caer víctima de **phishing**, falta de entrenamiento en ciber prevención y navegar por sitios inadecuados. **¿Entiendes la importancia de este curso ahora?**

# ¿PUEDO HACER ALGO A NIVEL TÉCNICO COMO PREVENCIÓN?

- Tener un entorno de navegación seguro, porque vía web entra la mayoría (12% de los casos)
  - Como se explica en el **S-64 “Narval”**
  - También ayuda el **R-11 “Príncipe de Asturias”** (aislamiento)
- Conocer la “anatomía” de tipos de delitos habituales de esta clase (36% de los casos)
  - Como se explica en el **“Nautilus”**
  - Aunque también este curso participa en ello
- Conocer la “mente del criminal” para detectar y evitar caer en engaños (46% de los casos)
  - Si aprendes a pensar como ellos, ¡aprendes a defenderte de sus acciones!
  - También ayuda saber moverte en redes sociales **F-31 “Descubierta”**
  - ¡Vamos allá!



*¿Te das cuenta todo el mal que puedes llegar a evitar con un entrenamiento adecuado?*

# ¿CREEES QUE LO HAS ENTENDIDO TODO? ¡AUTOEVALÚATE!

?

- *Has entendido que con el phishing y el ransomware se cubren la inmensa mayoría de delitos en la actualidad?*
- *Entiendes que el objetivo de mucho malware es propagarse lo más posible mientras o antes de hacer daño?*
- *Has entendido que existe el fin para pobres y para ricos en función de la importancia de la víctima?*
- *Entiendes que si ves un aviso de cifrado de un ransomware ya es tarde?*
- *Te ha quedado claro que nadie se libra del efecto del ransomware, dedique a lo que se dedique?*
- *Eres consciente de que “conocer la mente de un criminal” es una pieza muy importante, junto con las otras que forman parte de otros cursos “hermanos”, para prevenir ataques?*



# MENTES CRIMINALES

*¿Cuáles son sus intenciones?*



# ¿QUÉ VAMOS A VER EN ESTE BLOQUE?



- Te enseñaré cuales son los objetivos de un ciberdelincuente
  - Siempre es un beneficio propio, pero no siempre es directamente dinero
  - Hay otros incentivos
- Te enseñaré las diversas formas de contacto que tienen los ciberdelincuentes para dar contigo
  - ¡El correo electrónico solo es una de ellas!
- Te enseñaré como piensa un ciberdelincuente
  - Esto te puede ayudar a entender que **no van a tener piedad de ti** y que van a recurrir a **cualquier táctica** con tal de engañarte



# Objetivos de un ciberdelincuente

Qué quieren y cómo lo intentan conseguir



# ¿PERO QUÉ QUIEREN LOS DELINCUENTES?

## ● Siempre es su propio provecho, lo que se puede traducir en

- **Conseguir dinero:** Que se lo transfieran, que se haga pasar por la víctima y te lo robe, que la víctima haga una compra que resulte ser un timo...
  - Datos de tarjetas de crédito, servicios de pago para comprar fraudulentamente...
- **Conseguir datos privados / suplantar identidad completa:** Con ello pueden hacer/facilitar más estafas usando el nombre de la víctima, engaños, ventas fraudulentas, extorsiones...
  - Usarla de “cobertura”, dañar su reputación, **infiltrarse y cometer delitos en su nombre...**
  - Robo y publicación de datos privados, enfrentándose a consecuencias penales / multas
- **Conseguir cuentas en algún servicio de la víctima** (Ej.: servicios en nube)
  - La víctima paga, el delincuente lo usa para su provecho o algo malicioso
  - Eliminar o comprometer la cuenta (parada de negocio)...
- **Conseguir el control de equipos:** Robo, extorsión, hacer estafas en nombre de la víctima...
  - Criptominería, espionaje, ...
- **Conseguir que le sigas/valides:** Para ganar influencia / reputación, dar credibilidad a noticias (fake news), pérdida reputacional para la víctima...

## ● Todo sobre particulares o empresas victimas

# ¿COMO SE HACE?

## ● La acción desencadenante es simple

- **Que hagas clic en un enlace y accedas a la web que el delincuente quiera**
  - Para instalar **malware** engañándote para que lo ejecutes
  - O por **vulnerabilidad de tu navegador**, ¡sin que hagas nada! 😬
  - O ser falsa y engañarte para que **des tú voluntariamente datos personales...**
- **Que hagas clic e instalas un programa o abras un documento**
  - Que tendrá malware con alguno de los efectos anteriores
- **Que hagas clic y sigas a un medio / cuenta / canal de YouTube, Twitch, etc...**
  - Para que des verosimilitud a sus noticias / afirmaciones
  - Incrementa la credibilidad de productos, noticias, afirmaciones, teorías de la conspiración, ofertas...y ¡estafas!



El clic de la muerte...

## ● Es decir: **que hagas clic en algo que les de beneficio**

- ¡El clic donde no debes es la raíz de casi todos los problemas!

## ● **¿Y cómo lo consiguen?**

- Contactando contigo de alguna forma para engañarte...



José Manuel  
Redondo López

# FORMAS DE CONTACTO CON LA VICTIMA

- Las formas son muy variadas
- Ejemplos de medios clásicos son
  - Tu **email** (**centro de este curso**) o **mensajes** de aplicaciones como WhatsApp, Telegram, Discord...
  - **Cualquier red social**
    - Perfiles falsos que te hablan y te piden cosas
    - Mensajes públicos o **privados** fraudulentos / publicidad engañosa que te llega o ves
  - **Páginas de compra/venta** de productos a nuestros proveedores falsas
    - Su sistema de mensajería, webs falsas que suplantan a las reales...
  - **SMS o Llamadas telefónicas** (vishing o voice phishing)
  - **Comentarios** en canales de YouTube, Twitch y similares

Sharon's  
Publicidad ·

El presentador del programa LA RESISTENCIA, David Broncano, calificó a Lorena Castell como "irresponsable" y declaró en directo que "la información financiera de esta magnitud puede sacudir los cimientos de la sociedad española".

Martes 14 de noviembre de 2023 | EL MUNDO | 20%

Opinión Actualidad Económica Internacionales Deportes Cultura IOC Televisión Ciencia y Salud La Lectura

DRYOU.COM

Más información

*El email o el WhatsApp es muy mainstream, ahora la moda de los timos es poner una publicación falsa o anuncio en una red social con un "clickbait" para que hagas clic en una web fraudulenta creyendo que es una noticia y entres. No, ¡aunque use el logo de "El Mundo" no es ese periódico!*

# FORMAS DE CONTACTO CON LA VICTIMA

## ● Pero nos podemos poner “esotéricos”

- **Carta física** (¡sí! ¡aún ocurre!)
- **Códigos QR** pegados en cualquier parte
- **Dispositivos USB** que provengan de lugares inseguros
  - Ej.: personales de los empleados
  - U “Olvidados” (a propósito) especialmente preparados
  - Hay dispositivos USB pensados expresamente para hacer daño
  - Al conectarlos a un PC, se desencadena una campaña de malware
- **El Google Calendar:** Llegan invitaciones automáticamente con el texto de alguna estafa

## ● O “intensos”

- Combinaciones de todos los anteriores, con ataques **en varias fases** e incluso que involucren **a varias personas**
  - Que a veces son la misma suplantando a varios...
  - No olvides que existen los deepfakes de audio y video...



**Rubber Ducky**  
(<https://shop.hak5.org/products/usb-rubber-ducky>) y **USB Killer** son **dispositivos USB pensados para conectarlos a un PC y liarla bien parda...**

# ¿CARTA FÍSICA? ¿A LA ANTIGUA? ¿ESTÁS DE BROMA?



José Manuel  
Redondo López

- Desgraciadamente no...
- En Asturias tuvimos un caso muy sonado hace muchos años con el “Petromocio”
  - [https://www.elconfidencial.com/cultura/2018-04-22/petromocho-asturias-timo-gobierno-gijon\\_1552457/](https://www.elconfidencial.com/cultura/2018-04-22/petromocho-asturias-timo-gobierno-gijon_1552457/)
- ¡El email es sólo **UNA FORMA** posible de contacto!
  - Aunque una de las más comunes...
- Es necesario entender que los mismos ataques pueden llegar de muchas formas



## CAMBIO DATOS BANCARIOS SEG SOCIAL

Estimado

Desde la seguridad social nos ponemos en contacto con usted porque es necesario que nos envíe la siguiente documentación debido a que la ley que entró en vigor el pasado mes y debido al ataque informático en los sistemas de Hacienda y Seguridad social muchos de los datos de los ciudadanos se han perdido.

1. Ante todo va haber un incremento de las prestaciones, jubilaciones por lo que es necesario que nos adjunte la siguiente documentación, si es tan amable:
  - a. Fotos de ambas caras del DNI o NIE
  - b. Foto del extracto bancario donde usted aparezca como titular u autorizado en una entidad bancaria.
  - c. Última cantidad que cobró el mes pasado, una estimación.
2. El incremento será de 75€ a 150€ dependiendo el caso.

Deberá mandar la documentación a la siguiente dirección de correo:

- [Seguridadsocial.granada@outlook.es](mailto:Seguridadsocial.granada@outlook.es)

Y en el asunto poner Documentación + Num DNI

Atentamente,

A handwritten signature in blue ink, appearing to read '(Directora General INSS)'.



José Manuel  
Redondo López

# FORMAS DE CONTACTO CON LA VÍCTIMA MÁS ATÍPICAS

## ● Las formas de contacto evolucionan con la tecnología

- Nuevos programas, redes sociales....

## ● Se “ponen de moda”. Ej.:

- Los **Códigos QR** pegados en cualquier parte son cada vez más comunes

- Incluso **pegando falsos encima de verdaderos**
  - Lo escaneas con tu teléfono, accedes a la página web que contienen y...ya la has liado

### • El Google Calendar

- *¿Tienes eventos en el calendario que no recuerdas?*  
**CUIDADO**
  - Quieren que hagas clic y entres a una web chunga

## ● Asume que todos los timos pueden llegarte por **TODAS** estas formas de contacto

- ¡“Clásicas” o nuevas!

The image consists of three parts. At the top is a screenshot of a Google Calendar interface for October. It shows a single event on Sunday, 16th, from 13:00 to 14:00, titled "You've won the big prize! It's ready to go!". Below this is a large QR code with the text "CONTACT TRACING Help us create a safe environment." and "SCAN THE CODE". At the bottom is a photograph of a black USB flash drive lying in green grass.

You've won the big prize!  
It's ready to go!  
Today • 13:30 – 14:30  
Repeats daily

Join with Google Meet  
[meet.google.com/daa-trer-ado](https://meet.google.com/daa-trer-ado)

[https://docs.google.com/drawings/d/18xqhQHgQ85hR2F1tiila9uRVb5\\_cJTIx84DuCLSI5u/preview](https://docs.google.com/drawings/d/18xqhQHgQ85hR2F1tiila9uRVb5_cJTIx84DuCLSI5u/preview)

30 minutes before

The full guest list has been hidden at the organizer's request.

Organized by petr글ushkov106@gmail.com

THE UNRECEIVED TRANSFER FOR YOU IS DETECTED. IT IS POSSIBLE TO PICK UP IT WITHIN 24 HOURS. YOU CAN IN PROCESS IN A FEW MINUTES. THE TRANSFER WILL BE VALID ON CALENDAR DAY FROM THE TIME YOU RECEIVE THIS MESSAGE.  
GET TRANSFER CAN BE ON OUR OFFICIAL WEBSITE <https://docs.google.com>

Yes No Maybe ^

¡Un USB salvaje apareció!  
¡Es super efectivo! (por desgracia)

Sí, este es muy obvio. Ahora imagina uno de “Pedir cita urgente en <página web>”



# Psicología de los ciberdelincuentes

En la mente del mal



# PSICOLOGÍA DE UN DELINCUENTE

- Como hemos dicho, ten bien claro que el objetivo de un delincuente es siempre **obtener un beneficio de ti**

- Obviamente, uno de los principales objetivos es el **beneficio económico**
  - Directo: Dinero, productos, servicios
  - Indirecto: Formas de conseguir dinero con la información de otro
- Una de las formas **más comunes** de hacerlo es **ofertarte** dinero, productos, servicios, empleo, etc... **con "truco"**
  - Tendrás que **pagar por adelantado** una cantidad de dinero (además del supuesto precio) antes de acceder a esa oferta, producto o servicio
  - Con una **ENORME** variedad de excusas que justifiquen ese pago
  - En el "**Nautilus**" veremos muchas variantes
  - Se denominan Advance-Fee Scams
  - **Mucho cuidado con ella**



De una forma u otra, directa o indirectamente al final el objetivo es obtener un beneficio

# PSICOLOGÍA DE UN DELINCUENTE

- *¿Entonces es la típica estafa de pagar por algo que no existe?*
- ¡Sí!, pero hay más: **el delincuente va a intentar que pagues varias veces**
  - Inicialmente te pide dinero para completar el envío / transacción
  - Si envías el dinero, **inventará otra excusa** para que envíes más dinero para “desbloquear el proceso”
    - Siempre problemas fortuitos
  - A medida que lo vayas haciendo más veces, el delincuente “**subirá la apuesta**”
    - Te dirá que esta es la última vez (mentira)
    - Que estás **sólo a un paso** de conseguir el producto/servicio, que no lo dejes escapar (mentira)
  - **Te trata de engañar el mayor nº de veces posible** para que hagas los pagos
    - **NUNCA** recibirás NADA a cambio, o recibes algo falso (**tenlo BIEN claro**)
    - Hasta que “amigo/a date cuenta” y “cortes el grifo”
    - Entonces el delincuente **cortará el contacto** y se centrará en sus otras víctimas...



La víctima cae en una “espiral de engaño” de la que es MUY difícil salir a nivel sicológico

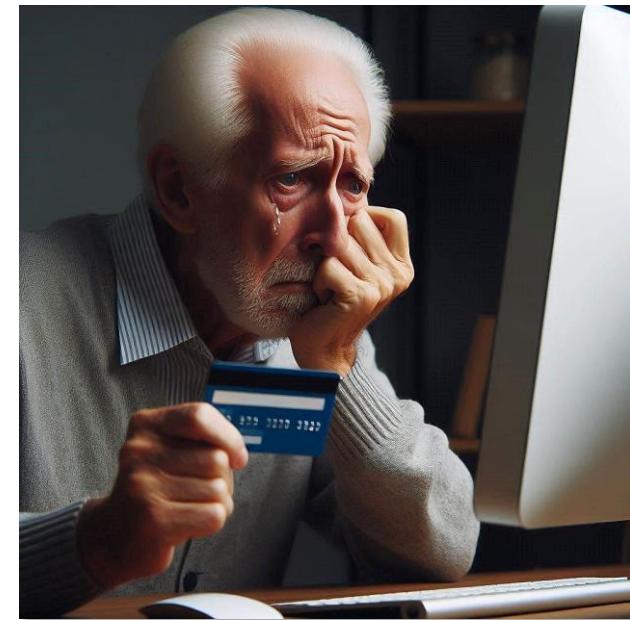
# ¿CÓMO ES POSIBLE QUE ESTO FUNCIONE?

- Puedes pensar que tú estás a salvo de estas estafas...

- Pero veremos que hay algunas **MUY BUENAS, DEMASIADO**
- ¡Ojo con el exceso de confianza!

- Pero también estás rodeado de gente que **no ha tenido la suerte de tener tu formación y conocimiento**

- Y son **su principal tipo de víctima** (nuestros mayores, nuestros hijos...)
- Siempre puede haber una víctima potencial en tu entorno
- Seguro que se te viene un nombre de alguien que conoces a la cabeza ahora mismo, ¿verdad?



El objetivo siempre es el más débil. Te puedes imaginar quiénes van a ser, ¿verdad?

# ¿CÓMO ES POSIBLE QUE ESTO FUNCIONE?

## ● Porque las víctimas “**invierten emocionalmente**” en el tema

- Si “pican” y pagan la 1<sup>a</sup> vez, **la probabilidad de que lo sigan haciendo es muy alta**
- **Han “invertido” en el tema**
  - Económica y emocionalmente, las excusas para enviar dinero suelen “**atacar**” **la parte emocional**
  - No pueden permitirse / se avergüenzan de **perder su inversión**
- El delincuente crea una sensación creciente de **urgencia** (“venga, esto se acaba ya”)
  - Para que las víctimas crean que su inversión tendrá por fin resultados a muy corto plazo
- Siempre se recurre a **tácticas** para hacer ver a la víctima que su inversión / sacrificio económico **merece la pena**
  - Porque lo que va a obtener a cambio es mucho más valioso
  - O introducir un **sentimiento de urgencia** para evitar que la víctima piense o consulte
  - O atacar sentimientos primarios (**codicia**, la **buenas fe** o la **necesidad** (de relaciones o económica))
- **En resumen:** La víctima se mete en la “**espiral del engaño**” de la que hablamos
  - De pérdidas económicas y promesas de “salir” con éxito en la siguiente “vuelta”
  - **Lo que NUNCA** ocurre

# ¿CÓMO PUEDE LA GENTE “CAER” EN ESTO?

- Si ya has caído, “romper la cadena” podría ser difícil
  - Aún te lo crees, te niegas a reconocer que te han estafado...
- Recurren a cualquier táctica que se les ocurra (luego detallamos esto)
  - Crean **páginas falsas** de bancos / tiendas online / empresas
    - Para que veas que el dinero / producto ofertado existe
    - De manera muy muy elaborada (páginas que funcionan, no solo copian el aspecto)
    - Como es el delincuente quien las controla, te pueden dar incluso un usuario de acceso
  - **Falsifican identidades de personas reales**
    - Ligadas a una web real que supuestamente te está ofertando algo
    - Con información pública o privada real de la persona
    - Obtenida de filtraciones de datos (ej.: direcciones, DNIs...)
  - El mismo delincuente suele usar **múltiples identidades de personas** involucradas en el proceso
    - Abogados, procuradores, empresas de seguridad, sacerdotes, etc...
    - Para ganar credibilidad (“monta una película”)
  - **Falsifican documentos** de distintos tipos para aumentar la credibilidad
    - O usa documentos reales robados

# ¿CÓMO PUEDE LA GENTE “CAER” EN ESTO?

- Antes de continuar, quiero destacar tres cosas

1. **Cualquiera de nosotros podemos ser víctimas:** la formación es como las vacunas: impide caer en una gran cantidad de estafas
  - Pero hay estafas extremadamente buenas, y **nadie está exento de ser una víctima**
  - Hasta los mayores expertos en ciber fraude confiesan que han tenido **graves problemas** distinguiendo una estafa de un mensaje real
  - Otros confiesan haber tenido “un día tonto” (que podemos tener cualquiera) y haber caído
  - Esto último no se puede evitar, pero si **no tienes una falsa sensación de confianza** es más difícil caer
  - Si una persona no ha tenido la suerte de ser formada contra ellas, es un objetivo prioritario para estos delincuentes
  - **Ayúdale**s y encima no les recrimines que les hayan engañado
    - ¡Ya se sienten los suficientemente mal!



Joven, “nativo/a digital”, “techie”,  
lo sabes todo, tienes confianza en ti  
mismo, eres un hakin bestia, etc. Lo  
siento, tú también puedes caer...

# ¿CÓMO PUEDE LA GENTE “CAER” EN ESTO?

2. Los delincuentes **no tienen límites morales (cualquier táctica)** vale para convencer)
  - Religión, aficiones...
  - Complicidad por ser “hermano”, ser **familia**, ser de un **mismo grupo**...
  - Ofrecer **relaciones amorosas**
  - Fingir **miserias y pobreza extrema**...
  - Víctima de **terrorismo**, de **violencia**, de una **guerra**...
  - Compartir **ideales**
  - Y un largo etc... ¡cualquier excusa, no hay límite con tal de engañar!
  - **Suelen involucrar la actualidad**
    - Terremotos, inundaciones, volcanes, pandemias...
    - Lo hacen para ser más creíbles: estate atento a las noticias y prepárate para recibir cosas así
  - **No juegan con tus reglas** (ni con ninguna), no se mueven con tus parámetros, en serio, piensan de otra forma



“**Todo por la pasta**”, literalmente. ¿Has oído hablar de los perfiles sicopáticos, personas sin ninguna empatía? Pues eso. Los mismos que hacen ciberbullying mayoritariamente (P-74 “Atalaya”), por cierto

# ¿CÓMO PUEDE LA GENTE “CAER” EN ESTO?

## 3. Los delincuentes **NO** son como tú y como yo

- **Esta gente piensa distinto**, "prey on the weak"
  - Ellos son "depredadores", nosotros todos "presas"
  - No descartes la extorsión (fingida o real)
  - Robo de identidades de tus conocidos
  - Que te vigilén (stalking) tus RRSS o en la vida real (se llama "hacer OSINT")
  - Para saber más de ti, y que la estafa resulte más creíble
  - Espionaje...
  - ¡O cualquier maldad que se te ocurra! 😊
- Se llega incluso a **autojustificaciones** como
  - "La víctima se lo merecía por ser tan tonto", "Haber estado más atento", "Ya tenía mucho dinero"...
  - Culpar a la víctima, victim blaming
  - Hay delincuentes que incluso dicen que, como la sociedad "les roba", ellos tienen carta blanca para robar
- **No trates de entender sus motivos**
  - **Porque salvo que seas uno de ellos no los vas a entender**

**NO SE VAN A APIADAR DE TI**



**Detrás del cibercrimen no solo hay estafas, puede haber muchas otras cosas más: ciberacoso, espionaje, ciberguerra entre empresas o países...es otro mundo del crimen, mucho más profundo y turbio de lo que imaginas....**

# ¿QUIÉN ESTÁ DETRÁS?

- Generalmente, **bandas organizadas y especializadas de todo país y etnia** que viven de esto y son profesionales del timo

- Nunca asumas que son “tontos”, este tipo de criminales son cada vez más sofisticados
- Se pueden ganar **grandes sumas de dinero**, e invierten en su propia formación
  - ¡Como tú estás haciendo ahora para protegerte de ellos!
- <https://twitter.com/elhackernet/status/1527197191755948033?t=Q8NOfopmwhSJ2OZjdvtUA&s=19>



Banda encarcelada por timo telefónico a pensionistas  
[bbc.co.uk](http://bbc.co.uk)



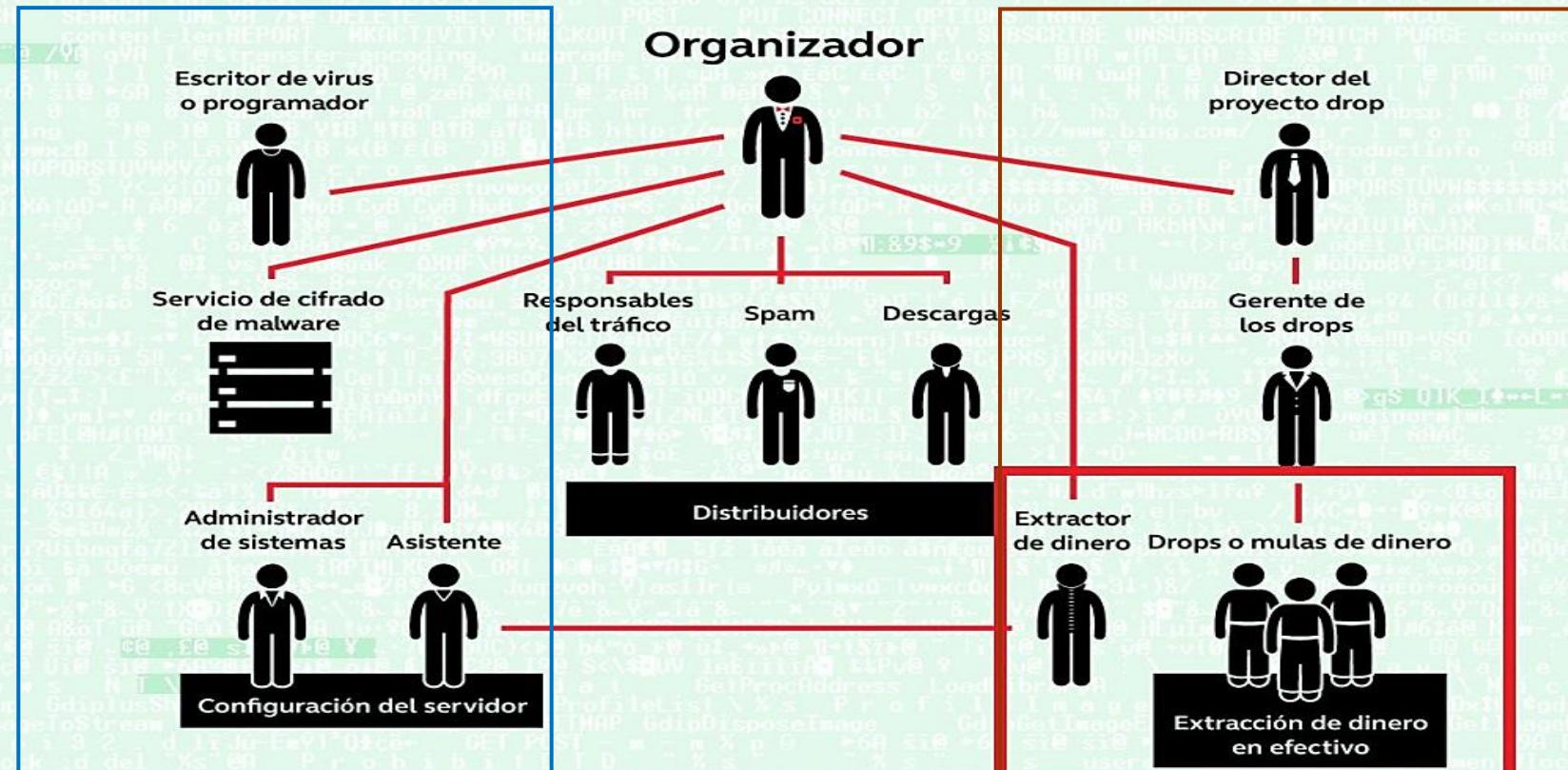
Banda londinense encarcelada por una estafa multimillonaria con entradas falsas  
[kentlive.news](http://kentlive.news)

# ¿GRUPOS CRIMINALES PROFESIONALES ORGANIZADOS?

## Cómo está organizado un grupo cibercriminal

En este momento, Kaspersky Lab está investigando cinco grupos cibercriminales de habla rusa involucrados en robo de dinero mediante malware.

