



Financiado por
la Unión Europea
NextGenerationEU



Gobierno
de España

MINISTERIO
PARA LA TRANSFORMACIÓN DIGITAL
Y DE LA FUNCIÓN PÚBLICA

SECRETARÍA DE ESTADO
DE DIGITALIZACIÓN
E INTELIGENCIA ARTIFICIAL



Plan de
Recuperación,
Transformación
y Resiliencia

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD



Universidad de Oviedo

SIENDO UN HACKING BESTIA CONOCE TÉCNICAS DE ATAQUE



Campus Tecnológico-Deportivo para
Jóvenes

Universidad de Oviedo



JOSÉ MANUEL REDONDO LÓPEZ PROYECTO "F-74 'ASTURIAS'" v1.2





ACERCA DEL USO DE CONTENIDO GENERADO POR IA



José Manuel
Redondo López

- En esta presentación se usan algunas imágenes generadas por IA
 - Salvo error, cualquier imagen a la que no se le atribuya una fuente u origen expreso
- La IA generativa usada para ello es Microsoft Copilot
 - <https://copilot.microsoft.com/>
- Se ha restringido el uso de estas imágenes a la ilustración de los conceptos explicados en algunas de las páginas
 - Es decir, **como refuerzo visual** a lo explicado en algunas transparencias
 - El procedimiento ha sido describirle a la IA con toda la precisión posible los elementos que quería que apareciesen en la imagen (**prompt**)
 - Y la selección del mejor resultado obtenido, a juicio del autor de esta presentación
 - **No se ha mencionado ni indicado que se copie el estilo a ningún autor, ni que se plagien obras concretas**
- El autor declara expresamente su apoyo al trabajo de los artistas, ilustradores y creadores, de extrema importancia en la actualidad
 - El uso de estas técnicas se ha hecho solo con fines de mejora de las explicaciones, y cuando la alternativa era **no contar con refuerzos visuales** por restricciones de tiempo y presupuesto



¡BIENVENIDO/A!

- Bienvenidos/as a este recorrido por las técnicas de ataque comunes a las que os enfrentaréis
 - Tanto tú como los tuyos
 - **Nadie está a salvo**, y estas cosas pasan todos los días
- Es bueno conocer las técnicas de ataque para luego poder defendernos de ellas 
- Esto es REAL, y os dará conocimientos que os permitirán defenderos
 - ¡Entendiendo la mente del criminal!
- **Un hacker NO ES UN CRIMINAL**
 - Hacker soy yo *¿tengo pinta de chungo?* (Mejor no contestéis a eso... 😅)
 - Un criminal es...un **delincuente** 😅
 - ¡La prensa usa mal el término!



Se puede llevar sudadera con o sin capucha y ser buena persona. ¿No veis la cara de buenos que tienen? ¡No somos criminales! ¡Los delincuentes son criminales! 🕵️



¿QUÉ ES UNA MÁQUINA VIRTUAL?



● Es un ordenador dentro de un ordenador

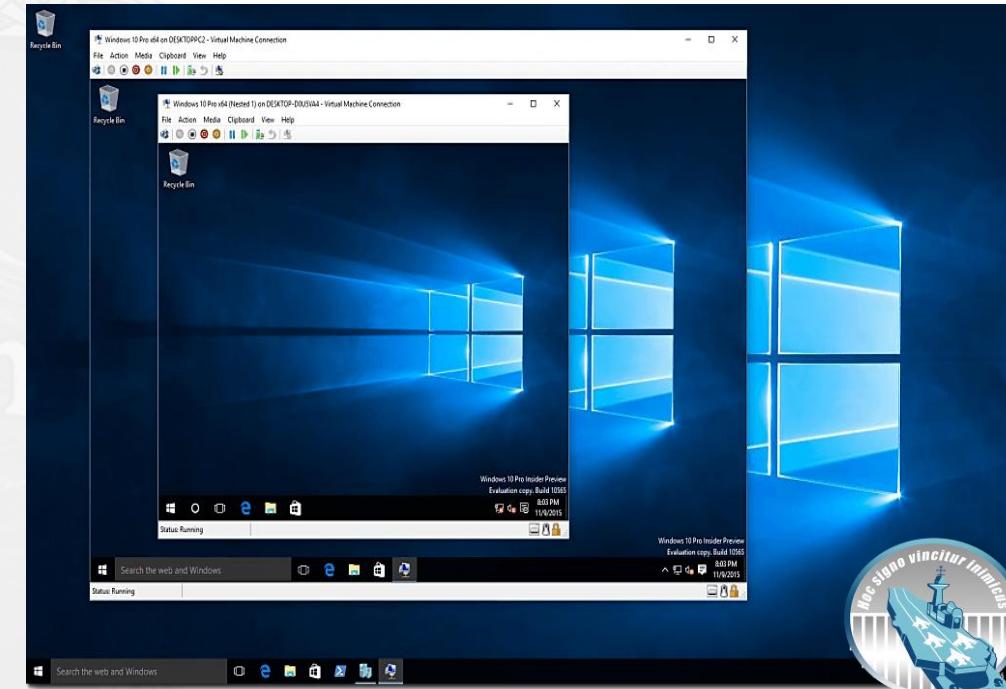
- ¿No conocéis los emuladores? Pues lo mismo, pero de un PC completo
- Windows ... o Linux