Gente  
técnica



El extractor de dinero transfiere fondos desde las cuentas financieras atacadas hacia las cuentas provistas por el gerente de drops. Éste les indica a los drops o mulas de dinero adónde transferir el dinero. Una parte del dinero resulta en manos del director del proyecto drop, mientras que el resto se transfiere al director del grupo criminal.

# ¿CREEES QUE LO HAS ENTENDIDO TODO? ¡AUTOEVALÚATE!



## ● Respecto a los objetivos...

- *¿Entiendes los distintos objetivos de un ciberdelincuente?*
- *¿Comprendes que no siempre buscan dinero directo, sino cosas que les den beneficios económicos indirectos?*
- *¿Entiendes que la base de todos los problemas es un clic donde no debes?*
- *¿Eres capaz de recordar las distintas formas de contacto principales que tiene un ciberdelincuente?*

## ● Respecto a la sicología del delincuente...

- *¿Has comprendido cómo funciona la mente de un ciberdelincuente, y que se puede tratar como un "depredador" de la naturaleza?*
- *¿Entiendes que nadie está a salvo de estos problemas debido a la sofisticación de las falsificaciones?*
- *¿Comprendes que son bandas profesionales organizadas y no personas probando suerte desde su casa?*



## FORMAS DE ENGAÑO

Corre más que el veneno que llevan dentro



# ¿QUÉ VAMOS A VER EN ESTE BLOQUE?

- **Voy a enseñarte cómo se falsifican los distintos elementos que participan en un fraude**
  - Para ello voy a usar una **escala de sofisticación** propia que uso para categorizarlas
- **Te voy a mostrar que cualquier cosa que puedes recibir vía email puede ser falsificada**
  - Y que algunas falsificaciones son **prácticamente indistinguibles** de la real
- **Con ello, quiero que tomes conciencia de que puedes ser una víctima cuando menos te lo esperes**
  - Tu nivel de conocimientos técnico **no te puede mantener 100% a salvo**
  - En realidad, **nada** puede hacerlo...



# ELEMENTOS FALSIFICABLES

- Ya vimos que la cantidad de cosas falsificables hoy día **es enorme**
  - **Medios digitales:** Emails, SMS, mensajería (WhatsApp, Telegram, Discord, en público/grupos cerrados de cualquier red social...), llamadas telefónicas...
  - **Medios físicos:** **QR colocados estratégicamente** o suplantados, **USBs “perdidos”...**
- Las falsificaciones **ya no son "cutreces"** fácilmente identificables
  - Las “**fugas de datos**” (data leaks), tan frecuentes hoy en día, se usan para mejorarlasy
    - Se usan **datos reales robados** de las víctimas para aumentar la credibilidad
  - Y con el **uso de la IA**, los spear phishing son **MUY** elaborados
  - Muchas falsificaciones integran **varios elementos de forma coordinada**
    - **“Obra de teatro” del mal**
    - Emails, webs, documentos, personas (vidas incluidas), llamadas, mensajes...se crea una ilusión completa
- **NUNCA te confíes**
  - Incluso la estafa con la premisa más absurda puede ser muy peligrosa con una falsificación bien elaborada

# “NIVELES” DE COMPLEJIDAD DE UNA FALSIFICACIÓN

- Yo clasifico las falsificaciones en 5 niveles

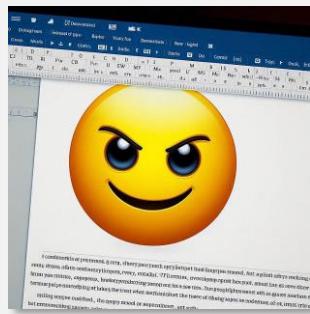
- De más a menos cutre, ya que resulta fácil de entender a quién se lo explico (**no es oficial**)
- El nivel 5 incluye la suplantación:** No hay falsificación de elemento alguno, es alguien usando algo real tras robarlo (incluido cuentas de usuario)

Probabilidad de engaño

- ↘ +

Trabajo de elaboración del delincuente

Nivel	Tipo de falsificación
1	Falsificación <b>burda</b> , sin cuidado alguno y/o en un lenguaje no nativo del delincuente (errores obvios)
2	Falsificación <b>fácilmente detectable</b> con entrenamiento sobre ciberestafas básico
3	Falsificación <b>trabajada</b> que puede engañar incluso a personas entrenadas que no le presten la debida atención (factor prisa, sorpresa...)
4	Falsificación <b>avanzada</b> con un trabajo considerable detrás, que requiere atención y entrenamiento en detalle para su detección
5	Falsificación <b>¿casi? indistinguible</b> del elemento real incluso a ojos expertos, robo de la identidad del emisor real de manera que no es posible distinguirlo de algo falso, o <b>falsificación avanzada con técnicas de IA, extremadamente peligroso</b>



# Documentos maliciosos

Cuando un fichero lleva el mal dentro



# DOCUMENTOS FALSIFICADOS Y/O MALICIOSOS

- Cualquier nivel de documento falso **puede venir con malware adjunto que se ejecutará al abrirlo**
  - Especialmente de Office, pero también PDF
  - **¡Mucho cuidado al abrir documentos, aunque resulten “cutres” pueden venir con “bicho”!**

Probabilidad de engaño



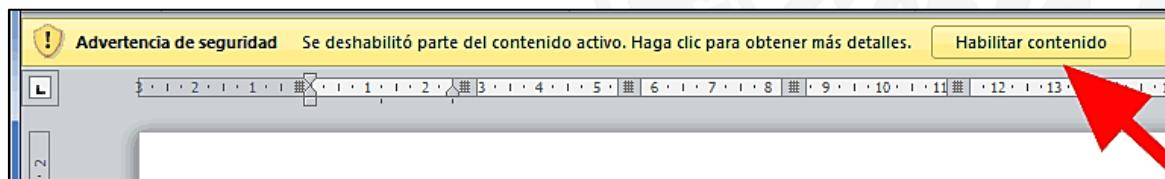
Trabajo de elaboración del delincuente

Nivel	Tipo de documento falsificado
1	Documento <b>redactado de forma negligente</b> , sin formato profesional y/o evidentes defectos en el uso del idioma o la disposición de la información presentada
2	Documento que <b>usa logos e iconos oficiales</b> , pero con aspecto no profesional y pequeños errores en el uso del idioma
3	Documento <b>manipulado a partir de un clon</b> con evidentes muestras de manipulación, o imitación de una comunicación/documentación real, o con un estilo visual mucho más convincente y profesional
4	Lo anterior con <b>elementos falsos que refuercen su “veracidad”</b> para aumentar su credibilidad y no detectar la manipulación: falsos sellos, firmas, textos que indiquen que ha sido verificado por alguna entidad o persona...
5	Comunicación <b>indistinguible de una real</b> hecha por un empleado malicioso o por un delincuente que ha robado la cuenta de un empleado real (data leak): ¡la única defensa es ver si lo que pide es razonable!

# FORMAS POR LAS QUE EL CONTENIDO DE UN DOCUMENTO PUEDE SER MALICIOSO

- Cuando abres un documento malicioso (independientemente de su “cutrez”) te pueden pasar dos cosas

1. Que sea un documento “normal” que “sólo” te pida **hacer clic en un enlace**
  - Ya vimos que en la página a la que irás al hacer ese clic se encuentra el malware ¡**No hagas nunca clic!**
  - Esto se tratará cuando hablamos de enlaces posteriormente
2. **Que el documento tenga el malware dentro**, con lo cual te pedirá que lo ejecutes
  - Es decir, **que “habilites su contenido”**
  - Hazte a la idea de que equivale a “hola, soy un virus, ejecútame”: **va a engañarte para que lo hagas**
  - **¡Cualquier cosa con tal de que pulses en el botón “Habilitar contenido”!**



Pulsar este botón es equivalente a decir “Hola, sí, inféctame el PC con un virus por favor”  
**¡NO HAGAS CLIC! (esto no te pasa si lo abres con un programa de Office 365 online, por cierto)**

- **Cuidado:** ¡Si tu visor (Word, Acrobat...) no está actualizado, podría ejecutarse solo sin que habilites nada!

- ¡Veamos unos ejemplos de ambos tipos!



## Documentos con enlaces maliciosos





José Manuel  
Redondo López

# DOCUMENTOS CON ENLACES MALICIOSOS

- Estos son documentos PDF con un enlace malicioso de **Nivel 1**
- No tienen aspecto profesional en absoluto
  - Texto y poco más
  - No hay logos, estilos...
- Usa la urgencia y el falso agradecimiento para que no pensemos y hacer clic
  - Muy típico...
- Tiene errores gramaticales
- *¿Crees que son los más comunes? Pues lo siento, pero ya no*
  - Ha llegado la IA amigos...

Ya (casi) nadie pica con estas cosas...

Barrister Bills Adams 13:35 (hace 1 hora)

Buenas noticias de Barrister Bills Adams.

Espero que usted está leyendo este mensaje por la buena salud. Quiero hacerle saber que he recibido ayuda de un Estado Unidos de América ciudadano que es un hombre de negocios. Él fue capaz de ayudar con la transacción / herencia que anteriormente empecé con usted.

No he olvidado su esfuerzo pasado que hizo que me ayude. Sé que ha intentado todo lo posible para que me ayude, aunque las cosas no funcionaron para los dos. Debido al esfuerzo que hizo en asistir a mí y el gran amor y preocupación que me mostró durante el periodo que estuvimos comunicarse entre sí, me trasladaron a compensar con la suma de \$ 500,000.00 (quinientos mil dólares estadounidenses).

Esto es para hacerle saber que me dejó un cheque bancario con Virgin Atlantic Delivery Company en Dubai en los Emiratos Árabes Unidos para la seguridad antes de viajar a mi país.

En este sentido, yo le aconsejaría que en contacto con el Virgin Atlantic entrega Compañía tan pronto como sea posible saber cuándo van a entregar su paquete a usted antes de la fecha de caducidad.

Para su información, he pagado por los gastos de envío para su giro bancario pero sólo a exigir la suma de (\$ 580 USD) quinientos ochenta dólares por tasas de seguridad y de demora, que se va a enviar a la empresa de mensajería y seguridad para entregar su proyecto directamente a su dirección postal en su país. Por lo tanto usted necesita ponerse en contacto con la empresa de mensajería y seguridad de inmediato y pagar las cargas que no excederá la suma de (\$ 580 USD).

A continuación se presentan los datos de contacto de la empresa de entrega:

[View document](#)

E-mail: [infovirginatlantic@gmail.com](mailto:infovirginatlantic@gmail.com)  
Número de registro: [wwdsc100 / 2016](#)  
Número de Referencia: [Virgin / wwdsc / 0000453](#)

Hi,

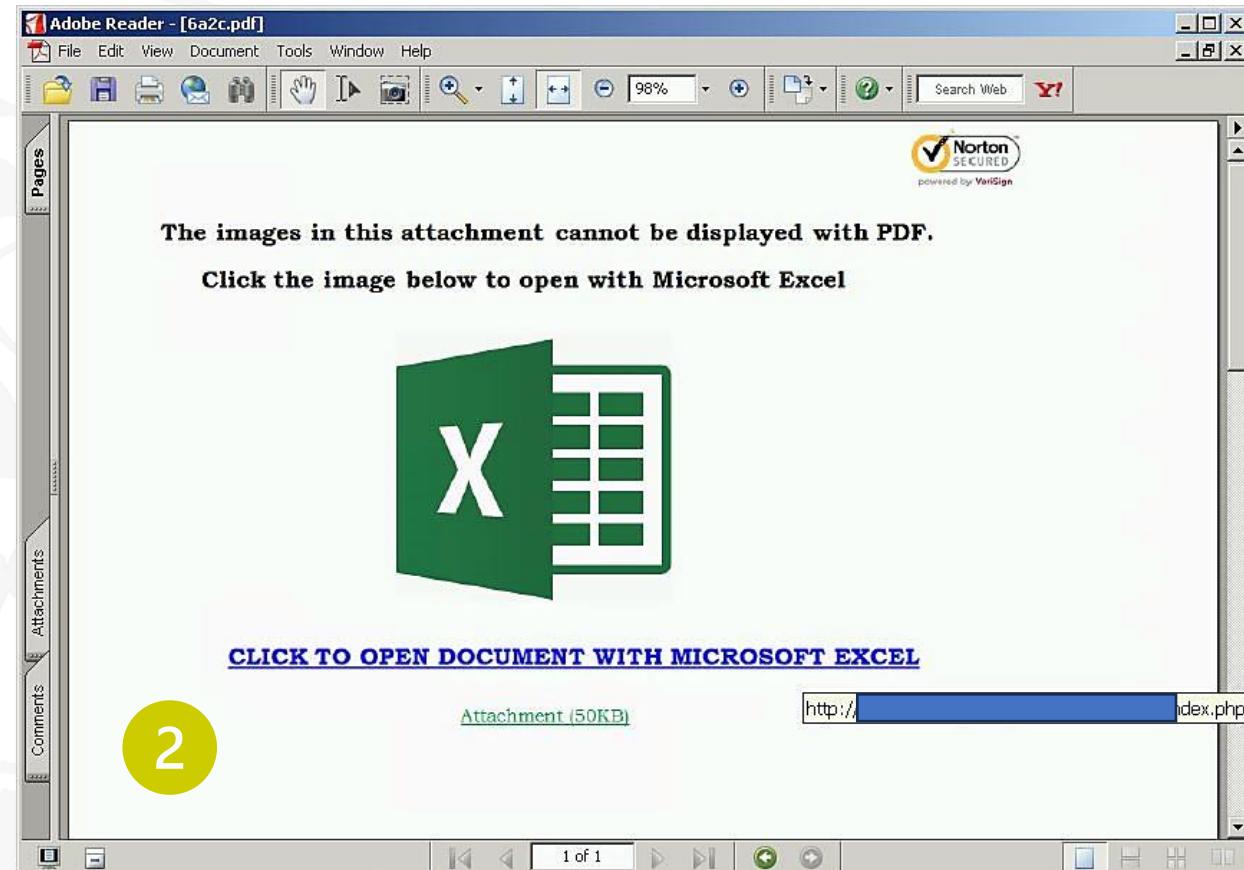
I have shared an important document via Dropbox, for security reasons. To view shared document, log in with your email address and password to access. Please quote immediately.

[View document](#)

Thank you.

# DOCUMENTOS CON ENLACES MALICIOSOS

- Este documento PDF es de **Nivel 2**
- Dice que abre un **Excel**, pero en realidad va a una web
- Usa logos para ganar credibilidad
  - Falsamente verificado por el antivirus Norton
  - Básicamente **han pegado la imagen del logo** y ya está ☺
- El estilo es malo, pero al menos usa imágenes y colores



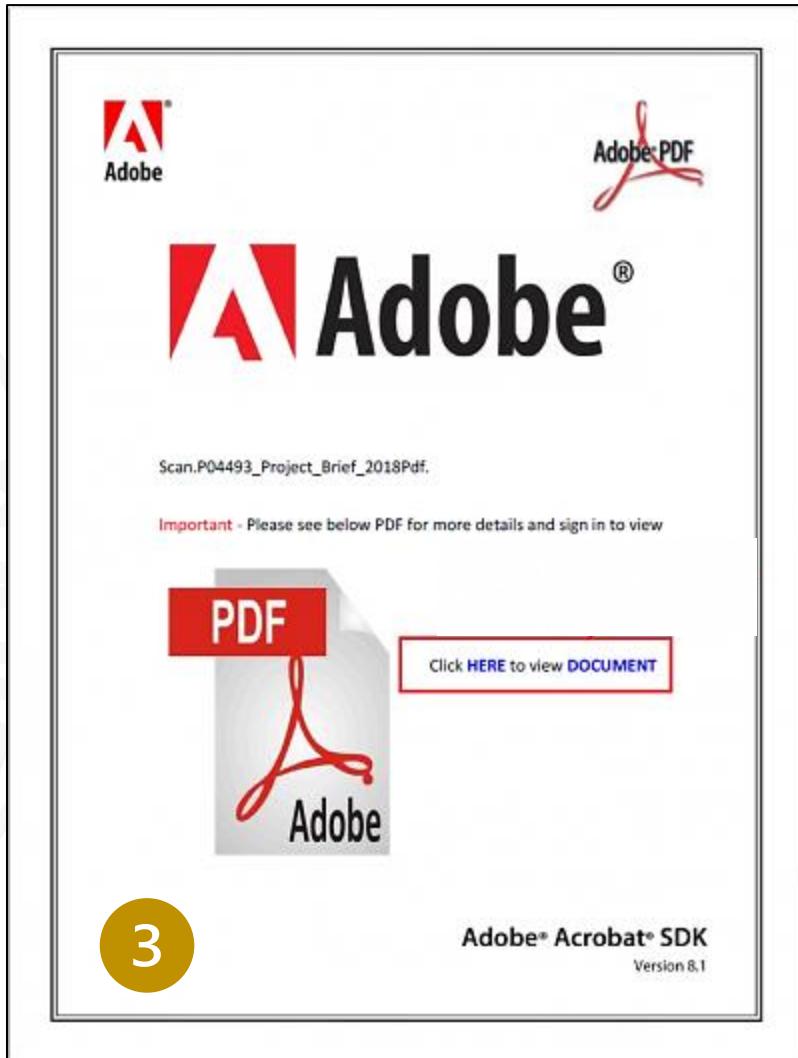
Al menos usa el logo correcto...



# DOCUMENTOS CON ENLACES MALICIOSOS

## • Esto es un documento de **Nivel 3**

- Estilo más cuidado que los anteriores, más profesional
- Aspecto más cuidado, que imita la pantalla de bienvenida del **Acrobat PDF Reader**
- Muchos logos oficiales
- Tiene aún algún error gramatical pequeño



Repleto de imágenes e iconos robados,  
pero al menos no da asco verlo

# DOCUMENTOS CON ENLACES MALICIOSOS



José Manuel  
Redondo López

## ● Este es un documento de Nivel 4

- Correspondiente a una falsa denuncia por tenencia de pornografía
  - Timo clásico (ver “**Nautilus**”)

## ● ¿Por qué es bueno?

- Estilo sobrio profesional y correctamente redactado
- Estructura de documento formal
- Logos y sellos oficiales falsificados
- Seguramente plagiado de una real

## ● Pero con un correo de Gmail de contacto

- *¿Documento oficial y contacto por Gmail?  
¡Estafa seguro!*

**INTERPOL CONVOCATORIA**

Carpetas N°:ES00415215-03/22

4

Sr. Sra,

A solicitud del Sr. ALEJANDRO MAYORKAS, Secretario de Seguridad Nacional de los Estados Unidos de América, Jefe del Departamento de Riesgos Mayores "Brigada para la Protección de Menores (BPM)" le hacemos llegar la presente invitación.

La citación por un agente de la policía judicial está prevista en el artículo 390 -1 del Código de Procedimiento Penal. Vale citación ante el tribunal y lo decide el Ministerio Público.

*De conformidad con lo dispuesto en el artículo 372 del Código Penal establece: "El atentado al pudor cometido sin violencia ni amenazas contra la persona o con ayuda de la persona de un niño de cualquier sexo, menor de 16 años, será reprimido con pena privativa de libertad".*

El artículo 227-23 del Código Penal dispone: "El hecho, con vistas a su difusión, de fijar, grabar o transmitir la imagen o representación de un menor cuando esta imagen o esta representación tiene un carácter pornográfico es castigado con 5 años' prisión y multa de 80.000 dólares.

Emprenderemos acciones legales contra usted poco después de la incautación de una computadora de la ciberinfiltración por:

**(PORNOGRAFÍA INFANTIL - PEDOFILIA - EXHIBICIONISMO - PORNOGRAFÍA CIBERNÉTICA)**

Para su información, la ley 390-1 del Código Procesal Penal de marzo de 2007 aumenta las penas cuando las proposiciones, agresiones sexuales o violaciones se hayan cometido a través de Internet.

**Cometió el delito después de ser atacado en Internet (sitio de publicidad), ver videos de naturaleza pornográfica infantil, fotos/videos desnudos de menores fueron grabados por nuestro gendarme cibernético y constituyen prueba de sus delitos.**

En aras de la confidencialidad, le enviamos este correo electrónico, por lo que lo invitamos a responder a la dirección que se indica a continuación, por supuesto, brindándonos sus documentos de respaldo y las razones que lo llevaron a actuar de esta manera, sus justificaciones para que sean investigados y verificados para evaluar las sanciones; esto en un plazo estricto de 72 horas.

Contactar: [ppoliciainterpol793@gmail.com](mailto:ppoliciainterpol793@gmail.com)

Ahora está llamado a responder por su propia voluntad de inmediato para evitar que este asunto se propague y tome otro giro desagradable a su favor.

Pasado este tiempo, nos veremos obligados a enviar nuestro informe al Ministerio Fiscal para que dicte orden de detención contra usted y procederemos a su detención inmediata por parte de la policía más cercana a su lugar de residencia.

Atentamente

Sr. Général-major Ahmed Nasser Al-Raisi

Presidente de Interpol, presidente electo de la Organización Internacional de Policía Criminal

Secretaría General Sección de Delitos Ciberneticos Brigada de Protección Civil

*[Handwritten signature]*



Mira las firmas , sellos, etc. aquí hay calidad...hasta que ves el mail

# DOCUMENTOS CON ENLACES MALICIOSOS: COSAS A TENER EN CUENTA...

- Aunque algunos de los ejemplos estén en inglés, lo mismo nos puede llegar en Español
  - Con errores gramaticales obvios...**¡o sin ellos!**
  - **¡La falta de errores ya no es una razón para confiar en un documento!**
- **¿Motivo de eso?** La IA, como veremos luego
- El objetivo de todos estos documentos es **que hagas clic en el enlace que adjuntan**
  - Sus enlaces pueden además estar diseñados para engañarte (lo veremos luego)
- **A dónde vayas determinará como te atacarán, recuerda...**
  - Descargar y ejecutar algo
  - Pedirte datos personales con algún pretexto
  - Directamente, instalarte un **malware**
    - Más probable en navegadores sin actualizar

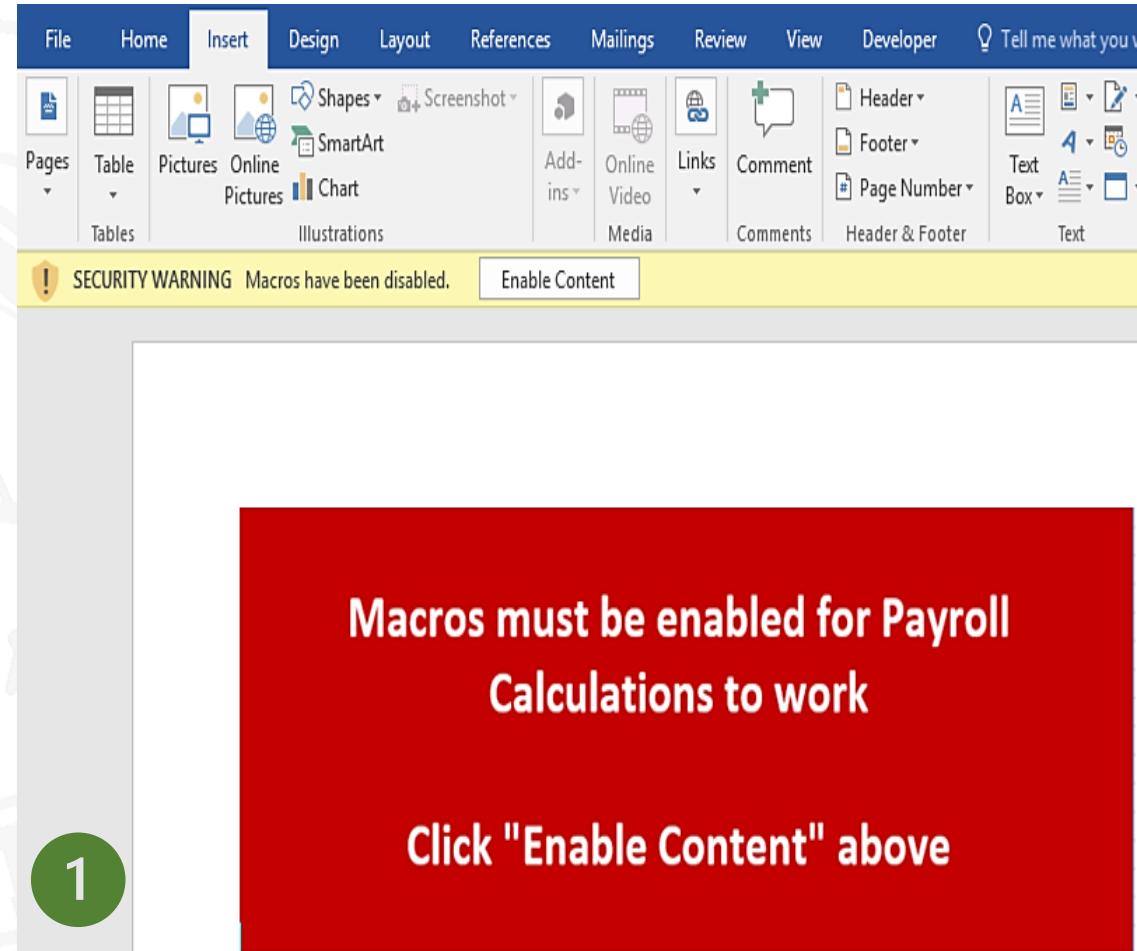


## Documentos con malware dentro



# DOCUMENTOS CON MALWARE DENTRO: CÓMO TE CONVENCEN

- Este es un documento con malware adjunto de **Nivel 1**
- Un cuadro rojo con letras, sin más ☺
- Un mensaje simple con una excusa cutre
  - Cero esfuerzo en intentar que parezca algo creíble...
  - Los delincuentes o pasan de todo o no tienen formación alguna...
- De nuevo, ¿es esto lo común? **Ya no**



Insertar Forma -> Rectángulo-> Añadir texto y hala, ya está...



José Manuel  
Redondo López

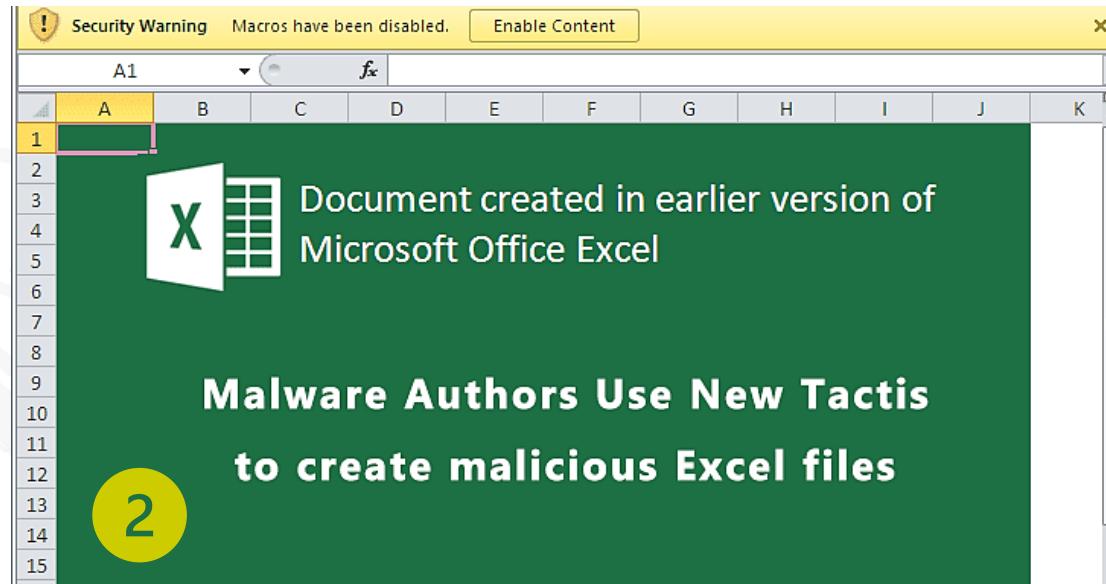
# DOCUMENTOS CON MALWARE DENTRO: CÓMO TE CONVENCEN

## ● Estos los considero Nivel 2

- Se inventa la excusa de que se ha creado en una versión anterior de Excel o Word
- **Mentira:** Los documentos de versiones anteriores los abre cualquier programa Office actual
- ¡Encima critica a los autores de malware!

## ● Se usa el logo oficial de la Excel o Word como “gancho”

- Logos que se pueden descargar de Internet con una simple búsqueda en Google
- Se hace creer al usuario que el contenido del documento está “tapado” hasta que lo autorice



Imita una especie de aviso del programa para que hagas lo que no debes



José Manuel  
Redondo López

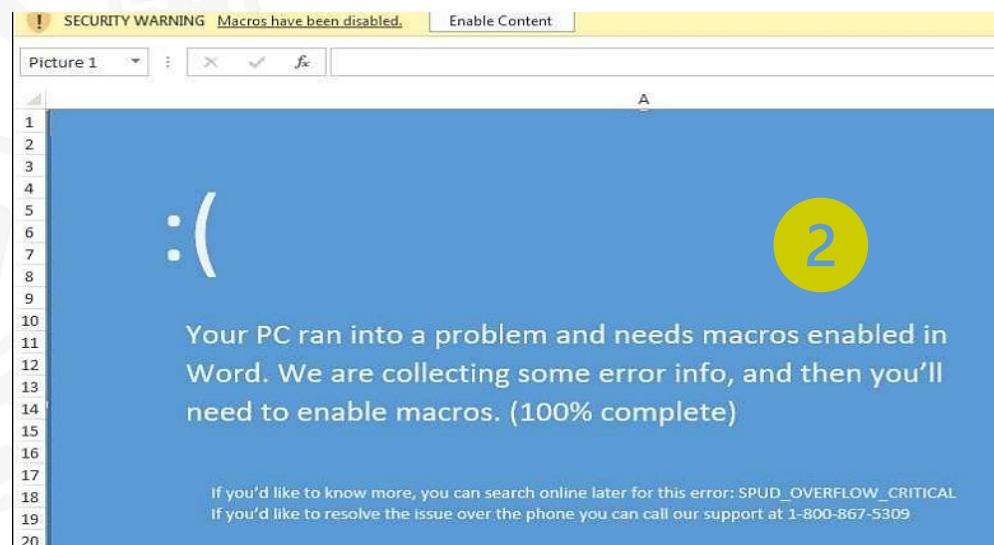
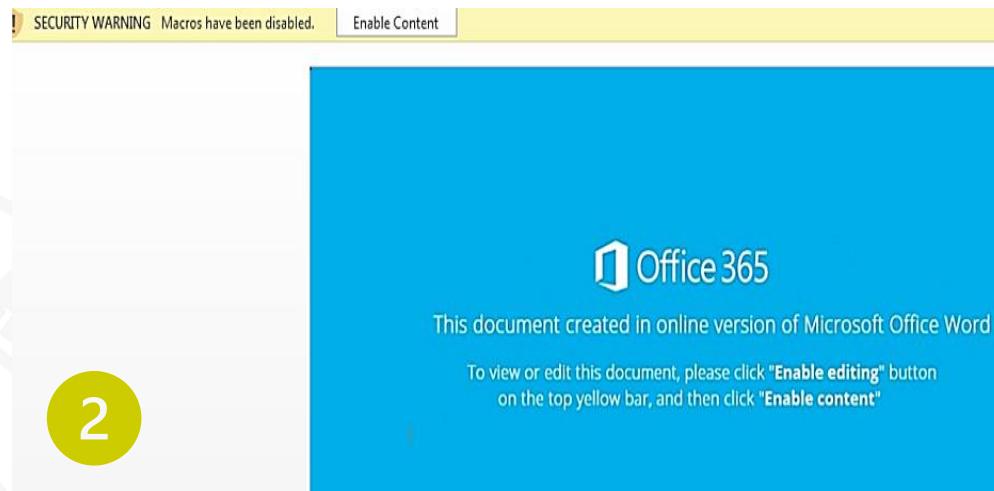
# DOCUMENTOS CON MALWARE DENTRO: CÓMO TE CONVENCEN

## ● Otros ejemplos de **Nivel 2** con excusas varias

- Creado con la versión online de Word
  - **Mentira:** Todo lo creado con esa versión pueden abrirse con el Word “normal”
- Copia de la pantalla de fallo catastrófico de Windows para que habilites el contenido...
- ¡Cualquier excusa que se os ocurra les sirve!

## ● Cualquier documento **de cualquier programa de Office** vale para propagar malware

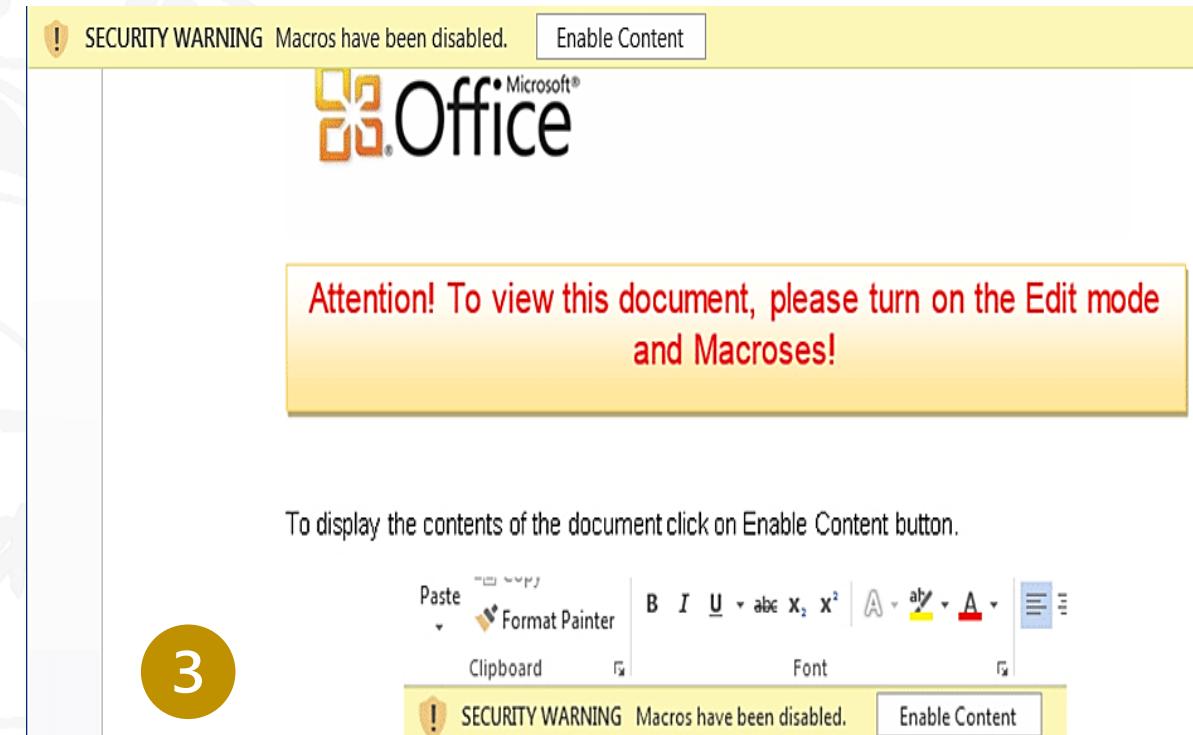
- Excel, Word, PowerPoint...
- ¡No abras ninguno que no conozcas!



**Más imitaciones de avisos, una de ellas incluso imita la típica “pantalla azul” de Windows**

# DOCUMENTOS CON MALWARE DENTRO: CÓMO TE CONVENCEN

- Esto es un **Nivel 3**
- Incluye logos oficiales e instrucciones precisas para activar las macros
  - Quieren que lo hagas y no les vale la excusa de que no sabes hacerlo ☺
- El aspecto es algo más profesional...
  - Pero la disposición de los elementos en el documento “canta” bastante



¡Te hacen mansplaining! ☺



José Manuel  
Redondo López

# DOCUMENTOS CON MALWARE DENTRO: CÓMO TE CONVENCEN

- Estos dos documentos los he clasificado como de **Nivel 3** por la excusa que alegan

- Pero podrían ser nivel 4 fácilmente...
- **El documento está cifrado:** Si lo estuviera, no podrías leerlo (ni las instrucciones)
- **El documento está protegido:** Si lo estuviera te pediría una clave, no que “habilites el contenido”

- Vemos logos oficiales y de empresas de seguridad para dar “credibilidad”

- Vemos un aspecto gráfico más cuidado
- Especialmente el de abajo
- Y más mansplaining...

The image contains two side-by-side screenshots of Microsoft Word documents. Both screenshots show a yellow security warning bar at the top with the message "SECURITY WARNING Macros have been disabled." and a "Enable Content" button.

**Screenshot 1 (Top):** This screenshot shows a document from "GlobalSign PKI Secure". It features a large blue circular logo with the text "GlobalSign® PKI Secure". Below the logo, there is a section titled "FOLLOW THIS STEPS TO DECRYPT DOCUMENT". A numbered list starts with "1. Read the privacy policy www.globalsign.com/en/repository/". A callout bubble with the number "3" points to a context menu that includes options like "Insert...", "Delete", "Rename", "Move or Copy...", "View Code", and "Unguard Sheet...". To the right of the menu, there is explanatory text about enabling editing if the document was downloaded from the internet and about running Plugin Core decryption.

**Screenshot 2 (Bottom):** This screenshot shows a Microsoft Word document with the "Office" logo at the top. The main content area says "Oops, something went wrong". Below this, there is a numbered list of three steps:

1. Open the document in Microsoft Office. Previewing online is not available for protected documents
2. If this document was downloaded from your email, please click Enable Editing from the yellow bar above
3. Once you have enabled editing, please confirm update the fields in this document

To the right of the list, there is an illustration of a padlock on a stack of papers. A callout bubble with the number "3" points to the third step in the list.

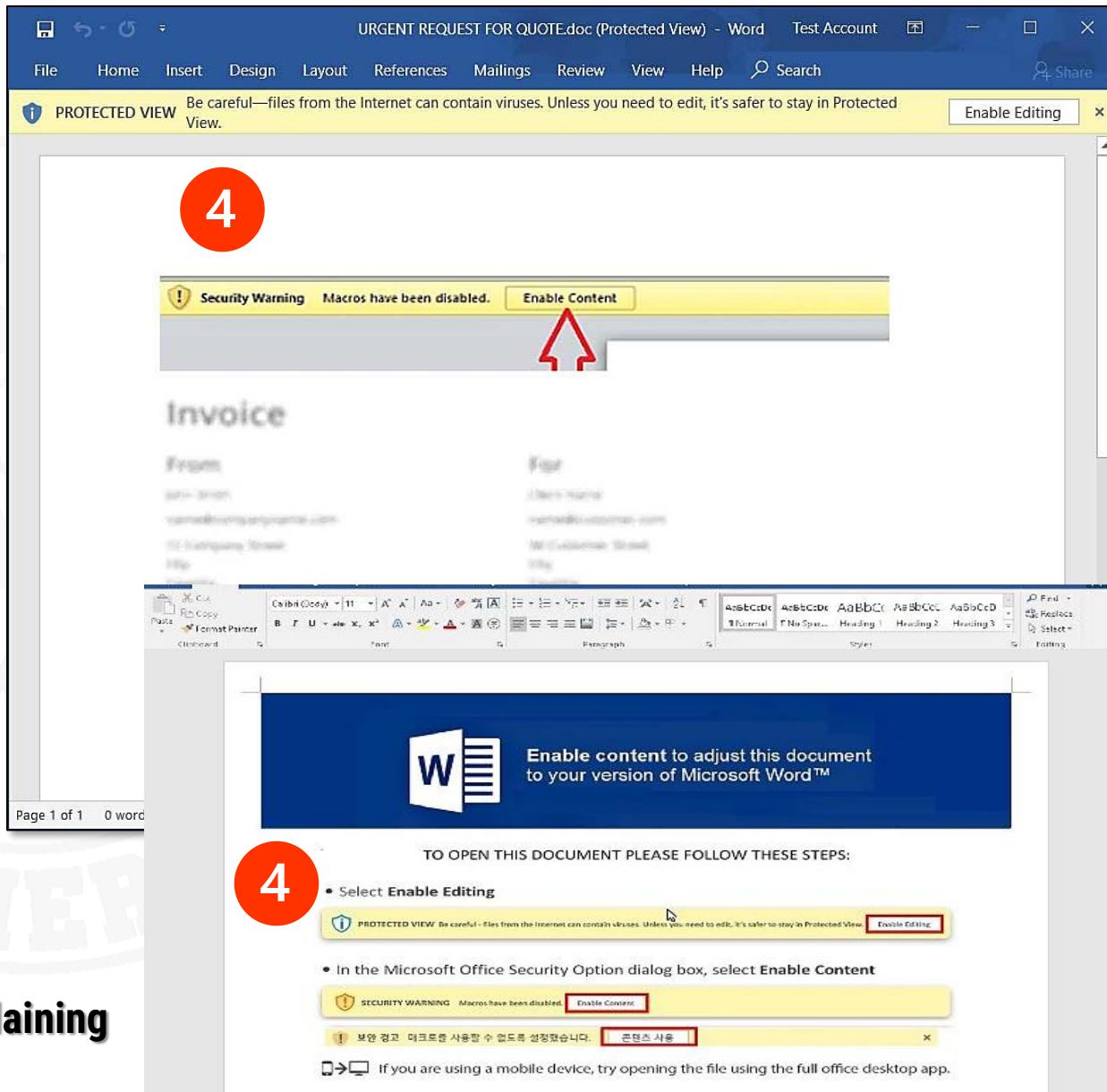


José Manuel  
Redondo López

# DOCUMENTOS CON MALWARE DENTRO: CÓMO TE CONVENCEN

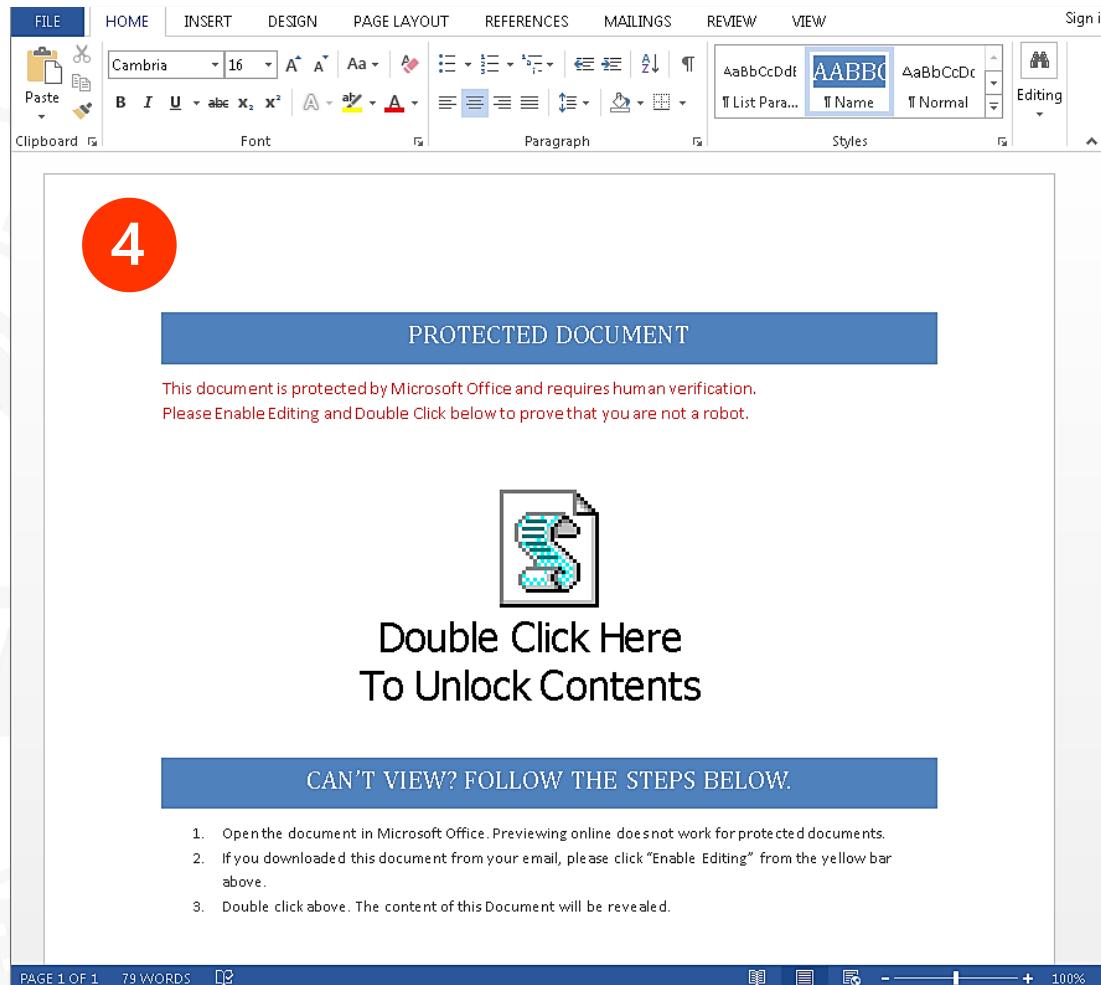
- En un **Nivel 4** ya vemos mucho más trabajo gráfico
- En algunos el supuesto documento que contiene el fichero aparece sombreado
  - A la espera de que lo “desprotejamos”
  - Es totalmente falso, claro, es otra táctica para engañarnos
- Tienen instrucciones precisas y un aviso en colores de Windows
  - ¡Todo vale para pedirnos que le demos al botón!