● Vamos a usar una Linux para este curso

- Tranqui, solo vas a tener que arrancarla y ya
- Es **gratis y menos vulnerable** que un Windows
- ¿Por qué? Porque si pasa algo, **queda dentro de ella** y no nos rompes el PC

● ¿Quieres tener una para ti? Ok, herman@

- Te la regalamos al final para que la pruebes en casa si quieras con VirtualBox, pero si quieras experimentar...
- Si te mola, te regalo el mini-curso “**R-11 ‘Príncipe de Asturias’**”, ¡que trata precisamente de esto!



You dawg, I Heard you like computers, so I put a computer inside a computer to compute more. Esta es una Windows dentro de un Windows. Nosotros te regalamos “La Perla Negra”, que es un Linux 😊. Fuente: <https://www.xataka.com/especiales/maquinas-virtuales-que-son-como-funcionan-y-como-utilizarlas>

ÍNDICE



▶ Cosas sobre las Personas

- Autenticación
- Computación “sensata”

▶ Uso de Internet

- Usando el navegador de forma segura
- Uso de Redes Sociales

▶ Sistemas de Mensajería

- Email
- Aplicaciones de Mensajería

▶ PCs y Móviles

- Telefonía Móvil
- Ordenadores

▶ Redes y Cosas “Smart”

- Redes de Comunicaciones
- Dispositivos “Smart”

▶ Seguridad “En la calle”

- Seguridad “Física”
- Seguridad Financiera



Accede a este
Módulo en YouTube

[< Ir al Índice](#)

[Autenticación >](#)

[Comp. "Sensata" >](#)



COSAS SOBRE LAS PERSONAS

Cosas que están en nuestra mano para mejorar la seguridad





José Manuel
Redondo López

¿QUÉ TE VAS A ENCONTRAR EN ESTE BLOQUE?

- En este bloque de seguridad personal te voy a enseñar...
 - La tremenda movida que supone tener una contraseña de hacking plebeyo
 - La mala gente que hay por Internet robando cuentas para hacer el cabra, y cómo puedes ser tú una víctima
 - Que Internet está plagado de mentiras (y más de las que imaginas)
 - Que hay peña que va a ir a comerte el tarro con mil historias para que les pagues por cosas que...bueno...son una mezcla entre humo, FOMO y magia
- *¿Te molan estas movidas? ¡Pues si quieres saber más mírate éstas!...*





Autenticación

Asegurando tu identidad





José Manuel
Redondo López

EL PELIGRO DE TENER UNA MALA CONTRASEÑA

● ¿Sabes cómo “revientan tu contraseña”?

- Te engañan 😨 y te la roban contándote alguna movida
 - ¡phishing! ¡ten mil ojos!
- La averiguan “por fuerza bruta” 😬
 - Prueban muchas hasta que dan con la tuya, que es mucho más fácil si es mala
- Prueban una que te han robado de otro servicio y está publicada “por ahí” 😱
 - Asúmelo, usas la misma para muchas cosas
- Prueban una robada de tu PC o móvil 🤔
 - ¡Ojo con lo que instalas en tu máquina!
 - Los cracks de los juegos te pueden hacer crack a ti...
 - Bajarse cualquier cosa de Internet puede hacer que te pase cualquier cosa también...