¡Te hacen mansplaining  
“on steroids”! ☺



# DOCUMENTOS CON MALWARE DENTRO: CÓMO TE CONVENCEN

- Este es otro ejemplo de un **Nivel 4**
- Redacción profesional, con estilos y párrafos
- Presentación cuidada de los contenidos
- Excusa más creíble (“**human verification**”)
  - ¡Quieren que le des al botón para comprobar que eres una persona!

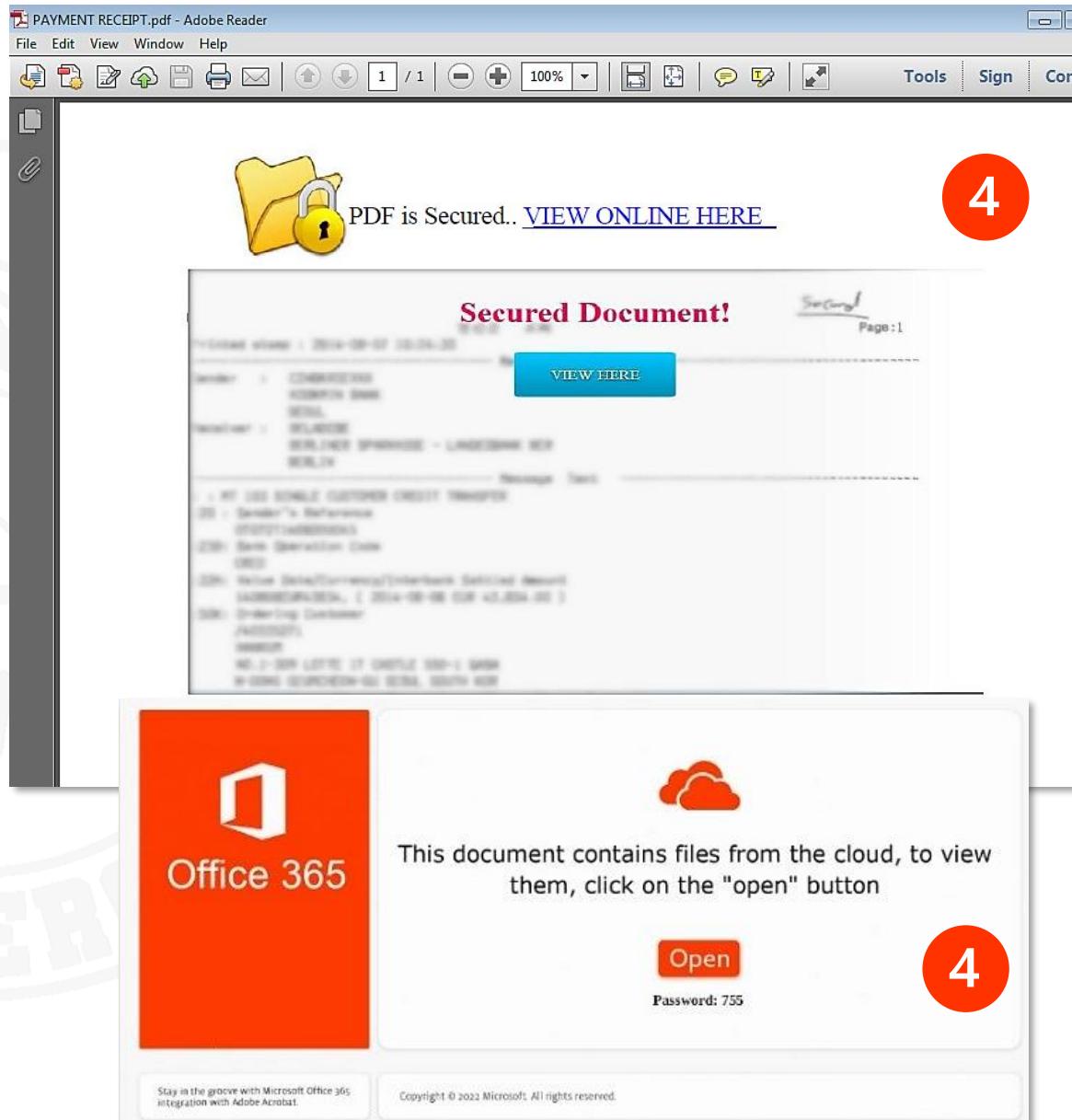


**Mansplaining “on steroids” y encima apelando a que no eres humano...**

# DOCUMENTOS CON MALWARE DENTRO: ¿Y LOS PDF?



- Hay una creencia popular de que los PDF no pueden contener malware, pero no es cierto
    - Pueden ser peligrosos aprovechándose de versiones viejas del lector
    - O de fallos conocidos del mismo o su configuración
  - O pueden engañarte para que cliques en un enlace que te lleva a una web
    - Y en esa web es donde está el peligro
  - Es decir, tienen “bicho” o son portadores del sitio donde está el “bicho”



# DOCUMENTOS CON MALWARE DENTRO: COSAS A TENER EN CUENTA...

## ● De nuevo no te dejes engañar porque muchos ejemplos estén en inglés

- He visto equivalentes en Español de casi todo lo que te propongo aquí
- *¿Y por qué no nos los has puesto en Español?* Porque la redacción era muy cutre, y desvirtuaba la explicación del timo ☺
- Y recuerda, las IA traducen muy bien hoy en día...

## ● Da igual el nivel, el objetivo siempre es el mismo: **que pulses en el botón de “habilitar contenido”, ¿Para qué?**

- El documento trae dentro un programa (malware)
- Al habilitar contenido das permiso al Office para que arranque ese código
- **Y es el que hará el verdadero daño**
  - Robarte datos, instalarte más malware, bloquearte el PC, cifrártelo...
  - Es decir, sí que le estás diciendo al malware “venga, arranca”...
    - Solo que con la pulsación de ese botón “Habilitar contenido”
- **Así que ¡NO PULSE EN ESE BOTÓN NUNCA!**

# DOCUMENTOS CON MALWARE DENTRO: COSAS A TENER EN CUENTA...

- **¿Esto de habilitar contenidos tiene entonces algún uso legítimo?**

- Siempre me preguntan *¿Por qué no se quita si solo da problemas?*

- **¡Sí!, se creó para hacer documentos “inteligentes”**

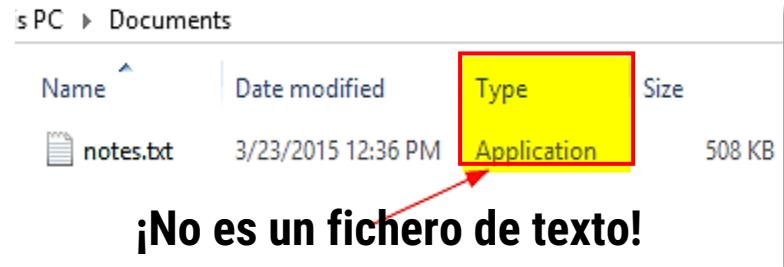
- Que **comprueben los datos** que se le introducen (fechas que sean fechas, edades que sean números, etc...)
- Que den **mensajes de error** / aviso / instrucciones si el usuario hace algo mal
- Que **calculen datos** a partir de otros datos
- Que se **auto rellenen** en función de lo que los usuarios vayan introduciendo
- ...

- **Pero todo esto ahora se usa mayoritariamente para el mal**

- Se que muchas administraciones usan documentos con esas características...
- ... pero debemos estar **MUY SEGUROS** de la procedencia del documento para habilitar su contenido

# ¿PUEDE UNA IMAGEN O UNA CANCIÓN TENER UN MALWARE?

- Es técnicamente posible (aunque bastante raro) que un fichero de esta clase tenga dentro **malware**
  - Pero para que se ejecute, necesitan aprovecharse de una vulnerabilidad del visor/reproductor
    - O de un segundo programa que lea y execute ese contenido malicioso
  - **Cosa que puedes evitar si los mantienes actualizados**
- Otra cosa es que abramos un documento que **CREAMOS** que es una imagen / canción, pero es un malware
  - Se suele recurrir a técnicas que **falsifican la extensión de un fichero**
  - Por ejemplo, poner una doble: `mitexto.txt.exe`
    - Es un programa, pero vemos `mitexto.txt`
    - Por defecto no se muestran las extensiones de los ficheros
    - Si hacemos doble clic estamos perdidos
    - ¡Se ejecuta un programa!





## Documentos falsos



# FALSIFICACIONES: MALICIOSOS, PERO PORQUE TE ENGAÑAN

## ● A veces lo que engaña es el contenido

- El documento no tiene malware alguno... pero el contenido es completamente falso
- **Se usan como refuerzo (aumentar la credibilidad) en estafas**
- Vamos, **son falsificaciones** ☺

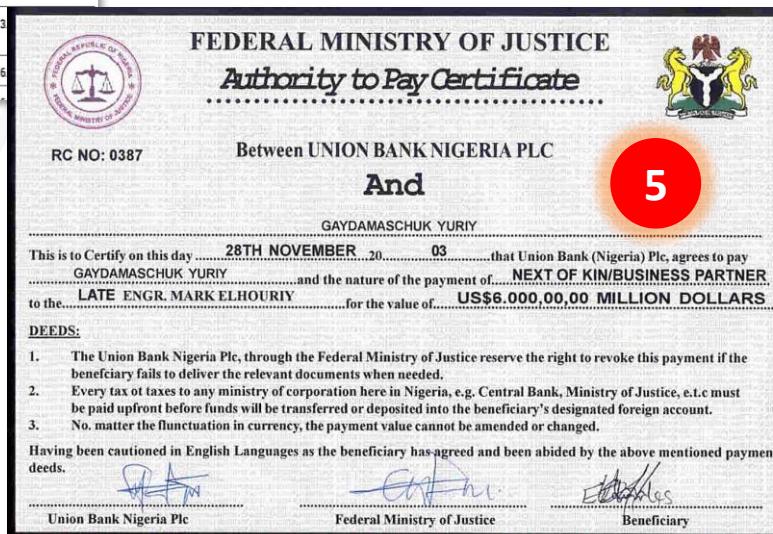
## ● Hoy en día se puede falsificar **TODO** para que parezca real

- De nuevo: las IA...
- Por muy “guapo” que parezca un documento, **todo es falsificable**

## ● Por tanto, ¡no hay que basar las decisiones solo por el aspecto de un documento!



**Firmas, sellos, logos,  
emblemas...da igual  
¡Todos estos son  
falsos!**



# FALSIFICACIONES: MALICIOSOS, PERO PORQUE TE ENGAÑAN

- Por tanto, es el contenido el problema, pero porque es mentira

- Es uno de los vehículos más usados para **propagar desinformación**

- Hay canales de **Telegram**, etc. donde se difunden muchos documentos falsos

- Con fines políticos, religiosos, ideológicos...

- Algunas falsificaciones son **muy buenas**

- Algunas pueden descubrirse con la búsqueda de imágenes en Google (**F-31 “Descubierta”**)
- Otras, con **Maldito Bulo** (**F-31 “Descubierta”**)
  - Lo mismo que **Maldito Timo** (<https://maldita.es/timo/>)
  - Pero para fake news

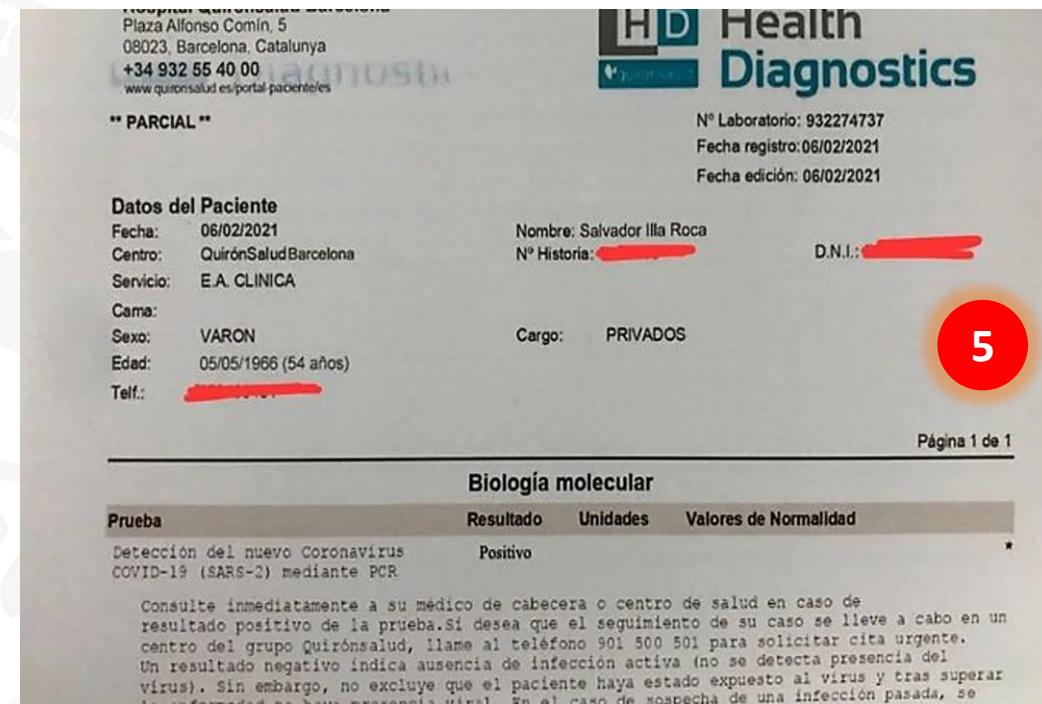


Imagen que se difundió vía Telegram de una falsa PCR positiva del entonces ministro Salvador Illa con fines políticos. Fuente:

[https://www.lasexta.com/noticias/nacional/elecciones-Cataluña/psc-denuncia-fiscalia-alvise-perez-difusion-falsa-pcr-positiva-salvador-illa\\_2021021260267d0fec8b8d0001a891b6.html](https://www.lasexta.com/noticias/nacional/elecciones-Cataluña/psc-denuncia-fiscalia-alvise-perez-difusion-falsa-pcr-positiva-salvador-illa_2021021260267d0fec8b8d0001a891b6.html)

# ¿CREEES QUE LO HAS ENTENDIDO TODO? ¡AUTOEVALÚATE!



- *¿Entiendes que las falsificaciones ya no son "cutres", sino lo contrario?*
- **Respecto a los documentos que recibes...**
  - *¿Comprendes el problema de los documentos maliciosos que llevan enlaces?*
  - *¿Comprendes el problema de los documentos maliciosos que llevan archivos adjuntos (aunque no los veas) y lo que quieren los delincuentes que hagas con ellos?*
  - *¿Entiendes que hoy en día se puede falsificar todo en lo relativo al aspecto de un documento?*
  - *¿Has entendido que, aunque un documento no llegue contenido malicioso per se, en caso de que sea falso se puede usar para otro tipo de ataques que pueden ser igual o más peligrosos?*
  - *¿Entiendes como esto afecta a las enormes campañas de desinformación que tenemos en nuestro día a día tanto en internet como en algunos medios de comunicación?*



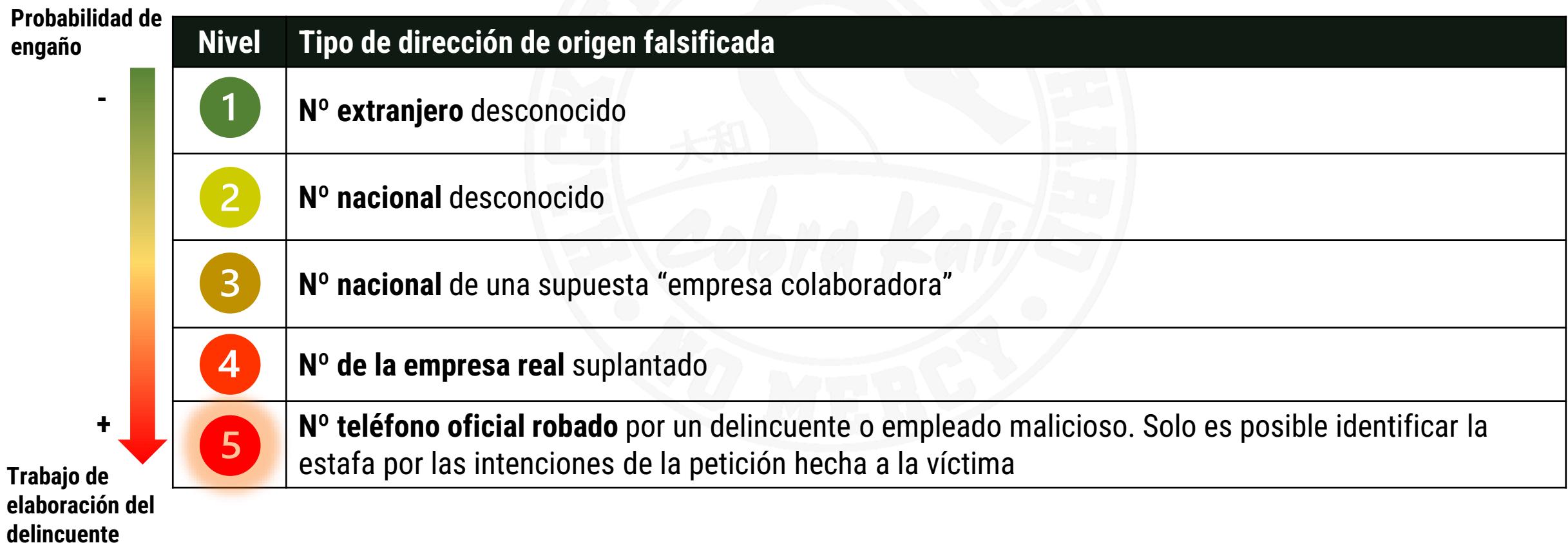
## Llamadas y mensajes falsos

Formas de comunicarse contigo (teléfono, emails, mensajes de RRSS, apps...) para engañarte



# SMS O LLAMADAS FALSIFICADAS: Nº DE TELÉFONO DE ORIGEN

- Los nºs de origen de llamadas / SMS pueden ser falsificados con el equipamiento adecuado ¡No te fíes!
  - Es una técnica llamada “Caller ID Spoofing”: [https://en.wikipedia.org/wiki/Caller\\_ID\\_spoofing](https://en.wikipedia.org/wiki/Caller_ID_spoofing)





José Manuel  
Redondo López

# SMS O LLAMADAS FALSIFICADAS: Nº DE TELÉFONO DE ORIGEN

- ¡Los SMS falsos con nº falsificados **aparecen en la misma lista que los reales!**

- Esto es muy peligroso, al aumentar su credibilidad

- Si es un SMS, su contenido será como el que veremos en el apartado de mensajería

- En general puedes asumir que **si un SMS lleva un enlace ES FALSO**
- Los reales te dicen “Vete a tu cuenta de...” pero no te ponen el enlace para que pulses en él

- Si es llamada, el interlocutor usará **CUALQUIER PRETEXTO** para que

- Le **des información personal** (cuentas bancarias, etc..)
- **Instales un programa** (virus, toma de control de tu PC...)
- Que **contrates un servicio** que no cumpla lo prometido, sea engañoso o fraudulento (falsos contratos de telefonía/luz/gas...)
- Cualquier otra cosa que le dé un beneficio (recuerda lo que hablamos)

¡Puede pasar con cualquier remitente!

Unicaja Banco: Vas a enviar 20,66 EUR por BIZUM al telefono [REDACTED] Clave de seguridad 436963 REAL

Unicaja Banco: Vas a enviar 2,20 EUR por BIZUM al telefono [REDACTED] Clave de seguridad 376333 REAL

sábado • 12:13

Unicaja Banco: Vas a enviar 10,50 EUR por BIZUM al telefono [REDACTED] Clave de seguridad 773689 REAL

14:35

ESTAFADA!

Se ha vinculado un nuevo dispositivo (iPhone X, Ibiza) el 11/07 a las 14:33h. Si no reconoce verifique inmediatamente: <https://unicaja-movil-alerta.com/r/univia>

Toca para cargar la vista previa



José Manuel  
Redondo López

# SMS O LLAMADAS FALSIFICADAS: Nº DE TELÉFONO DE ORIGEN

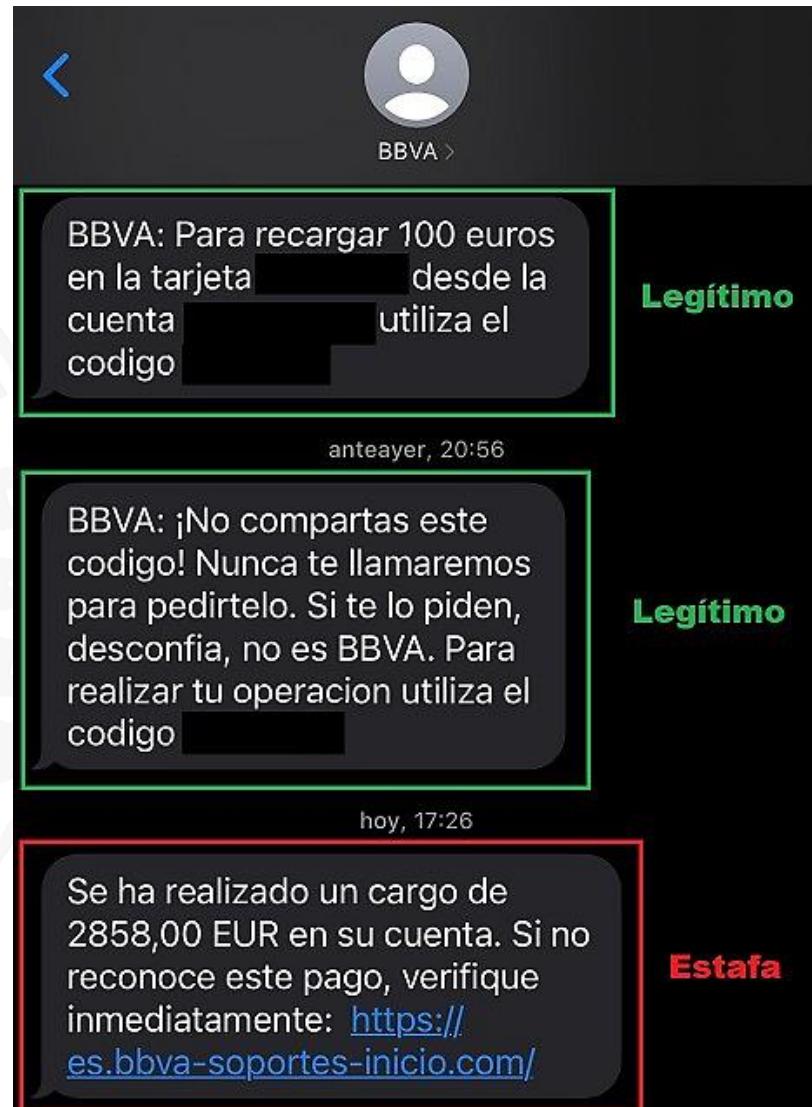
- Esto de que se mezclen mensajes reales y falsos en el mismo hilo de mensajes está causando estragos

- Recuerda lo siguiente: **El teléfono realmente no sabe quién te escribe**

- Él solo ve **un nombre o nº de remitente** cuando le llega
- Y mete el mensaje en el “cajón” que tiene con ese nº o nombre
- Pero, como decía, ese nº o nombre es **100% falsificable...**
- Así que el teléfono no tiene la culpa
- **Le han engañado**, como lo están intentando hacer contigo

- Por supuesto hay servicios que trabajan detectando estas cosas

- Si el teléfono te dice que un mensaje es spam, **créelo**
- **¡Es muy muy raro que falle!**

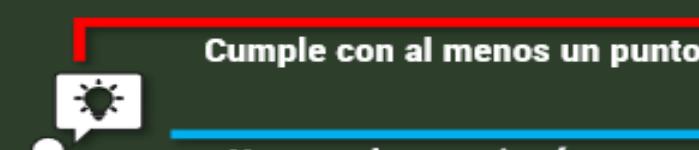


De verdad, esto es un señor problema...

# RECONOCIMIENTO RÁPIDO DE MENSAJERÍA / SMS SOSPECHOSOS

¿El mensaje cumple con alguno de estos puntos? ¡Considera seriamente borrarlo!

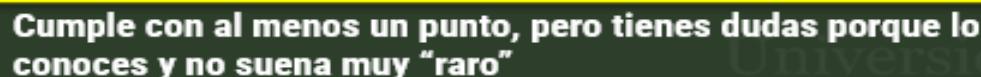
## ¿QUÉ HAGO?



Cumple con al menos un punto



No cumple con ningún punto



Cumple con al menos un punto, pero tienes dudas porque lo conoces y no suena muy "raro"

Bórralo y/o denuncia



Contacta tú con el interlocutor



Confirmación

Ábrelo, pero cuidado con los adjuntos (si los lleva)

### 🚫 De:

- Remitente **desconocido, no habitual** o no tengo **referencias** suyas
- No es de mi empresa** o no tiene que ver con ella
- Le conozco** (empleado, proveedor, cliente...) pero me escribe algo **atípico o diferente a lo habitual**
- El nº del que viene es **conocido**, pero el contenido **me causa alarma e incluye un enlace**

### 🚫 A:

- Es de un **grupo de conocidos**, pero cuentan noticias u opiniones sin contrastar (**típica distribución de bulos**)



### 🚫 Adjuntos

- No lo esperaba o sin relación** con el contenido
- Nunca manda adjuntos** y ahora sí, sin explicación
- Es un fichero comprimido, un fichero Office, un PDF o similar**
- Doble extensión** (Ej.: .txt.exe) (**fraude seguro**)

### 🚫 Texto

- Me pide hacer clic en un enlace o abrir el adjunto, da igual el motivo (**++fraude**)
- Es atípico, **usa mal el idioma** (ortografía, tiempos verbales, vocabulario...), usa un **traductor automático** o usa un **saludo genérico**
- Me manipula con **culpa, chantaje, preocupación** (robo de cuentas, pago de multas...) o **amenazas veladas** (**++fraude**)
- Me pide **una acción urgente / inmediata**

### 🚫 Enlaces

- Enlace acortado** (**++fraude**)
- Apunta a webs parecidas a la real pero **con errores** (Ej.: rnrw.es, google.com...)

# MENSAJES FALSIFICADOS: DIRECCIÓN DE ORIGEN

- Por dirección de origen entendemos cuenta de correo (email) o usuario emisor (RRSS, app de mensajería, videojuego), etc...
  - El **remitente de un email puede ser falsificado si tu servidor de correo está mal configurado**
  - Es algo que tú no puedes saber ¡no te fíes de un remitente conocido si el contenido es extraño!

Probabilidad de engaño



Nivel	Tipo de dirección de origen falsificada
1	Dirección aleatoria (números y letras sin sentido de proveedor público, ej. Gmail) / cuenta de nombre aleatorio sin verificar/desconocida, posiblemente recién creada y/o con pocos seguidores
2	Dirección con el nombre del remitente o empresa, pero de <b>proveedor público</b> / cuenta con un nombre de persona o proveedor sin verificar/desconocida, posiblemente recién creada y/o pocos seguidores
3	Dirección que <b>trata de imitar en su nombre</b> a la dirección completa de una cuenta oficial, pero de proveedor público / cuenta sin verificar/desconocida con contenido clonado de la oficial, con bastantes seguidores comprados o bots
4	<b>Dirección falsificada pero idéntica a la oficial</b> / cuenta verificada robada, pero que se modifica su nombre y contenidos para ser un clon perfecto de la oficial, con muchos seguidores comprados / bots
5	Dirección / <b>cuenta oficial robada</b> por un delincuente o empleado malicioso. Solo es posible identificar la estafa por las intenciones de la petición hecha a la víctima

Trabajo de elaboración del delincuente



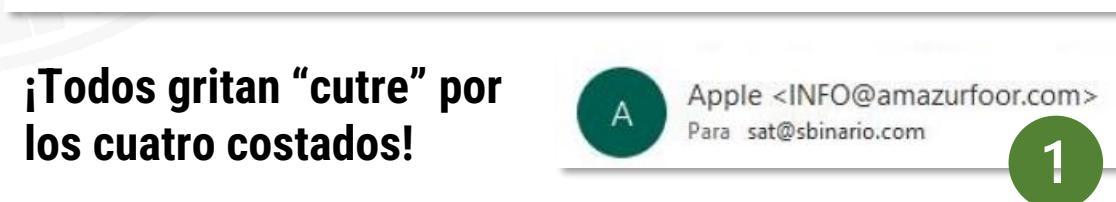
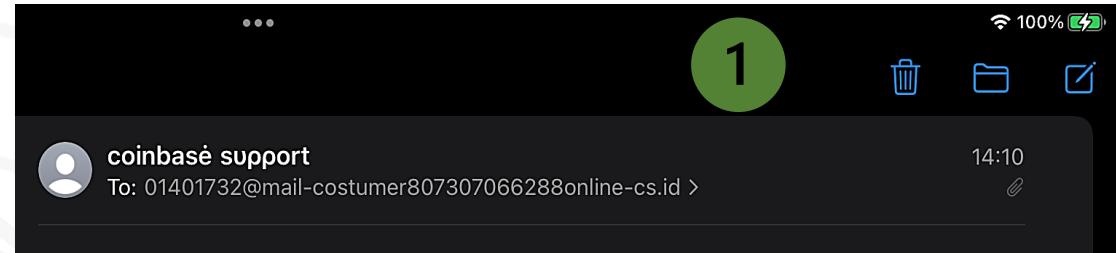
José Manuel  
Redondo López

# EJEMPLOS DE DIRECCIONES FALSIFICADAS

## ● Ejemplos de direcciones de email de Nivel 1

- Enormes direcciones con nºs y letras aleatorios
- Direcciones de proveedores públicos (Gmail, Outlook...) haciéndose pasar por una empresa u organismos
  - Sí, ya sé que no pocas empresas usan un correo personal en lugar del oficial
  - Pero en vista de cómo están las cosas, hay que tener mil ojos en estos casos
  - O no fiarte nunca de ellos
- Direcciones con nombres con evidentes faltas de ortografía
- Direcciones que no tienen nada que ver con quien manda el mensaje

## ● ¿Es esto común? Ya sabes la respuesta, ¿no? Ya no





José Manuel  
Redondo López

# EJEMPLOS DE DIRECCIONES FALSIFICADAS

## ● Aquí varios ejemplos de Nivel 2

- Comisarios que te escriben desde Gmail
  - Los comisarios no te contactan así, y menos desde un proveedor público de email
- Empresas que te contactan
  - Pero el dominio del correo (lo que va tras la @) no es el de la empresa
- Direcciones que **imitan sitios conocidos** (youtub) pero de Gmail
- Sistemas de transferencias de archivos gratuitos (**WeTransfer**) para simular emails de otra persona
  - Incluyendo una dirección real en el asunto
  - Ejemplo:  
[https://twitter.com/ing\\_juan7a/status/1512413417960792064?t=nCxqQH0ZfkwJEaJtf5qg6w&s=19](https://twitter.com/ing_juan7a/status/1512413417960792064?t=nCxqQH0ZfkwJEaJtf5qg6w&s=19)

En este caso su falta de fe (en que el timo funcione) no resulta perturbadora

The image contains three screenshots of fake emails, each with a yellow '2' in a circle in the top right corner:

- Screenshot 1:** An email from 'POLICIA NACIONAL' at 18:07, addressed to 'comisario.veronique.bechu22@gmail.com'. The 'To:' field shows 'comisario.veronique.bechu22@gmail.com'.
- Screenshot 2:** An email from 'Billing <donotreply\_4875@eltbooks.com>' at 3/9/2022 5:59 AM, addressed to 'You'. The 'To:' field shows 'You'. The email subject is 'Your Refund Amazon'. A red oval highlights the recipient's address 'donotreply\_4875@eltbooks.com'.
- Screenshot 3:** An email from 'Seguridad <contact@webcorreo.in>' at 05/04/2022 13:18:10, addressed to 'You'. The 'To:' field shows 'You'. The subject is 'Peligro! Problemas de seguridad con tu cuenta.' The 'From:' field is 'Seguridad <contact@webcorreo.in>'. A red oval highlights the recipient's address 'You'.



José Manuel  
Redondo López

# EJEMPLOS DE DIRECCIONES FALSIFICADAS

En general, hay más trabajo puesto en crear una dirección de email medianamente creíble...

## • Aquí vemos ejemplos más avanzados de Nivel 3, con dos casos

1. En el nombre del remitente y/o parte de la dirección de correo **imita la dirección de correo real**
  - Pero el correo es falso (otro proveedor de correo)
2. La dirección de correo **se crea en función del objetivo** del email (pagos, cobros...)
  - Pero el dominio no es el real (el proveedor de email es **diferente al oficial**)
  - Se suelen usar proveedores poco conocidos por el público general para levantar menos sospechas
  - ¡Hay otros aparte de Gmail y Outlook! ☺

The screenshot shows an email inbox with four messages, each highlighted with a large orange circle containing a number (3). The messages are:

- UD** Unidad de Investigación de la Tecn... 20:12  
Ministeriodejusticia@gov.com
- A** apoyo.actualizar.pago74... 10:19  
para mí ^  
De apoyo.actualizar.pago7444@debb...me via SurveyMonkey • member@surveymonkeyuser.com
- DS** DKV Salud <manager@rankon.co>  
Para sat@sbinario.com
- AB** Amazon Business <supplier@promcenter.co>  
Para sat@sbinario.com
- V** Voss@gaudiosa.greencom...  
Para sat@sbinario.com



José Manuel  
Redondo López

# EJEMPLOS DE DIRECCIONES FALSIFICADAS

- Aquí tenemos ejemplos de **Nivel 4**
- Es la suplantación de direcciones de correo reales
  - Es decir, **tu LEES la dirección que conoces**
  - Pero quien te escribe es un delincuente que la suplanta
  - La culpa es **de vuestro sistema de correo**, no vuestra
    - No verifica que la dirección de origen sea realmente quien dice ser
    - Si se hiciera bien, el correo se rechaza o acaba en spam
  - Los atacantes saben que vuestro sistema no está bien y pueden mandaros un correo en nombre de quien quieran
  - Además, buscan nombres de empleados (Ej.: LinkedIn)
- ¡Son MUCHO más frecuentes de lo que crees!

Algunos remitentes son 100% falsificables y no hay nada que puedas hacer.

**Asume que todo correo puede ser falso, aunque venga de la dirección real**

De: [SERVICIO\\_AL\\_CLIENTE48350207@santander.es](mailto:SERVICIO_AL_CLIENTE48350207@santander.es)

Fecha: 12/4/22 2:07 (GMT+01:00)

Para:

<REDACTED>

Asunto: ! SERVICIO AL CLIENTE Santander Espana - tu cuenta necesita atencion. - ( 478695732431 )

4

Notificación Dirección General de la Policía



notificaciones@policia.es (notificaciones@policia.es)

Para:

4

RA

Rosana Alfonso <r.alfonso@ibipal.com>  
Para Rosana Alfonso

4

RG

Rodríguez Gonzalez <rodrigonarez@prolactea.com>  
Para Raul Jesus

4

FY

Factoring y Confirming - Grupo Santander <fycout@gruposantander.es>  
Para undisclosed-recipients:

4

DS

Deniz SEVİNÇ <denizsevinc@marslogistics.com>  
Para undisclosed-recipients:

4

C

Confirming.bbva@bbva.com  
Para undisclosed-recipients:

4

PS

Pablo Soler Lillo <psoleir@hinojosa.es>  
Para Pablo Soler Lillo

4

M

MetaMask

[support@metamask.io](mailto:support@metamask.io)

Para

Tú

4

miércoles, 16 de febrero 08:30

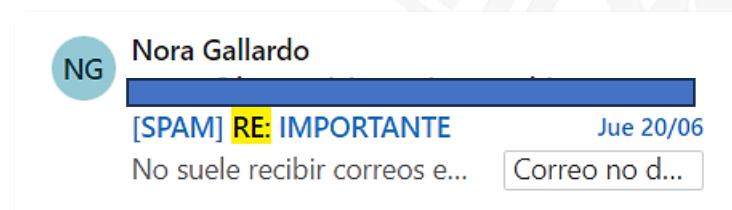
:

# MENSAJES FALSIFICADOS: CONTENIDO DEL MENSAJE

- Los cuerpos de los mensajes tienen los **mismos niveles que los documentos**
- Con las siguientes particularidades
  - A veces se usa la **excusa de no ser nativo** para justificar la mala redacción
  - **Saludos y formas de dirigirse genéricas**, no nombres (indicio de mass mailing)
  - Pueden tener **adjuntos** (programas, documentos) y enlaces a páginas que, como vimos...
    - Al navegar por ellas descargan e instalan (o te invitan a hacerlo), cualquier tipo de malware
    - Te piden datos para robártelos
    - **Te invitan a instalar "extensiones" para tus RRSS**
      - Que propagan el intento de estafa a tus contactos
  - Es mucho más probable que **se juegue con el factor prisa**
    - Para que no pienses y hagas clic o instales lo que te pidan
  - En cuanto a los enlaces recibidos...
    - Usan acortadores de enlaces ([t.com](#). [lnkd.in](#)...) para que no se sepa exactamente a donde van
    - **¡Nunca te fíes de nada que lleva un enlace acortado!**
    - Si no los usan, pueden recurrir a los trucos que veremos luego para falsificar la URL

# EL TÍTULO DE UN MENSAJE Y EL “CLICKBAIT”

- Para que seas víctima de un mensaje fraudulento lo primero que tienes que hacer es leerlo
- Y para eso se recurren a las mismas técnicas que las noticias de muchas webs y periódicos: el **clickbait**
  - Crearte **alarma** (multas, denuncias...) o urgencia (debes contestar rápido)
  - Hacerte creer que es una **oportunidad/oferta increíble**
  - Hacerte creer que es la **respuesta a un correo que has enviado tú** (incluyen “Re:” en el asunto)
  - Estudian lo que haces en tus redes sociales y con esa información mandarte algo que creen que te interesará
    - Aunque eso es más frecuente cuando la víctima eres expresamente tú por algún motivo
  - ...



Si tu cliente de correo añade [ SPAM ] al asunto del mensaje, ni te molestes. Si en lugar de eso es [ BULK ] tiene una probabilidad altísima de ser spam

# EL TÍTULO DE UN MENSAJE Y EL “CLICKBAIT”

## • Vemos aquí varios ejemplos reales

- **Meter prisa** (asunto urgente o que caduca)
- **Supuestos premios**
- **Supuesta confirmación de asuntos importantes** (transferencias)
- Simular **comenzar un negocio** (que la empresa oferte algo)
- **Fingir ser la respuesta** a un mail anterior (en realidad solo añaden “Re:” al título)

Todos transmiten el mensaje: “¡Haz clic! ¡Ya! ¡Mira!”

**Re: [Alert] [Dear Customer]: We lock your amazon account and hold all your last orders on Monday, April 4, 2022 (EST)**

You Could Win! See Inside to Get your Apple Reward

Pago de factura pendiente

Notificación de Transferencia realizada

SOLICITUD DE OFERTA

RE: presupuesto urgente

Re: Orden de compra de enero (P.O\_343209) ¡Un recordatorio!

¡Rápido, rápido, rápido! De momento se ofrecen 30€ con Amazon Business

# RECONOCIMIENTO RÁPIDO DE CORREOS SOSPECHOSOS

*¡Cuantas más casillas puedes marcar, el mensaje será menos de fiar!*



**De:**

- Remitente **desconocido, no habitual** o no tengo **referencias** suyas
- No es de mi empresa** o no tiene que ver con ella
- Le conozco** (empleado, proveedor, cliente...) pero me escribe **algo atípico o diferente a lo habitual**
- El dominio del remitente es "raro"** (muy largo, con guiones, con letras y nºs sin sentido...) y es el oficial (Ej.: [mrw-clientes.com](http://mrw-clientes.com), [unicaja-banco.uk](http://unicaja-banco.uk)...)



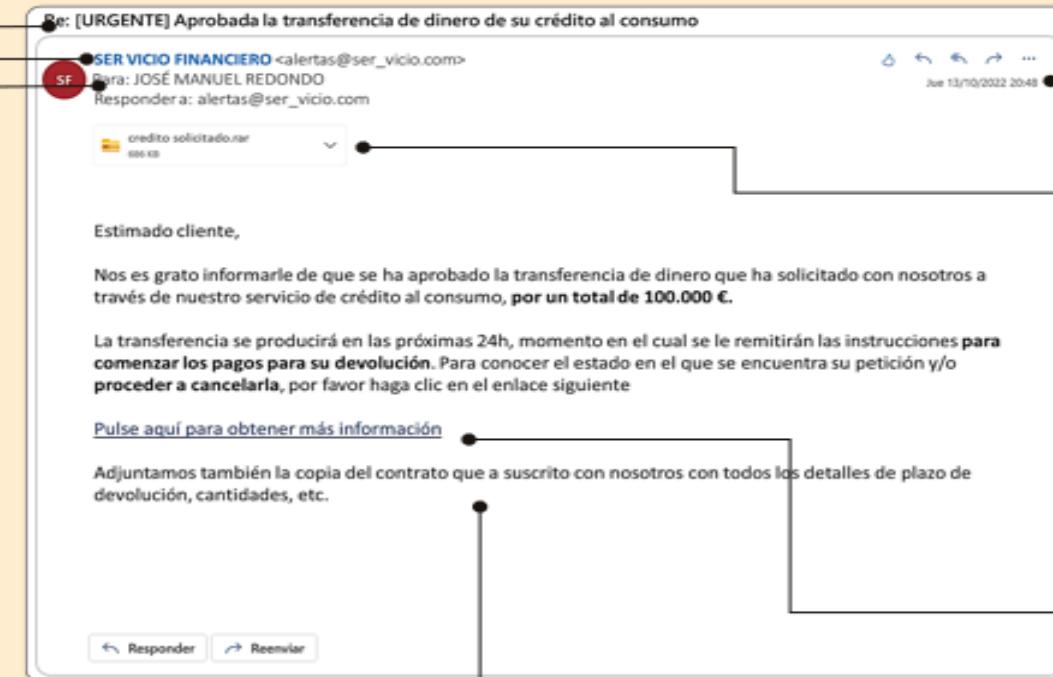
**A:**

- Estoy en copia (CC) con más personas, **pero no sé quienes son**
- Estoy en copia (CC) con gente de mi trabajo, pero **no veo relación** entre ellos o hay un **patrón** (Ej.: orden alfabético de apellido)



**Asunto**

- No tiene sentido o no encaja con el contenido** del mensaje
- Pone **Re:**, pero **nunca le he mandado un mensaje**
- Me habla de algo **urgente**



**Texto**

- Me pide hacer clic en un enlace o abrir el adjunto **para ganar algo**, porque tiene **información comprometedora** u otros **motivos extraños** ([++fraude](#))
- Es atípico, **mal uso del idioma** (ortografía, tiempos verbales, vocabulario...), usa un **traductor automático** o tiene un **saludo genérico** (Ej.: "Estimado usuario")
- Intenta manipularme con **culpa, chantaje, preocupación** (robo de cuentas, pago de multas...) o **amenazas veladas** ([++fraude](#))
- Me pide **una acción urgente / inmediata**



**Fecha**

- Es de mi trabajo, pero **fuera de horas**



**Adjuntos**

- No lo esperaba o sin relación** con el contenido
- Nunca me manda adjuntos** y ahora sí, sin dar explicación
- Es un fichero comprimido, un fichero Office, un PDF o similar**
- Doble extensión** (Ej.: .txt.exe) (**fraude seguro**)



**Enlaces**

- Si paso el ratón por encima **SIN HACER CLIC**, la dirección en la barra inferior del navegador es otra ([++fraude](#))
- Es un enlace acortado**
- Apunta a webs parecidas a la real pero **con errores** (Ej.: [nrw.es](http://nrw.es), [google.com](http://google.com)...)