● ¿Te la han robado? ¡Cámbiala ya!

The screenshot shows the homepage of haveibeenpwned.com. At the top, there's a navigation bar with links to Home, Notify me, Domain search, Who's been pwned, Passwords, API, About, and Donate. Below that is a large button with the text ':--have i been pwned?'. A subtext below it says 'Check if your email address is in a data breach'. There's a search bar labeled 'Email address' and a button labeled 'pwned?'. Below the search area, there are four large numbers: 776 pwned websites, 13,155,814,566 pwned accounts, 115,770 pastes, and 228,884,645 paste accounts. To the left, under 'Largest breaches', are listed various data breaches with their sizes and names, such as Collection #1 accounts (772,904,991), Verifications.io accounts (763,117,241), and Onliner Spambot accounts (711,477,622). To the right, under 'Recently added breaches', are listed more recent ones like Operation Endgame accounts (16,466,858) and pcTattletale accounts (138,751).

Si te han robado tu contraseña de alguna web, aquí te lo dirá. Fuente: <https://haveibeenpwned.com/>



José Manuel
Redondo López

¿QUÉ PASA CUANDO TE ENTRAN EN UNA CUENTA?

● Se pueden hacer pasar por ti 🦸, con todas las consecuencias

- **Engañar a tus amigos** 😬 para que cuenten cosas privadas tuyas, pedir fotos, etc.
 - O propagar estafas que, por ser tú, tus colegas se creerán más fácilmente
- **Dejarte en ridículo** 😳 posteando barbaridades, bajarte de ranking / fundirse tu pasta en un juego
- **Mandar mensajes con insultos** 😡 , virus, etc. en tu nombre a gente que aprecias
 - **El marrón te lo comes tú, ahora demuestra que te han robado la cuenta y que no eras tú...**
- **Registrarte en sitios “turbios”** 😲
- ... (piensa cualquier maldad, que te va a pasar)

● ¿Ves por qué es importante lo que te dije?

The infographic is titled "Indicadores de que te han robado la cuenta" (Indicators that your account has been stolen) and is produced by incibe (Instituto Nacional de Ciberseguridad) and OSi (Oficina de Seguridad del Internauta). It features a central illustration of a smartphone displaying a social media profile with a lock icon, surrounded by social media icons (Twitter, Instagram, Facebook, WhatsApp) and two people. A speech bubble asks: "¿Mensajes leídos? ¿Publicaciones no realizadas por ti? ¿Contactos desconocidos? ¿Cambios en los datos de recuperación de la cuenta? ¿No funcionan tus contraseñas de acceso?" (Read messages? Unpublished posts? Unknown contacts? Changes in recovery data? Your login passwords not working?). Below this, a section titled "Si te sientes identificado, sigue estos consejos:" (If you feel identified, follow these tips) provides six steps:

- Recupera el control de la cuenta a través de los procedimientos que ofrece el servicio afectado.
- Cambia la contraseña de acceso que estabas usando y también la de todos los servicios online en los que utilizas la misma.
- Activa la doble verificación.
- Revisa que los datos de recuperación de la cuenta son los correctos.
- Avisa a tus contactos y conocidos de la situación.
- Si no has conseguido recuperar el acceso, denuncia ante las FCSE aportando las evidencias.

#OSIconsejo
incibe.es/ciudadania

No es broma, y te puedes meter en un lío guapo. ¡Cambia la contraseña, avisa y denuncia lo antes posible, herman@!