**Basado en:**

<https://www.knowbe4.com/hubfs/Social-Engineering-Red-Flags.pdf>



José Manuel  
Redondo López

# EJEMPLOS REALES DE MENSAJES FALSOS

## ● Estos mensajes de **Nivel 1** son los que la gente cree más comunes

- No hay elementos gráficos, texto mal redactado, etc..
- **¡Ya no son comunes! ¡Los delincuentes están evolucionando!**

## ● Algunos meten una cantidad enorme de caracteres en blanco o puntos

- Para saltarse filtros de contenido
- Todo email que venga así es falso, no hay mucho que discutir ☺

## ● En general, tienen un aspecto nada profesional y son fácilmente identificables

### Ejemplos de correos falsos de calidad terrible

----- Forwarded message -----  
De : JURISDICCIÓN <m262143@gmail.com>  
Date: sam. 5 févr. 2022 à 12:52  
Subject: Fwd: J-ES 05/02/2022  
To:

2 archivos adjuntos



1

Recursos humanos Recibidos

V Recursos humanos 6:46 p. m.  
para mí ▾

Usted a sido despedido de su empresa para que pueda ser reintegrado debe consignar \$45000 a la siguiente cuenta  
453 [REDACTED]

Es muy importante que usted haga esto para que pueda seguir trabajando en la empresa

Gracias

Recursos humanos

Get Outlook para Android

☆

...

1

De: "WeTransfer Noticia 13034" <aviso03199@transfer.mu>  
Para: "Cobros [REDACTED]"  
Enviado: 05/04/2022 13:18:10  
Asunto: juridico@abogados204.es te ha enviado archivos

juridi.co@abogados976.es  
te ha enviado archivos  
2 archivos, 1 MB en total. Se eliminará el 5 de Abril de 2022.  
Descarga tus archivos

Le hemos enviado la citación sobre la infracción de la marca en su sitio [REDACTED]  
Enlace de escanear  
<http://wetransfer.com/d/ownloads/syfssKN7> [REDACTED]  
2 archivos  
citación del juzgado Abril 2022.pdf  
infracción de la marca en su sitio [REDACTED]

Acerca de WeTransfer Ayuda Condiciones de uso Denuncia transferencia como spam

1

...

# EJEMPLOS REALES DE MENSAJES FALSOS



José Manuel  
Redondo López

- Estos mensajes de **Nivel 2** ya usan una redacción más cuidada
- Siguen sin usar elementos gráficos
- Suelen tener muchas menos faltas de ortografía

Rv: investigación

UD Unidad de Investigación de la Tecn... 20:12  
Ministeriodejusticia@gov.com

conv es.pdf PDF - 494 KB

Reporte de investigación

Nuestros servidores nos han permitido identificar y geolocalizar en tiempo real sus direcciones IP utilizadas para ver contenido de pornografía infantil. se le solicita que responda lo antes posible.

Para más información ver el documento

To undisclosed-recipients:☆

Apreciado cliente,

Tu paquete no se ha podido entregar el 28/02/2022 porque no se han pagado los gastos de envío . (2,99 €).

Localizador de envíos: DT20155269ES  
Motivo: Gastos de envío no pagados.  
Terminal: 346841091-1  
Fecha Operación : 29-02-2022  
Importe : 2,99 €

\* [Haga clic aquí](#)

Si la carta certificada no se recibe dentro de los 4 días hábiles, SEUR tendrá derecho a reclamar una compensación en la oficina más cercana. Este es un mensaje generado automáticamente.

Información sobre Protección de Datos:

Condiciones de entrega complicadas Debido a la situación excepcional por el Covid-19 hay dificultad para realizar de todas formas, estamos trabajando para entregarte el pedido lo antes posible Gracias por tu paciencia

Los datos que nos facilite se tratarán con la finalidad de cursar su solicitud y mantener la relación contractual. Puedes consultar la [Política de Privacidad](#)

Sinceramente

El equipo de SEUR Te agradecemos tu confianza.

Greetings,

It's been almost a month since I first contacted you, I'd like to know if you're going to give me any solution

silvia@ewinracing.com 9 dic 2020

Hello ,

The important information for you. See the attachment to the email.

Password - 3426211

Thanks

Info.zip zip

Thank you, I got it. Got it, thanks! Thanks a lot.

Responder Reenviar

acusación contra ti

POLICIA NACIONAL 18:07

para info, Cco: mí

De comisario.veronique.bechu22@gmail.com  
POLICIA NACIONAL y •  
Para info@europol.eu  
Cco [REDACTED]  
Fecha 27 abr. 2022 18:07

Mostrar texto citado

PDF ORGANIZA...INAL 24.pdf

# EJEMPLOS REALES DE MENSAJES FALSOS



José Manuel  
Redondo López

- En el **Nivel 3** aparecen elementos que aumentan la credibilidad del mensaje

## ● Imitación de mensajes reales

- Iconos de webs oficiales
- Aspecto gráfico más cuidado, imitando al original
- Enlaces acortados
  - Para que no se vea claramente a donde se va con un clic
- Falsos iconos para adjuntos ejecutables

Iconos, colores, tipos de letra...son imitaciones, algunas bastante buenas

The collage includes examples from:

- El Ahorro de Estas Navidades:** A message from 'Fibra 100Mb+Móvil 25GB por 39,90€/mes. PRECIO FINAL PARA SIEMPRE.Y GRATIS un Smartphone.' It features a small exclamation mark icon and a link to [bit.ly/2azyb](https://bit.ly/2azyb).
- OFERTON UNICO:** A message from 'Por solo 9,90€/mes llevate 10GB en tu móvil con llamadas ilimitadas. PRECIO PARA SIEMPRE, SIN PERMANENCIA.' It also features a small exclamation mark icon and a link to [bit.ly/2azyb](https://bit.ly/2azyb).
- Departamento Bank America - En Linea:** A message from 'Online ealerts Bank. para Yo Hoy 11:49 a.m.' It includes a logo for 'BANK OF AMERICA' and a link to 'Verificar Datos Personales'.
- Verificación Bank of America:** A message from 'Le agradecemos su preferencia y apreciamos la oportunidad de atender sus necesidades financieras.' It features a photo of Holly O'Neill and a link to 'Divulgaciones legales e información'.
- DHL:** A message from '[DHL]: Su paquete no ha podido ser entregado no se han cobrado las tasas de aduana(1.79€) Puede pagar en este enlace: <https://dhl.express.the-chefcaos.com/track/>'
- Santander:** A message from 'Tu cuenta necesita atención!' It includes a red banner with the Santander logo and a link to 'Comience la verificación'.
- NETFLIX:** A message from 'Error en el pago automático.' It features the Netflix logo and a link to 'Seguridad <contact@webcorreo.in>'.
- cPanel:** A message from 'SU CUENTA DE EMAIL SERÁ BORRADA' with a link to 'CONFIRMAR'.
- Factura Electrónica:** A message from 'Estimado (a) @gmail.com' with a link to 'Contraseña: Últimos 3 dígitos de tu DNI.'
- Amazon:** A message from 'Request your refund now' with a link to 'Request your refund now'.

# EJEMPLOS REALES DE MENSAJES FALSOS



José Manuel  
Redondo López

## ● El Nivel 4 es ya una amenaza mucho más seria

- Y hoy en día muy común

## ● Calcos de mensajes reales

- Direcciones de webs para hacer clic muy bien falsificadas
- Uso de datos reales del destinatario para aumentar su credibilidad
  - Procedentes de filtraciones o ingeniería social

**NETFLIX**

No deje de ver sus películas y series favoritas.

Hola

Hemos cancelado su Netflix cuenta, ya que su pago ha tenido un problema en nuestro centro de cobros. Este cambio tendrá efecto desde 17/09/2019.

Si cambias de opinión y deseas continuar con el servicio, solo actualiza y confirma tus datos, haciendo clic en el siguiente botón para reiniciar la membresía y disfrutar de programas y películas sin interrupción.

**ACTUALIZAR CUENTA AHORA**

**amazon**

Order confirmation

Your "ASUS ROG Strix G17 17.3" FHD 144Hz" is has been dispatched, below are the details related to the purchase.

If you want to make any changes please call +1 (360) 334-6376

Arriving: Friday, April 1, 2022

Ship to: David B. Zaragoza  
1092 Hart Ridge Road  
Saginaw, MI 48607

Your purchase with Order ID -195-1589150521-050812501 is under process.

Order summary

 \$1,599.00

Item Subtotal:	\$1,598.00
Shipping & Handling:	\$15.00
POD Convenience Fee:	\$0.00
Delivery:	\$0.00
Shipment Total:	\$1614.00

If you did not Order it. Contact immediately Amazon Fraud Department +1 (360) 334-6376

We hope to see you again soon!  
Amazon.com

This message is sent to you by the Amazon entity noted.  
2022 Amazon.com, Inc. or its affiliates. Amazon, Prime, Prime Video, and all related  
logos are trademarks of Amazon.com, Inc. or its affiliates.  
Please note that this email was sent you from a notification-only address that can't accept  
incoming emails.  
Please do not reply to this message. If you have any questions and wish to contact  
us, you can call us at +1 (360) 334-6376

Ministerio de Sanidad - 28638  
Tenemos un anuncio urgente sobre la dosis extra de vac...  
Para: PEDRO C...

GOBIERNO DE ESPAÑA MINISTERIO DE SANIDAD

Ministerio de Sanidad  
Estimado(a) - correo electrónico con carácter de urgencia.

Su número de suscripción 6549025-414.802 ha sido seleccionado para recibir una dosis adicional de vacunas contra el COVID-19 en los próximos días. La elección de qué fabricante tomar es opcional según disponibilidad y debe realizarse en un plazo máximo de hasta 72 horas antes de la aplicación de la dosis.

Ahora vea su tarjeta con las instrucciones, el día y la hora. Estará disponible en nuestro portal hasta el 31 de marzo.

**VER TARJETA**

Si desea elegir la marca para la vacunación presencial, imprima el adjunto a continuación y acuda a cualquier puesto de salud con un documento personal con foto.

**PDF**  
[Tarjeta-Vacuna-6549025-414.802.PDF](#)

#YoMeVacunoSeguro © Ministerio de Sanidad

Correo privado a ...

A partir de un mensaje real, lo clonan y lo alteran

# EJEMPLOS REALES DE MENSAJES FALSOS



José Manuel  
Redondo López

## ● La redacción de estos mensajes es exquisita

- No presentan faltas de ortografía
  - Lógico si los hacen básicamente clonando comunicaciones reales
  - Que alteran sutilmente para añadir enlaces/adjuntos maliciosos...
- También mediante el uso de IA

## ● Copian elementos gráficos de los mensajes originales de la compañía, etc.

- Hay trabajo detrás de su elaboración, y por tanto mayor % de éxito

Fíjate en el curro que tienen algunos...aunque muchas veces el curro real lo hizo el original, que se clona

A fake promotional email from Amazon Business. It features a dark blue header with the Amazon logo and the text "Con Amazon Business" and "Compre sus suministros profesionales a precios rebajados". Below this is a yellow button labeled "Cree su cuenta gratis". A circular badge in the top right corner contains the number "4". In the center, there's a blue circle with the text "Ahora, le ofrecemos 30€ a partir de 120€ de compra" and a yellow circle with the text "código promocional BTW22". At the bottom, it says "Amazon Business es la plataforma Amazon reservada en exclusiva a los profesionales. Cree gratis su cuenta y acceda a millones de productos al mejor precio. Además, los precios tienen descuento por cantidad y la entrega en un plazo de 1 día laborable es gratuita para miles de artículos incluidos en Business Prime."

Con Amazon Business  
Compre sus suministros profesionales a precios rebajados

Cree su cuenta gratis

Ahora, le ofrecemos 30€ a partir de 120€ de compra

código promocional  
**BTW22**

Amazon Business es la plataforma Amazon reservada en exclusiva a los profesionales. Cree gratis su cuenta y acceda a millones de productos al mejor precio. Además, los precios tienen descuento por cantidad y la entrega en un plazo de 1 día laborable es gratuita para miles de artículos incluidos en Business Prime.

A fake notification from Santander. It shows a green header with the text "Amazon Business también le brinda:". Below this are three icons: a document labeled "Facturas fáciles", a euro symbol labeled "Supervisión y control", and a credit card labeled "Flexibilidad en".

Amazon Business también le brinda:

Facturas fáciles Supervisión y control Flexibilidad en

A fake notification from Mars Logistics. It starts with "Buenos Días" and asks the recipient to sign and return the attached contract analysis. It then lists the recipient's details: Deniz Sevinic, Especialista asistente de operaciones en el extranjero, Asistente Especialista en Operaciones, and provides a phone number. The footer includes the Mars Logistics logo and website.

Buenos Días

Se adjunta el análisis del contrato. Por favor, firme y devuelva el contrato adjunto para continuar.

Deniz Sevinic  
Especialista asistente de operaciones en el extranjero  
Asistente Especialista en Operaciones  
Teléfono: GSM:

Dirección de Transporte Internacional de Mars Logistics Montaña. Ve tic. Cº  
Mahmutbey Mah. Taşoçagi Yolu Cad.Balance Güneşli No:19/7 Piso del bloque C: 6-7-8  
Madrid  
Teléfono: +34 (212) 4114444 Fax: +34 (212) 4114445

[www.marslogistics.com](http://www.marslogistics.com)

A graphic for the "Women-Friendly Brands Award to Mars Logistics". It features a large green award plaque with a white dove in the center, surrounded by laurel wreaths. The text on the plaque reads "Women-Friendly Brands Award to MARS LOGISTICS". Below the plaque is a smaller text: "We won an award with our Equality Has No Gender project, which we started with the idea that women should have equal rights in every field."

Women-Friendly  
Brands Award to  
Mars Logistics

We won an award with our Equality Has No Gender project, which we started with the idea that women should have equal rights in every field.

A fake promotional offer from DKV Integral Completo. It features a woman swinging on a swing in a park. The offer includes a discount of 36% and a mention of a bonus for choosing a payment method. A circular badge in the top right corner contains the number "4".

DKV INTEGRAL COMPLETO

desde 21,89€

**13€/mes**

**36%** de descuento

¡Oferta mayor!

4 Una bonificación adicional eligiendo la modalidad de pago

Notificación de Transferencia realizada

SF SOTORRIO FERNANDEZ-MIJARES JOSE <josesotorriofer@gruposantander.es>  
Para undisclosed-recipients:  
Justificante de Pago 27012022.docx  
10 KB

Buenos días,

Le comunicamos que hemos recibido instrucciones para emitir la siguiente transferencia a su favor.

Para obtener más detalles, revise el justificante de pago adjunto.

Abrazo y muchas gracias!

Santander | José Sotorrio Fdez.-Mijares  
Director Oficina  
C/ Marqués de Larios, 10. 29005-Málaga  
985.793.950 | 625 480 562  
[josesotorriofer@gruposantander.es](mailto:josesotorriofer@gruposantander.es)

Plan Santander Iberia Plus.   
A TODOS LOS CLIENTES

# ¿CREEES QUE LO HAS ENTENDIDO TODO? ¡AUTOEVALÚATE!



## ● Respecto a teléfonos y mensajes...

- *¿Entiendes que el nº de teléfono/email que te llama o escribe se puede falsificar?*
- *¿Has entendido como esto puede hacer aparecer mensajes SMS falsos en la misma lista de mensajes que otros que son verdaderos?*
- *¿Te ha quedado claro que, en general, cualquier SMS que lleva un enlace es no fiable?*

## ● Respecto a teléfonos, SMS y mensajes...

- *¿Te ha quedado claro que tienes que mirar con lupa al remitente de un correo electrónico para detectar si es una estafa?*
- *¿Eres consciente de que nadie “oficial” te va a mandar un email con una cuenta de un proveedor público (es decir, que se puede hacer una cuenta todo el mundo), como Gmail u Outlook?*
- *¿Has entendido que, incluso aunque la cuenta que te envía el mensaje sea la real, se podría falsificar si el sistema de correo del remitente no está bien configurado, y que eso es algo que tú no puedes controlar?*
- *Por tanto, ¿Te ha quedado claro que lo más sensato es tratar cualquier mensaje de correo como falso por defecto, venga de quien venga, diga lo que diga, y este lo “currado” que esté?*



## Webs falsas

Cuando nos redirigen a webs que son imitaciones (o clones exactos) de las reales





José Manuel  
Redondo López

# WEBS FALSIFICADAS: URL DE LA WEB

- En general se cumplen más o menos las mismas cosas que en los orígenes de los mensajes, con las particularidades de las URL

- Si recibes un enlace cuya dirección visible no es la real (la que se ve cuando pones, **sin hacer clic**, el ratón encima) **es un fraude seguro**

Probabilidad de engaño	Nivel	Tipo de URL falsificada
-	1	<b>URL aleatoria</b> (colección de números y letras sin sentido) de un proveedor de cloud o hosting contratable por un particular cualquiera (Ej.: godaddy)
-	2	<b>URL que imita el nombre de la empresa</b> (paipal.com), o que se aprovecha de errores típicos a la hora de escribir (google.com)
-	3	<b>URL que trata de imitar la de una web oficial</b> o una parte “sensible” de la misma, con un dominio distinto (Ej.: paypal-inspection.com, microsoft.miweb.com) o <b>enlace acortado</b>
+	4	<b>URL falsificada para que parezca idéntica a la oficial</b> con trucos con caracteres, uso creativo de Unicode, etc... muy difícil o imposible de distinguir a simple vista (Ej.: <a href="https://www.xn--80ak6aa92e.com/">https://www.xn--80ak6aa92e.com/</a> en realidad aparece como <a href="http://www.apple.com">www.apple.com</a> en un navegador, pero son caracteres cirílicos Unicode)
+	5	<b>URL oficial robada</b> / dominio oficial expirado comprado por un delincuente o empleado malicioso. Sólo es posible identificarlo por software de seguridad de terceros / integrado en el navegador

# TÉCNICA PARA SABER CUÁNDO UNA URL ES FALSA

- Te llega un enlace acortado: ([t.co/...](#), [bit.ly/...](#), [goo.gl/...](#)) demasiado riesgo, **asume que es falsa**
  - Hay formas de saber hasta dónde llevan sin riesgo (expandirlas), pero **es mejor ignorarlos**
- Si no es un enlace acortado, hay **aprender a leer las URLs (las direcciones de las webs, vamos)** y para ello:
  - Quítale el [http://](#) o el [https://](#) si lo tiene
  - **Con lo que te queda, léelo empezando por el primer ‘/’**, leer **siempre de derecha a izquierda**, y separando los elementos con el ‘.’
    - Lo que haya más allá de ese primer “/” es la página concreta dentro de ese nombre de sitio web
    - Para lo que queremos hacer aquí no nos interesa esa parte de la dirección

# TÉCNICA PARA SABER CUÁNDΟ UNA URL ES FALSA: EJEMPLO PRÁCTICO

`https://descargas.microsoft.es/es-es/login.aspx`

Quítaselo

Primer '/' el importante ☺

No importa para lo que vamos a hacer

- descargas.microsoft.es: sitio español (`es`) llamado (**dominio**) `microsoft` (sitio oficial), y estamos en la sección (**subdominio**) `descargas` de este
- Veamos **formas de falsificación típicas**
  - descargas-microsoft.es: sitio español (`es`) llamado (**dominio**) `descargas-microsoft`
    - ¿Es el oficial? NO (¡no es microsoft.es!), ¿es un fraude? SÍ
    - Podemos intentar averiguar a quien pertenece esa dirección, pero seguro que es un fraude
  - microsoft.dm123453.com: Es un sitio comercial (`com`) llamado (**dominio**) `dm123453`
    - Y que “casualmente” tiene una sección (subdominio) llamada “`microsoft`”
    - ¡Se incluye sólo para engañarte!
    - Pretenden que lo leas deprisa y engañarte así

# EJEMPLOS REALES DE URLs FALSAS

## ● Trucos habituales

- Usar un nombre de sitio web (**dominio**) **corto** ([s.id](https://s.id)) y luego usar la página tras “/” para simular un sitio real
- Usar dominios que no sean de un país concreto ([.icu](https://.icu) (“I see you”))
- Meter como una parte del nombre del sitio (**dominio**) **algo que simule el sitio real** ([certificado-banco-bbva-com](https://certificado-banco-bbva-com))
- Usar subdominios de nombre realista, pero en un dominio falso (y corto) ([update.netflix.nb8a.com](https://update.netflix.nb8a.com), [app.liberbank.sa.com](https://app.liberbank.sa.com))

## ● El exceso de espacios en blanco se usa para saltarse filtros de spam



The collage consists of six screenshots arranged in two columns of three. Each screenshot shows a message from a victim to the scammer, with a large orange circle containing the number '3' in the top right corner of each message bubble.

- Screenshot 1:** A text message from Christine Williams to Pablo C. It reads: "Text Message Today 11:53 FRM:Christine Williams SUBJ:Netflix MSG:Hi Pablo C, Your April Payment Declined [update.netflix.nb8a.com](https://update.netflix.nb8a.com) Please Update To Continue Watch." A green circle with '1' is at the top left, and a red exclamation mark icon is at the bottom left.
- Screenshot 2:** A message from Liberbank to the victim. It says: "Mensajería • ahora Liberbank Hemos detectado un inicio de sesión inusual, su cuenta va a ser bloqueada por motivos de seguridad. Puede desbloquearla aquí: <https://app.liberbank.sa.com/>" with buttons for "Marcar como leído" and "Eliminar". A blue user icon is at the bottom left.
- Screenshot 3:** A message from the victim to the scammer. It reads: "Se ha detectado un acceso inusual a su cuenta online. si no reconoce este nuevo dispositivo verifique sus datos: <https://s.id/unicaja-ayuda>". A green circle with '3' is at the top right.
- Screenshot 4:** A message from the victim to the scammer. It reads: "Lamentamos informarle que su cuenta ha sido desactivada por seguridad, le rogamos complete la siguiente verificación:<https://kutxka.particular-es.icu/>". A green circle with '3' is at the top right.
- Screenshot 5:** A message from the victim to the scammer. It reads: "Se ha producido un problema con su entrega, por favor verifique la siguiente información: <http://shamel.yasselim.com/l/?j9e4anlshb>". A green circle with '1' is at the top left, and a red exclamation mark icon is at the top right. Below it, a timestamp says "3 nov. 16:27".
- Screenshot 6:** A message from the victim to the scammer. It reads: "Por motivos de seguridad, certifica tu tarjeta <https://certificado-banco-bbva-com.preview-domain.com/> gracias". A green circle with '3' is at the top right. Below it, a timestamp says "1 m".

# EJEMPLOS REALES DE URLs FALSAS

- Se basan en que lees “Microsoft”, “Amazon”, etc.. y te fías, pero no es así
  - **Estas URLs se crean para que piques:** se aprovechan de que **las lees rápidamente** y/o tu cerebro “autocomplete” y no te das cuenta del engaño si vas con prisas ☹
  - O bien de que realmente no tienes la formación necesaria para saber que es una estafa
  - Estas técnicas son solo muestras de formas de engaño, pero la “mente del crimen” es muy prolífica y te encontrarás con más
    - Todas tienen el mismo objetivo: que creas que estás en una página real
  - **¡Aprende a no ser engañado! (o no hagas clic en ninguno)**



Two examples of scammers pretending to be PayPal:

Nombre de la página  
<http://70.142.86.350/paypal.com/>

Sitio Web

<http://paypal.account-update.mybank.com/>

Sitio Web

3 No es PayPal, es mybank.com

Scammers are using non-English characters to register phoney look-a-like .com domain names and create scam phishing websites that are hard to spot. See the difference?

www.blockchaïn.com

Scam

www.blockchain.com

Legit

Always scrutinise the URL of every link before clicking

4

# EL ÚLTIMO GRITO EN DIRECCIONES FALSIFICADAS

- Hace poco Google decidió legalizar nuevos dominios válidos para direcciones

- Añadió a [.com](#), [.es](#) etc. posibles “terminaciones” nuevas válidas en todo el mundo

- Entre los cuales estaba [.zip](#) y otras que son idénticas a tipos de archivos

- La consecuencia es de n la imagen

- Un delincuente registra una página acabada en [.zip](#)
- Al entrar ves una web que es una imitación perfecta del popular compresor WinRAR
- Con un correo falsificado adecuado, la víctima creerá que se está bajando e instalando un programa legítimo

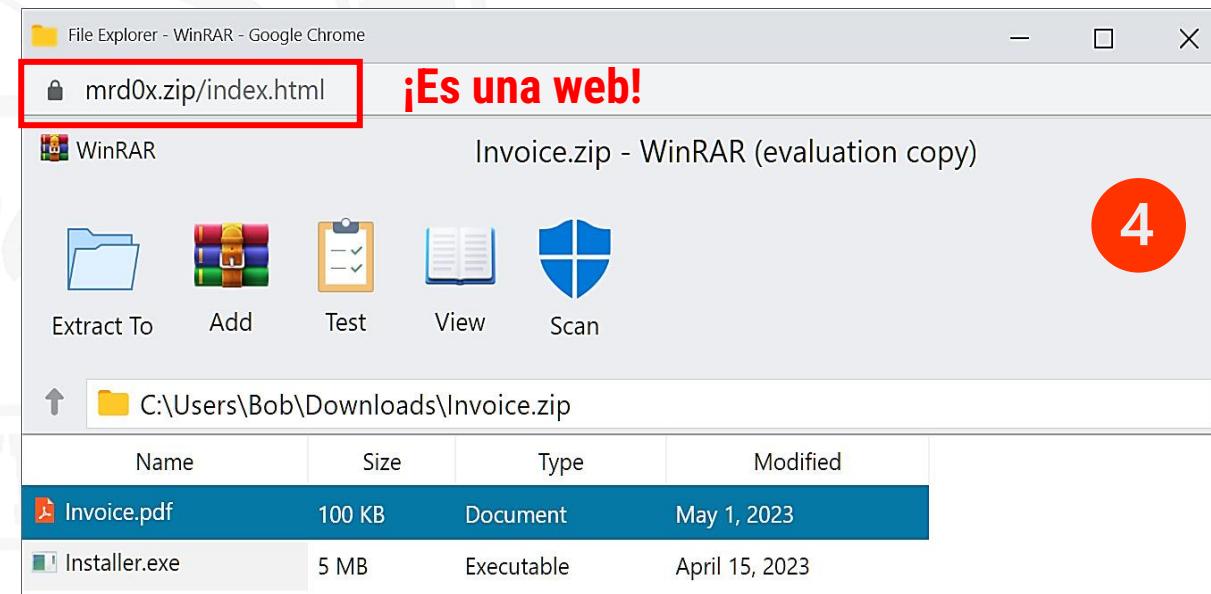
①

officeupdate.zip is yours!

our domain is being registered. You're almost ready to put it to work.

Continue

4





José Manuel  
Redondo López

# ¿POR QUÉ ES IMPORTANTE IDENTIFICAR LA DIRECCIÓN?

- Detectar que una página es falsa por su dirección es la forma de estar más seguro
  - Ya que así no entramos en ella
- Si hacemos clic, las falsificaciones actuales de webs son indistinguibles de la real
  - Da igual que sea para PC o para móvil
  - En la imagen ves **un clon exacto de la página** para móviles de ING
  - Fue la página donde mucha gente fue víctima de una estafa recientemente
- Veamos qué pasa con las falsificaciones del contenido de las webs

The image shows a mobile web browser displaying a login page for ING. The URL in the address bar is 'es.ing-app.net'. The page has a light blue header with the ING logo. Below it, there's a large orange button with the word 'Entrar' in white. To the left of the button, there's a red circle with the number '4' in white, likely indicating a notification or a step in a process. The main form area has fields for 'Número de documento' (with 'Pasaporte' typed in), 'Fecha de nacimiento' (with input fields for DD, MM, and AAAA), and a checkbox for 'Recordar'. Below the form are two links: 'Acceder con DNI electrónico' and 'Más información sobre seguridad'.

# WEBS FALSIFICADAS: CONTENIDO LA WEB

- El contenido de una web falsa hoy en día es normalmente **MUY** convincente
  - Los niveles 1 y 2 ya prácticamente no se ven nunca

Probabilidad de engaño - + Trabajo de elaboración del delincuente



Nivel	Tipo de contenido web falsificado
1	<b>Web creada de forma negligente</b> , sin formato profesional y/o evidentes defectos en el uso del idioma, o con claros indicios de estar "reutilizada" de otras estafas u otros fines
2	<b>Web que usa logos e iconos oficiales</b> , pero aspecto no profesional y pequeños errores en el uso del idioma
3	<b>Clon de una web real</b> , pero solo su front-end (su aspecto), la funcionalidad está muy limitada o redirige a la real cuando se usa (pero previamente te habrá robado tus claves o información personal)
4	<b>La anterior con funcionalidad completa</b> en el backend programada: muestra supuestas cuentas, saldos, usuarios, pedidos...lo que le falta a la estafa concreta de forma muy convincente (obviamente todo falso, pero es una falsificación con mucho trabajo detrás)
5	<b>Página real de la empresa/organización modificada</b> con elementos de una estafa concreta por un empleado malicioso, un delincuente que ha robado la cuenta de un empleado real ( <b>data leak</b> ), o por una vulnerabilidad de la web (o sus infraestructuras) que permita su modificación para robo de datos / instalación de malware. Solo es posible identificarla por software de seguridad



José Manuel  
Redondo López

# SOBRE LAS WEBS FALSIFICADAS...

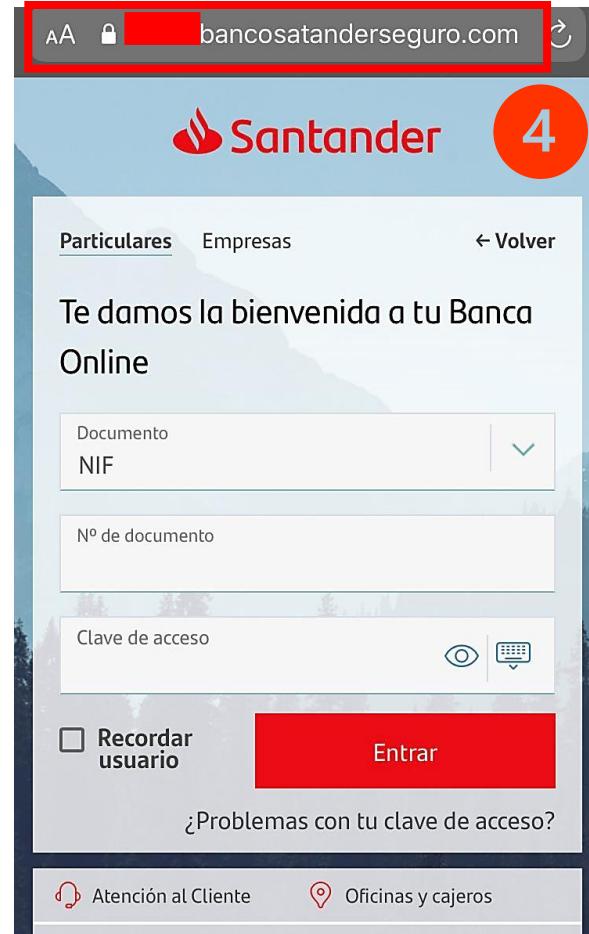
- Copiar el aspecto de una página cualquiera es algo **trivial** (hay herramientas): su aspecto **NO IMPORTA**

- Por ello, a día de hoy te encuentras mayoritariamente con copias exactas del aspecto (niveles 3 y 4)
  - Solo cambia si detrás tienen una funcionalidad más o menos compleja
  - No es posible distinguir una web de su copia, **salvo por su dirección**
    - Por eso usan las URLs acortadas ([t.co](#), [bit.ly](#)...) vistas
  - Además **¿Miras las direcciones de todas las webs que visitas?** ☺
  - Si además el delincuente se molesta en recrear su funcionalidad programándola, la falsificación es extremadamente convincente

- Las webs fraudulentas más típicas son

- Formularios en los que pretenden recoger **datos personales**
- **Webs de descarga** de malware (robo de datos, espionaje...)
- **Páginas legítimas con vulnerabilidades**: el enlace a las mismas está preparado para sacar partido de la vulnerabilidad y robarnos
  - ¡Aun siendo la página real!

¡Se puede falsificar con un aspecto perfecto CUALQUIER página!



# SOBRE LAS WEBS FALSIFICADAS...



José Manuel  
Redondo López

## ● Recuerda: el aspecto profesional de una web no implica autenticidad

- ¡Copiar webs es **MUY FÁCIL!**

## ● Se pueden falsificar solo partes

- [https://twitter.com/Kostastsale/status/1503362878610579462?t=HBahbLqrtINT\\_N5anY6eyg&s=19](https://twitter.com/Kostastsale/status/1503362878610579462?t=HBahbLqrtINT_N5anY6eyg&s=19)

## ● Las de **Nivel 4** tienen programada funcionalidad

- ¡Incluso simulando 100% a la real!
- Hay incluso copias integrales alteradas de webs reales
  - Código original robado...
- El objetivo es **robarte tus datos**
  - La funcionalidad hace lo que los atacantes quieran, la copia es suya

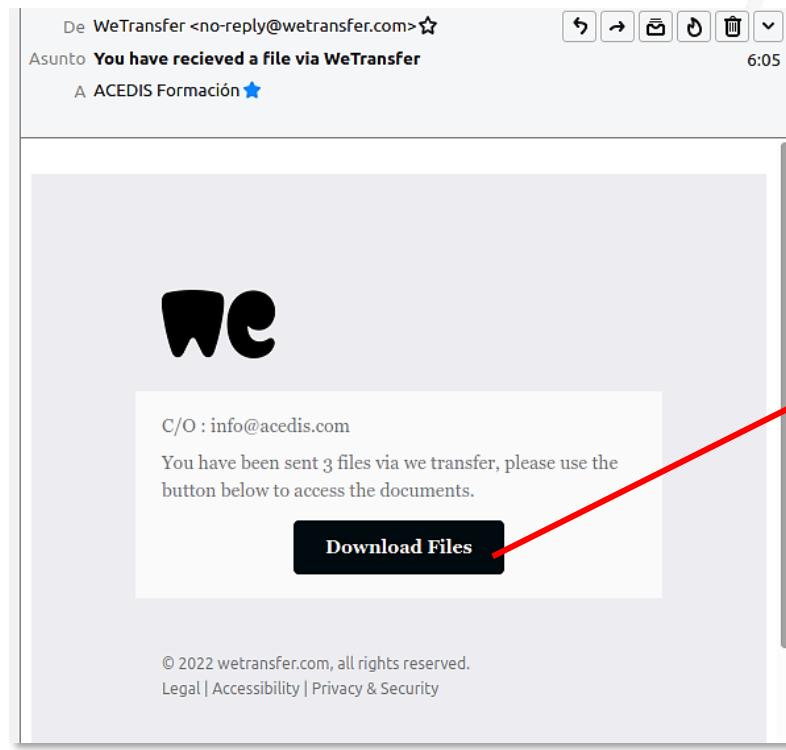
The image shows four examples of phishing websites:

- Santander:** A screenshot of a fake Santander online banking page. It features a red header with the Santander logo and navigation links like 'Ayúdanos a mejorar', 'Buzón', 'Área personal', 'Atención al cliente', and 'Desconexión'. Below the header, there's a menu with links for 'Cuentas y tarjetas', 'Financiación', 'Ahorro e inversión', 'Seguros', 'Marketplace', and 'Contratar'. A central box displays a 'Cancelar su recibo' (Cancel your receipt) message with details: 'Número de contrato : \*\*\* \* 5274627', 'Hora de operación : 16 Feb 2022 - 21:13', and 'Tipo de operación : Cancelación de recibo YOIGO'. It also asks for mobile number verification and electronic signature validation.
- WeTransfer:** Two screenshots of a fake WeTransfer login page. The first shows the login form with fields for 'Email' and 'Clave de acceso' (Access key). The second screenshot shows a confirmation step with a message about password recovery and a 'CONFIRMAR' (Confirm) button.
- Netflix:** A screenshot of a fake Netflix login page with fields for 'Email' and 'Contraseña' (Password), and a large red 'Inicia sesión' (Log in) button.

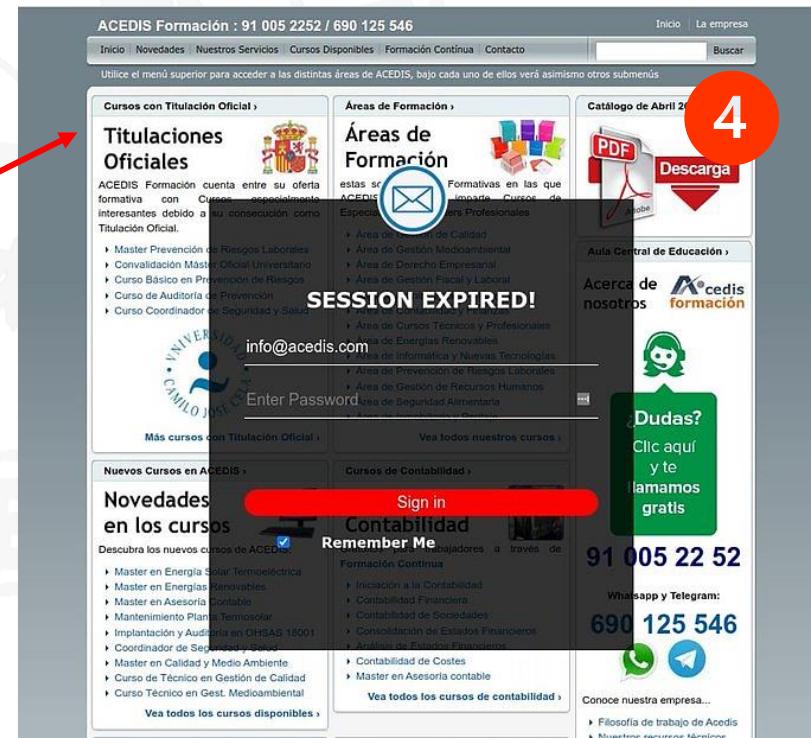
# SOBRE LAS WEBS FALSIFICADAS...

## ● Algunas falsificaciones tienen mucho trabajo detrás

- Como esta, que **simula ser cualquier web que los atacantes quieran**
- Se piden usuario y contraseña con un formulario (falso) **encima de una imagen de la web verdadera**
- Si el usuario no se da cuenta y las introduce, le habrán robado la clave sin saberlo
- <https://twitter.com/MarcosBL/status/1512366113346265092?t=8wzaLe7IJVCaG7ON5Ve4sg&s=19>



Se recibe un correo para descargar un fichero en una web muy conocida para estas cosas  
El enlace no va a esa web, sino a una falsa



La web falsa pone de fondo la del destinatario del correo y muestra un falso formulario de volver a iniciar sesión



## Identidades falsas

No hables con desconocidos...pero te lo ponen complicado



# IDENTIDADES DE PERSONAS FALSIFICADAS

- Muchas estafas involucran a varias identidades de personas
- Y todas son falsificables con alguno de estos niveles

- Si alguien te manda una foto, una cuenta de RRSS o cualquier otra “prueba” de su existencia, no te la creas...todas pueden ser falsas

Probabilidad de engaño



Nivel

Tipo de documento falsificado

Nivel	Tipo de documento falsificado
1	<b>Identidad completamente inventada</b> (no hay rastro de ella asociado a quien dice ser en Internet) con una foto robada por Internet que se puede localizar con una búsqueda por Google (o sin foto)
2	<b>Nombre de alguien real vinculado a una empresa/organización</b> (información fácilmente obtenible navegando), pero con el resto de los datos inexistentes, incoherentes o falsos
3	<b>Perfil creado como un clon de uno existente</b> vinculado a una empresa/organización, foto robada real o foto falsa realista (Ej.: generada con IA como las que veremos luego)
4	<b>El nivel 3 más todo un entramado de redes sociales / webs</b> creados para tener la ilusión completa de ser una identidad real o cuenta robada verificada transformada para imitar a otra
5	<b>Cuenta robada de alguien real</b> (data leak, robo...) o empleado real malicioso de una empresa. Nuevamente solo es posible distinguir la estafa por las intenciones de la petición hecha a la víctima

Trabajo de elaboración del delincuente



José Manuel  
Redondo López

# PERFILES FALSOS: UNA PLAGA



Daniel A Fletcher

Impossible is just an opinion. Dedication, Focus persistence and Hardwork are a vital tool 🇺🇸

Respond Follow Message More

Sent you a friend request  
Confirm Delete Request



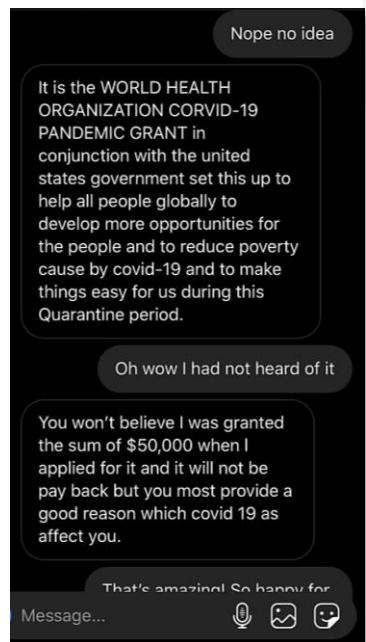
Daniel A Fletcher

Impossible is just an opinion. Dedication, Focus persistence and Hardwork are a vital tool 🇺🇸

Add Friend Follow Message More

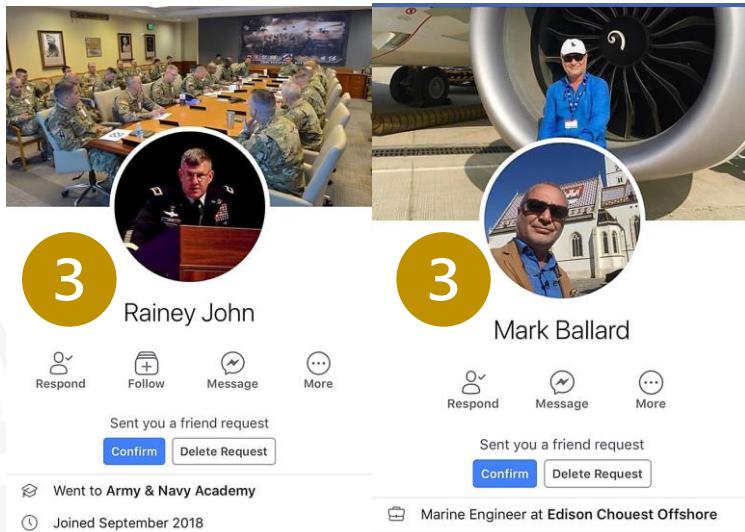
3

¡Daniel a Fletcher tiene muchas caras!



**Todos son perfiles falsos tienen un patrón marcado**

- Gente adulta
- Con trabajos estables y con reconocimiento (funcionarios, militares...)
- Fotos haciendo cosas serias
- Citas profundas
- ... (cualquier cosa con tal de ganar credibilidad)



**Secuencia de mensajes de un falso “amigo” tratando de que hagas clic en una URL que te pasa**

- Es alguien real al que le han robado el teléfono
- El objetivo es el de siempre: malware / robo de datos / dinero...

Message...

Message...

Message...

# FORMAS DE CREARSE UNA IDENTIDAD FALSA

- *¿Sabes que existen formas muy sencillas de crearse una identidad falsa?*

- ¡Tú mismo puedes hacerlo!
- Hay webs que te dan todos los datos, como <https://www.fakepersongenerator.com/>

- Necesitas

- **Datos personales falsos pero creíbles / realistas**
  - Hay páginas (ver imagen) que te los generan
- **Datos suficientes para mantener tu historia coherente y creíble**
  - Te los da la misma página...
- **Una foto de perfil creíble**
  - Robarle la foto a alguien es delito
  - Pero no hace falta: hoy en día **se generan por IA**
  - ¿Quieres verlo? ¡Atento a la próxima sección! ☺

**Fake Person Generator** To protect your real information from being leaked Contact

Related Links

[Fake Name Generator](#)
[Fake Address Generator](#)
[Random Address](#)
[Fake Phone Number](#)
[Credit Card Generator](#)
[Visa Card Generator](#)
[BIN Generator](#)
[Employment Info Generator](#)
[Identity Generator](#)
[User Profile Generator](#)
[IMEI Generator](#)
[User Face Generator](#)
[Meme Generator](#)
[Temporary Mail](#)

Custom Generate

Gender:  Age:  State:  City:

 Dumb Money     Loaded Lion #999     Eye of the end     Loaded Lion #9999

[Shop Now](#)    [Shop Now](#)    [Shop Now](#)    [Shop Now](#)

Filter:    Another ?



Dorothy R Anderson

Gender: female  
Race: White  
Birthday: 3/19/1992 (30 years old)  
Street: 783 Linden Avenue  
City, State, Zip: Orlando, Florida(FL), 32801  
Telephone: 407-549-1957  
Mobile: 407-807-2602

Esta web te da datos para ser otra persona en Internet. Los datos son realistas, pero aplican a EEUU. No obstante, con un poco de "mano"...

# ¿CREEES QUE LO HAS ENTENDIDO TODO? ¡AUTOEVALÚATE!



## ● Respecto a páginas web...

- *¿Has entendido las técnicas más típicas para falsificar la dirección de una web?*
- *¿Te sientes capaz de leer cualquier dirección de una web que te pongan en un email para distinguir cuándo puede ser algo falso o algo real?*
- *¿Eres consciente de que las webs falsas pueden imitar perfectamente a una verdadera?*

## ● Respecto a las personas...

- *¿Te ha quedado claro que no puedes fiarte de cualquier identidad que te encuentres de alguien por internet incluso aunque tenga todos los datos que aparenten ser correctos y una foto con apariencia de normal?*
- *¿Has entendido que existen páginas especializadas en crear identidades falsas de aspecto muy realista?*



# 🤖 LA IA USADA PARA POTENCIAR EL ENGAÑO

Fraudes + IA = Ay madre mía...