Computación “sensata”

Entrenando tu “ciber-sentido común”





José Manuel
Redondo López

BULOS Y FAKE NEWS

• ¿Sabes la de trolas que hay por Internet? 🙄

- Periódicos, redes sociales, WhatsApp, streamers, Discord...
- ¡Quieren manipularte! 🤡

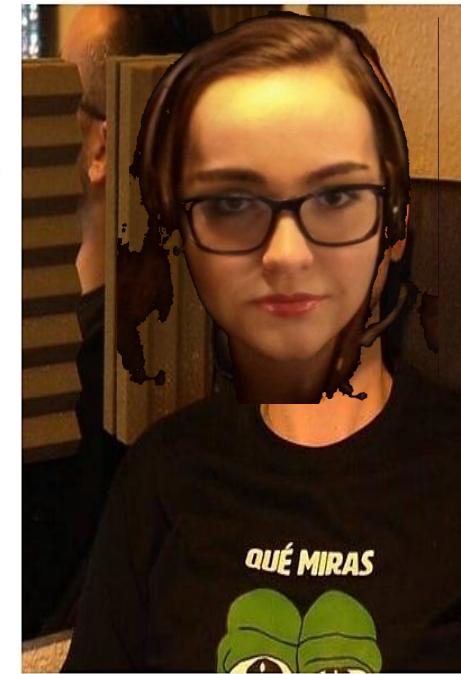
• ¿Y qué puedes hacer?

- ¡No creerte todo a la primera!, sobre todo si es muy bruto
- Muchos streamers crean “salseo” 🥳 para conseguir viewers
 - A más visitas, ¡más dinero para ellos!
- **Contrasta, lee y respira antes de cargar contra nadie!**
 - Si KatyFlipi dice una burrada, probablemente sea mentira
 - Si el Birrius se enfada con Ibay, también
 - Clics, visitas, dinero para ellos...¡que no te engañen!
- Si lees “Noticia patrocinada por” o similar, **estás viendo un anuncio que hacen pasar por noticia** 🎵
 - ¿No me crees? El precio de ponerlas es público. Ej.:
<https://publicidad.lne.es/contenido-digital/contenido-patrocinado/>

EL ALGORITMO Y EL DRAMA

Llámalo 'salseo' o 'Sálvame': por qué hasta los 'youtubers' han caído en el famoseo

Las últimas polémicas entre 'streamers' demuestran que incluso muchas de las estrellas que crecieron como alternativa a los contenidos tradicionales del corazón acaban en la noria



¿No me lo estoy inventando eh? Busca un poco y fliparás. Fuente:

https://www.elconfidencial.com/tecnologia/2022-03-23/salseo-youtubers-streamers-ibai-xokas-prensa-rosa_3395429/



Los “COACHES” (AKA “COMETARROS”)

- Son gente que tiene la fórmula mágica que te enseña a vivir como un máquina 💰💰

- Te ayudan a salir de “la Matrix” y **convertirte en tu mejor versión**
- Te enseñan buenos hábitos, rutinas y desarrollo personal...

- Pero debes tener cuidado con algunos...

- **Te apartan de amigos y familia 🤡**, porque “no te dejan crecer”
 - *¿No será que quieren que solo los escuches a ellos?*
- **Te piden “compromiso” 🤡**: Que es palmar cada vez más pasta 💰💰 para estar cerca de ellos
 - *¿Y tú realmente que obtienes a cambio?*
- **Te invitan a meter más afiliados 🤡** para “subir de nivel”
 - Todo negocio donde ganas metiendo a más gente **es un esquema piramidal** ▲ ...que acaba reventando **SIEMPRE**
- Una vez dentro **te anulan y/o te maltratan** verbalmente 😠
 - *¿Estás en un grupo y no puedes decir lo que opinas? Si lo haces, ¿la gente te insulta? ¿Seguro que quieras pagar por eso?*



Muchos tienen ideas y rutinas interesantes y buenas, pero...cuidado no te metas en un sitio donde sea complicado salir...o simplemente hablar. **¿No me crees a mí?**
Pues cree a La Gata de Schrödinger:
<https://www.youtube.com/watch?v=Y9yEoOKMAhE>



José Manuel
Redondo López

¿CREEES QUE LO HAS ENTENDIDO TODO? ¡AUTOEVALÚATE!

?

● Asegúrate de haber entendido lo siguiente

-  **Autenticación**
 - Cómo se *las apañan los delincuentes para robarte contraseñas*
 - Qué te puede pasar si te las roban, y por qué las debes defender
-  **Computación “sensata”**
 - Que *internet está plagado de bulos, y que solo depende de ti no caer víctima de ellos usando las herramientas adecuadas para desmentirlos*
 - *Por qué algunos coach que hay en internet solo quieren tu dinero y no que mejores en tu vida, y los indicios que te pueden hacer descubrir a uno de estos*

[< Ir al Índice](#)

[Navegación >](#)

[Redes Sociales >](#)



USO DE INTERNET

Navegando de forma segura





José Manuel
Redondo López

¿QUÉ TE VAS A ENCONTRAR EN ESTE BLOQUE?