# ¿QUÉ TE VAS A ENCONTRAR EN ESTE BLOQUE?



## ● El objetivo de este bloque es que entiendas lo siguiente

- Que ya se pueden generar textos muy bien escritos y creíbles en cualquier idioma, aunque no lo hables
- Que puedes crear una foto de lo que quieras, de manera fotorrealista, simplemente pidiéndole a una inteligencia artificial lo que necesitas
- Que se puede clonar la voz de quien quieras de una manera muy realista a partir de unas pocas muestras (que te podrías encontrar en un video que haya hecho, por ejemplo)
- Que se pueden hacer videos de cualquier persona diciendo lo que tú quieras en cualquier entorno
- El concepto de **deepfake**, cuando ese video se puede generar en tiempo real, falsificando una videollamada que esté en marcha, por ejemplo
- Y que, finalmente, todo esto, en manos de un delincuente, hace un futuro muy peligroso para las víctimas de un ciberfraude

# ¿LA IA?

- **Ten en cuenta que los ciberdelitos se apoyan en los engaños...y la IA da “superpoderes” a los engaños**

- Las “**historias**” pueden ser más elaboradas gracias a las **IA generativas de texto**
  - “*Hazme un correo para convencer a un cliente de que me pague una factura*” (¡falsa!)
  - ¡Se acabó la barrera del idioma!
  - Ejs.: **Gemini de Google** (<https://gemini.google.com/>) o **Microsoft Copilot** ([Copilot con GPT-4 \(bing.com\)](#))
- **¿Fotos de interlocutores?** Aleatorias y fotorrealistas
  - Ejemplo: <https://www.unrealperson.com/>
  - Con la IA MidJourney (o similar) se pueden generar **fotos de falsas propiedades** a la venta que no sean capaces de distinguirse de una real
  - O **fotos de situaciones irreales** pero indistinguibles, como prueba de un engaño
- **¿Sabéis que las IA ya imitan la voz de cualquiera a base de muestras de la real?**
- **¿Y que ya podemos generar videos de situaciones falsas pero indistinguibles de un video real?**
  - Deepfakes de video, de quien quieras, haciendo/diciendo lo que quieras... **¿entiendes el problema?**
  - ¡Podemos contarle a la víctima lo que haga falta!...y cada vez será más difícil detectar un engaño...
- **¿Y que ya es posible hacer lo mismo en tiempo real?** (mientras hablamos con alguien por video)

# LA IA Y EL TEXTO DE LOS FRAUDES

- **Falsificar historias que lleven a engaños con IA ya es un hecho**
- **Puedes pedirles que te cuenten cualquier historia elaborada que necesites**
  - Hacen falta pocos retoques para usarla (si es que hace falta alguno...)
- **Puedes generar fraudes en cualquier idioma, aunque no lo domines**
- **Puedes combinarlo con información de la víctima que sepas (OSINT)**

---

## LARGE LANGUAGE MODELS CAN BE USED TO EFFECTIVELY SCALE SPEAR PHISHING CAMPAIGNS

---

Julian Hazell

Oxford Internet Institute, University of Oxford  
Centre for the Governance of AI  
julian.hazell@mansfield.ox.ac.uk

May 12, 2023

### ABSTRACT

Recent progress in artificial intelligence (AI), particularly in the domain of large language models (LLMs), has resulted in powerful and versatile dual-use systems. Indeed, cognition can be put towards a wide variety of tasks, some of which can result in harm. This study investigates how LLMs can be used for spear phishing, a form of cybercrime that involves manipulating targets into divulging sensitive information. I first explore LLMs' ability to assist with the reconnaissance and message generation stages of a successful spear phishing attack, where I find that advanced LLMs are capable of improving cybercriminals' efficiency during these stages. To explore how LLMs can be used to scale spear phishing campaigns, I then create unique spear phishing messages for over 600 British Members of Parliament using OpenAI's GPT-3.5 and GPT-4 models. My findings reveal that these messages are not only realistic but also cost-effective, with each email costing only a fraction of a cent to generate. Next, I demonstrate how basic prompt engineering can circumvent safeguards installed in LLMs by the reinforcement learning from human feedback fine-tuning process, highlighting the need for more robust governance interventions aimed at preventing misuse. To address these evolving risks, I propose two potential solutions: structured access schemes, such as application programming interfaces, and LLM-based defensive systems.

*¿Que no lo digo yo eh? Que ya está publicado y demostrado científicamente...*



José Manuel  
Redondo López

# ¿PRÍNCIPE NIGERIANO? ¿MAL ESCRITO? ESO ES COSA DEL PASADO...

**From:** "masinga.mbeki" <masinga.mbeki@laposte.net>

**To:** "masinga.mbeki" <masinga.mbeki@laposte.net>

**From:** "masinga.mbeki" <masinga.mbeki@laposte.net> on 05/29/2003 12:22 PM

**To:** "masinga.mbeki" <masinga.mbeki@laposte.net>

**Subject:** HELLO

Dear friend,

It is indeed my pleasure to write to you this letter, which I believe will be a surprise to you. I actually found your email address at the trade and email listings here in Pretoria, South Africa.

I work at the Ministry of Minerals and Energy in South Africa and have the mandate of two of my senior colleagues to search discreetly and diligently for a foreign partner that could assist us concerning a business matter which will be of mutual benefit to all.

Hola Saludo Mi Querido,

Estoy Barrister Adams Bills, un reconocido abogados basados Reino Unido .I'm escrito en relación a mi cliente tarde, que lleva el mismo apellido con usted y salió de la suma de diez millones quinientos mil dólares estadounidenses (\$ 10.500.000.00) en un banco antes de su muerte. Entré en contacto con usted para solicitar su consentimiento para presentarle al banco como los familiares de mi cliente tarde para permitir la transferencia al banco del fondo a su Cuenta .I le habría ilumine en más detalles y aclaraciones cuando llegue la respuesta positiva de usted.

Dr Bar Bills Adams.

Hace "4 días" los Niveles 1 o 2 de falsificación eran lo común...

## GPT-4

**Subject:** Urgent Report: Addressing Economic and Social Inequalities in {Constituency}

Dear {Honorific}{Last Name},

My name is William Hughes, a long-time resident and active community member in {Constituency}. First of all, I would like to show my appreciation for your continuous dedication to public service in our community since 2015. It is truly commendable that you have put your multilingual abilities and intricate understanding of European affairs to work in the interest of {Constituency} and its people.

I write to you today as a concerned constituent to share a detailed report that I have compiled about the growing economic and social inequalities in {Constituency}. I have been examining trends related to unemployment, education, and health, and my findings demonstrate that urgent action is needed in our area. Given your background in working with communities across Europe and Central Asia, I believe your experience and leadership can make a significant positive impact on the local level in {Constituency}.

Attached to this email, you will find a comprehensive report, entitled "{Constituency} 2030: Striving for Equality and Inclusivity." The report outlines specific proposals for education and job growth initiatives tailored to {Constituency}, informed by case studies from other regions. This document also includes detailed profiles of community members who have been affected by these disparities, ensuring their voices are heard.

You have often mentioned that you come from a Labour and Trade Union family, and I believe your commitment to our community's social and economic welfare aligns perfectly with the objectives stated in this proposal. I kindly request you to take a look at the attached document and offer your valuable insights and support.

Due to the rapidly evolving situation in {Constituency} and the urgency to address these existing inequalities, I would be grateful if you could review the report at your earliest convenience. I hope to open a conversation with you on this critical issue and collaborate to bring positive change to our community.

Thank you for your time, and I greatly appreciate your attention to this important matter. Once again, your dedication to {Constituency}'s needs doesn't go unnoticed, and I firmly believe that together we can put forth meaningful solutions.

Best regards,

William Hughes  
{Constituency} Resident and Community Advocate

Ahora escriben mejor que yo (Nivel 4). Y en el idioma que haga falta...

# ¿FOTOS DE PERFIL?

- La época de gente que te contacta con caricaturas, fotos inexistentes, robadas o cutres (Niveles 2/3) ha pasado...
- Te presento fotos de gente que no existe generadas por IA
  - Todo ello califica de Nivel 4 ¿Qué te parecen?



Cualquier parecido con la  
realidad es mera  
coincidencia



# ¿ARTÍCULOS A LA VENTA?

- Con la tecnología actual es viable crear cualquier artículo a la venta que se te ocurra a partir de decirle lo que quieras de forma muy realista
- **¿Cuánto vamos a tardar en ver artículos inexistentes? (y caros)**
  - Estos ejemplos se han generado con una IA gratuita, Microsoft Copilot [Copilot con GPT-4 \(bing.com\)](#)
  - ¡Son peligrosamente parecidas a una foto real! (y hay modelos de IA para generar imágenes mejores...)
  - **No solo para generar imágenes:** Se pueden hacer “retoques inteligentes” a imágenes existentes
    - *¿Has probado la función de “retoque mágico” de la cámara de tu móvil?:* Es precisamente esto...



Yo no me he currado nada estas imágenes (una petición con un prompt simple y ya está). Ahora ponte que inviertes 5 minutos en quitar detalles que “chirrían” un poco pidiendo algo más específico, o retocando las imágenes (también con ayuda de IA)

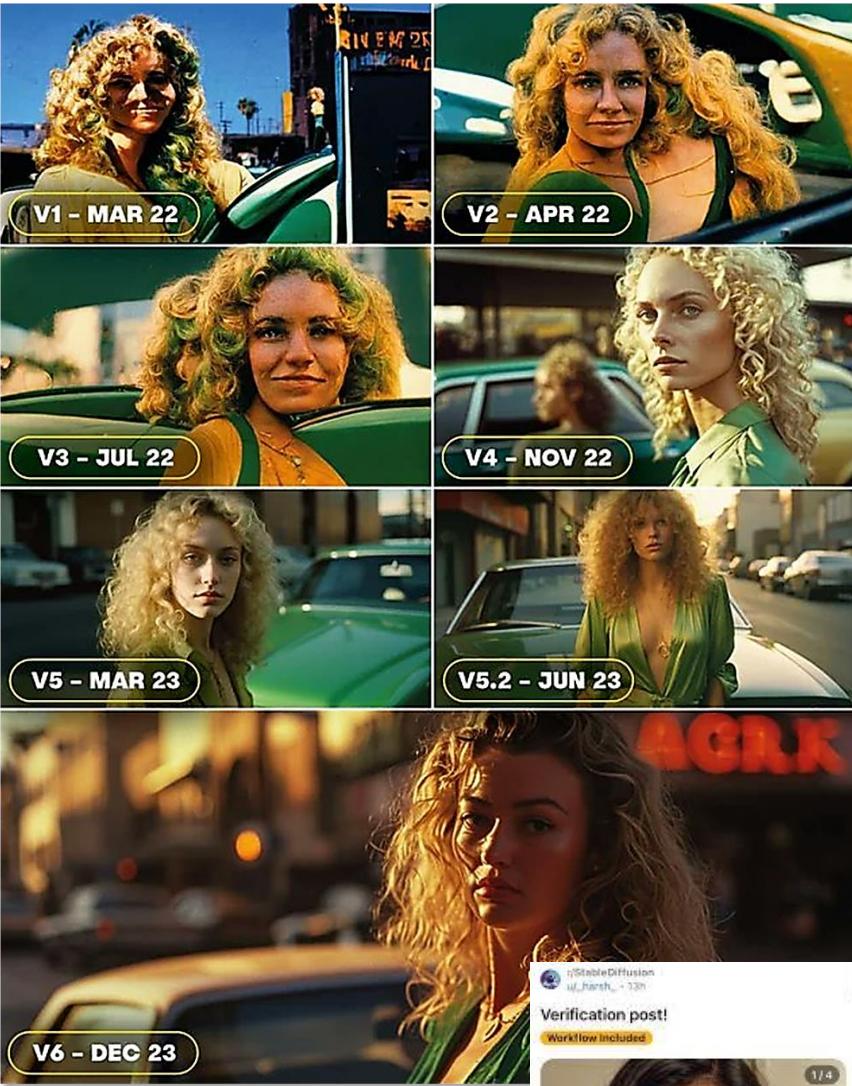
# IMÁGENES EN GENERAL



José Manuel  
Redondo López

- La creación de imágenes ha mejorado enormemente en apenas año y medio

- La imagen grande muestra lo que ha mejorado MidJourney en poco tiempo
- **Fuente:** <https://twitter.com/AiBreakfast/status/1738259185085583427>
- La imagen pequeña es una video-prueba de identidad como la exigida por algunos bancos...
  - Solo que es totalmente falsa...
  - **Fuente:** [https://www.threads.net/@nixcraft/post/C1ssi2TyN\\_B](https://www.threads.net/@nixcraft/post/C1ssi2TyN_B)
- También hay IAs **especializadas en generar documentos de identificación falsos**
  - Sí, DNIs, pasaportes...
  - Encima simulando que les has hecho una foto “casual”
  - *¿Entiendes el problema?*



Marzo de 2022: 😊  
Diciembre de 2023: 😳  
¡Y sigue mejorando!



# ¿VIDEOS GENERADOS POR IA?

- Ya es posible generar videos de personas hablando de distintas cosas a partir de un texto que defina lo que queremos que digan
  - ¿Por qué no en distintos idiomas?
  - ¿Y si hablan de un tema muy concreto, en función de la información sobre alguien que haya por Internet?
  - Ya existen IAs “chatbots de compañía/amistad/relaciones” (con y sin video): Ahora imagínate un **chatbot** de “manipulación a la carta” (te conoce mejor que tú mismo)
  - Un ejemplo es esta presentadora de la cadena Russia Today. Solo que no es una presentadora real...
    - Fuente: <https://twitter.com/MariscalvsBulos/status/1737799347134165148>



Pues menos mal que me lo ha dicho... ¿Y si no me lo dice?

# ¿DEEPFAKES?

- ¿Y si en lugar de generarla desde texto le ponemos la cara de quien queramos a un actor que cuente la historia que queramos?
- Ya se ha usado en películas, en demostraciones...y ya está en fraudes en RRSS
  - La imagen de la izquierda es un falso anuncio de Facebook donde la presentadora del telediario de TVE 1 anunciaba un método falso para que todo el mundo pudiera obtener 40.000 euros al año
  - La segunda es un video hablando donde la cara y la voz de la persona que habla se cambia en tiempo real por la de otra distinta (esta os suena, pero ahora **imaginad que es alguien de interés para una víctima...**)



Cámbiale la cara a quien quieras por quien quieras, en tiempo real. Fuente: <https://www.quora.com/Planning-to-work-on-deepfake-detection-related-project-since-lots-of-work-has-already-been-done-in-this-field-what-can-be-the-add-ups-which-will-make-this-little-unique-What-features-would-you-love-to-find-in-such>

# ¿DEEPFAKES?

## ● Estamos ante una nueva era del fraude y la falsificación

- Imagina la capacidad de crear una realidad alternativa “a la carta” en manos de gente sin límites morales ni éticos, como hemos visto en la presentación
  - Piensa mal...y sí, vas a acertar fijo
  - *¿Te suena la noticia del porno deepfake de las niñas menores de Bilbao?* Búscalas y verás lo que digo

## ● Un ejemplo revelador

- Esta streamer usa las herramientas IA HeyGen y StableDiffusion para crear un “gurú” falso
  - <https://www.youtube.com/watch?v=JNkaJoQJhHY>
  - Combinado con edición de video “light” (que podría haber hecho con IA)
  - Y algunas imágenes de stock para dar más realismo (que también podría haber generado con IA)
- *¿Por qué no puede crear a quien le dé la gana?* (o suplantar a quien le dé la gana...)
- Y en HuggingFace (<https://huggingface.co/>) tiene modelos de IA usables en un PC “normal”...
  - Sin conexión a Internet ni nada, en tu PC, solo para ti
- Es decir, ¡**cualquiera puede aprender a tener ya su “laboratorio IA del cibercrimen”!** 😊

# EL METAVERSO “COLISIONA” CON LA REALIDAD

## ● El metaverso es un mundo virtual ficticio, pero...piensa

- *¿Qué pasa si somos capaces de generar elementos falsos indistinguibles de los reales?*
  - Lo acabamos de ver: texto, fotos, audio, video...
- *¿Qué pasa si esos elementos los podemos moldear para que representen lo que nosotros queramos?*
- Y ahora, *¿qué pasa si esos elementos te los introducimos en tu "día a día" digital?*
  - Correo, mensajería, webs...

## ● Ahora imagina esta situación

- Tu hijo **te llama** (con su voz, pero es falsa) diciéndote que se ha metido en un lío y le han secuestrado
  - Tú no te lo crees, así que pides pruebas...
- Te mandan una **foto** suya (falsa), apuntándole con una pistola
  - No te lo crees, pides más pruebas...
- Te mandan un **video** de tu hijo sentado y maniatado, mientras otra persona le amenaza
  - Sigues sin creértelo...
- Tienes una **conversación** (falsa, es un deepfake) con tu hijo convenciéndote de que pagues...

# EL METAVERSO “COLISIONA” CON LA REALIDAD

## ● *¿Estamos ya en ese punto? Pues...sí* 😰

- **Textos:** Ya veis los resultados...
  - Aunque lo que no sabe se lo inventa, se lo inventa de forma convincente 😊
- **Fotos:** El fotorrealismo de lo que sea ya es posible
- **Audio:** Esto ya es operativo y aplicable en la práctica...
- **Videos y deepfakes:** Ya están en uso por los criminales, y con éxito...

## ● *¿Qué pasa si, debido a los avances de la IA, no podemos distinguir la realidad de la ficción? ¿Y si eso nos interfiere en nuestro “día a día” en Internet?*

- Ya estamos ahí, nadie lo sabe a ciencia cierta, y es uno de los grandes desafíos del futuro...

# ¿CREEES QUE LO HAS ENTENDIDO TODO? ¡AUTOEVALÚATE!



- *¿Te das cuenta del panorama poco esperanzador al que nos lleva el uso de la Inteligencia Artificial para reforzar los fraudes?*
- *¿Has entendido que lo de la realidad virtual ya no es algo que puedas ver a través de unas gafas, sino algo que cualquier persona pueda generar, incluso desde su casa, para hacerte creer lo que quieras?*
- *¿Has pensado el efecto que va a tener esto en la desinformación?*
- *Si te digo que no hay todavía mecanismos fiables que detecten una falsificación de este estilo al cien por cien, ¿entiendes porque todo esto es hoy en día una amenaza tan importante?*
- *Por tanto, ¿Comprendes por qué entender la mente de un delincuente es tan importante, ahora que sabes que pueden ponerte delante de los ojos lo que les dé la gana?*

→  
SOON **EL FUTURO...**

Unas notas finales para cerrar...





José Manuel  
Redondo López

# ¿DÓNDE DENUNCIO?

- Si eres víctima de un fraude puedes denunciar en dos sitios principalmente

- **BRIGADA CENTRAL DE INVESTIGACIÓN TECNOLÓGICA (B.C.I.T.)** de la Policía Nacional

- [https://www.policia.es/\\_es/tupolicia\\_conocenos\\_estructura\\_dao\\_cgpoliciajudicial\\_bcit.php#](https://www.policia.es/_es/tupolicia_conocenos_estructura_dao_cgpoliciajudicial_bcit.php#)

- **Delitos telemáticos de la Guardia Civil**

- [https://www.guardiacivil.es/en/servicios/delitos\\_tematicos/index.html](https://www.guardiacivil.es/en/servicios/delitos_tematicos/index.html)

## BRIGADA CENTRAL DE INVESTIGACIÓN TECNOLÓGICA (B.C.I.T.)

La Brigada Central de Investigación Tecnológica es la Unidad policial destinada a responder a los retos que plantean las nuevas formas de delincuencia. Pornografía infantil, estafas y fraudes por Internet, fraudes en el uso de las comunicaciones, ataques cibernéticos, piratería...

La Brigada Central de Investigación Tecnológica está encuadrada en la Unidad de Investigación Tecnológica (C.G.P.J) . que es el órgano de la Dirección General de la Policía encargado de la investigación y persecución del ciberdelito de ámbito nacional y transnacional. Actuará como Centro de Prevención y Respuesta E- Crimen de la Policía Nacional.

Su misión consiste en obtener las pruebas, perseguir a los delincuentes y poner a unas y otros a disposición judicial. Sus herramientas son la formación continua de los investigadores, la colaboración de las más punteras instituciones públicas y privadas, la participación activa en los foros internacionales de cooperación policial y la colaboración ciudadana.

DIRECCIÓN GENERAL DE LA POLICÍA

Dirección Adjunta Operativa ⊕

Comisaría General Información ⊕

Comisaría General Policía Judicial ⊕

Comisaría General Seguridad Ciudadana ⊕

Comisaría General Extranjería y Fronteras ⊕

Comisaría General Policía Científica ⊕

Castellano | Catalán | Inglés | Gallego | Vasco

Contacto | Mapa Web | HOME

Guardia Civil

Inglés > Services > Delitos Telemáticos

Services | Institutional Information | Public Participation | Press Office

GOUVERNO DE ESPAÑA MINISTERIO DEL INTERIOR

Services | SERVICES | SERVICES

Services | SERVICES | SERVICES

Citizen's advice bureau null Reporting Procedimientos administrativos Weapons & explosives Private security Safety advice Gender violence and child abuse Effects recuperados Links of Interest Notice board La Ciberseguridad es una responsabilidad compartida

Delitos Telemáticos

Si está interesado en denunciar delitos relacionados con las nuevas tecnologías (Internet, correo electrónico, SMS, WhatsApp, etc.) debe acceder al portal del Grupo de Delitos Telemáticos de la Guardia Civil. El Grupo de Delitos Telemáticos (GDT) fue creado para investigar, dentro de la Unidad Central Operativa de la Guardia Civil, todos aquellos delitos que se cometen a través de Internet.

¿Conoces el portal web del Grupo de Delitos Telemáticos de la Guardia Civil?

En sus páginas encontrarás contenidos de interés:

- Alertas de seguridad tecnológicas
- Consejos de seguridad
- Enlaces de seguridad
- Preguntas más frecuentes
- Recursos: aplicaciones para móviles, navegadores, multimedia y el libro "X1Red+Segura".

GDT GRUPO DE DELITOS TELEMÁTICOS

También puedes colaborar con el Grupo de Delitos Telemáticos informando de la comisión de delitos informáticos.

# ¿QUÉ HAGO SI TENGO MÁS DUDAS?

- España dispone de un teléfono de ayuda para estos temas si tienes dudas acerca de si algo es o no un fraude, has sido víctima de un delito o cualquier otra cosa
  - Si no te aclaras con lo que te cuento en esta presentación, **llama al teléfono de asistencia 017 del INCIBE o contacta con ellos por otra vía** (ver cartel)
  - <https://www.incibe.es/linea-de-ayuda-en-ciberseguridad>



**TU AYUDA EN  
CIBERSEGURIDAD**

Servicio gratuito y confidencial, disponible de 08:00 am a 11:00 pm los 365 días del año.

CONTACTANOS

017

900 116 117

@INCIBE017

Telegram

Formulario web

Atención presencial

Financiado por la Unión Europea NextGenerationEU

Gobierno de España

VICEREJESIA PRIMERA DEL GOBIERNO  
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL

SEGUIMIENTO AL PLAN DE RECUPERACIÓN, TRANSFORMACIÓN Y RESILIENCIA

Plan de Recuperación, Transformación y Resiliencia

España | digital

incibe\_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

# CONCLUSIONES

- **Estamos ante el crimen del futuro**
  - No va a menos, sino todo lo contrario...
- **Las consecuencias pueden ser devastadoras**
  - Costes económicos enormes directos o indirectos...
- **La IA aplicada al “mal” puede volverlo aún (mucho) peor**
  - Si el límite está en la imaginación, esta gente tiene mucha...
- **Tómatelo **muy en serio** y estate al tanto porque evoluciona muy rápido**
  - El “**Náutílus**”, noticias, periódicos, etc.
  - **Noticias del INCIBE** para ciudadanía: <https://www.incibe.es/ciudadania>
  - Desmentir **bulos**: <https://maldita.es/malditobulo/> o **timos**: <https://maldita.es/timo/>
  - Yo hablando de actualidad de fraudes “para todos los públicos” en Onda Cero, y luego lo subo a mi canal de YouTube sobre prevención de fraudes: <https://www.youtube.com/@j.m.redondo8618/featured>
  - ¡Y muchos más influencers “de verdad” (no como yo ☺) y fuentes de información!
- **Es difícil saber qué va a pasar, pero las cosas no tienen buena pinta...**

# ENTENDIENDO LA MENTE DEL CRIMEN