- En este bloque de seguridad a la hora de navegar y compartir información por Internet te voy a enseñar...
 - Que si el navegador te basilah tu lo ignorah y lo asimilah (vamos, que **pases de los avisos del navegador**)
 - Que Google a **veces tiene "bicho"** en los primeros resultados de búsqueda que te saca
 - La banda de boludos que se dedica a **okupar cuentas** de lo que sea para estafas y otras movidas turbias, y cómo lo hacen
 - Que hay peña **ofreciendo colaboraciones** y en realidad es otro invento para robarte la cuenta, pasta o mil historias turbias
- *¿Te molan estas movidas? ¡Pues si quieres saber más mírate éstas!...*





Usando el navegador de forma segura

La navegación es realmente una actividad de alto riesgo





José Manuel
Redondo López

ANUNCIOS Y NOTIFICACIONES FALSAS

● ¿Sabes que hay delincuentes que paga por meter anuncios “envenenados”?

- Meten en webs anuncios que parecen **ventanas de Windows con avisos chungos** (virus, etc.) 💀
- O con ofertas salvajes, etc. **lo que sea para llamar tu atención**

● ¿Para qué?

- Para que **cliques y descargas un virus** 💀
 - ¡O se te descargue solo si no tienes el navegador a la última! 😱
- Para que vayas a una web falsa y **metas datos tuyos** (robos de cuentas, dinero...) 📁
- **¿Sabes qué?** Ni un anuncio es bueno, ¡no lo toques ni con el ratón de otro!

Anuncio diciendo que te están espiando y que descargas un programa para protegerte. En realidad, es un virus. Encima te mete prisa...Fuente: <https://news.sophos.com/es-es/2020/09/10/alertas-falsas-como-detectarlas-y-detenerlas/>

The image contains two side-by-side screenshots of fake malware warning pop-ups. The left screenshot shows a browser window with a 'Malware detected!' message from 'apple-online-guard.com' over a Google search result. It claims the iPhone is infected with viruses and malware, with 31.3% damage from 15 instances of malicious code. It offers to 'Repair iPhone Now'. The right screenshot shows a similar warning from 'naked security by SOPHOS' with a 'FAKE' label at the top. It also claims someone may be watching the user's browsing activity and exposes their IP address. It provides steps to encrypt web traffic and change IP addresses, and ends with a 'Install Now' button.

Otra infección masiva (¡15 virus, herman@, massiiivo!), y encima con componente de prisa para provocar el pánico y que piques. Todo mentira. Fuente: <https://www.avg.com/es/signal/spot-fake-virus-warning>



José Manuel
Redondo López

ENLACES ENVENENADOS

● ¿Sabes que hay delincuentes que ponen anuncios de programas falsos en las búsquedas de Google?

- Para que te salga ese programa falso el primero cuando busques el verdadero
- Como “Enlace patrocinado” o “Anuncio” (“Ad” en inglés)

● ¿Para qué?

- Para que te salga el primero, no mires y piques
 - Vas a una página falsa...¡pero idéntica a la original! 🤖
 - Te descargas el programa falso y ¡ya tienes “bicho” en tu PC o en tu móvil! 🚨 🚨
- ¡Ni caso a los anuncios de Google!

● Los delincuentes son capaces de cualquier cosa, como te cuento en el M-31 “Segura”

¿Te suena el OBS? ¡Es un programa muy famoso para hacer streaming!

The screenshot shows a Google search results page for the query "obs". The top result is a sponsored link (Ad) from "http://www.obstreaming.site/" with the text "OBS Stream - Start streaming quickly". A red box highlights the URL. Below the ad, a note says "About 535,000,000 results (0.63 seconds)". Another note says "Es un anuncio". A red box highlights the word "Anuncio". The page also includes a note about OBS being used for video recording and live streaming.

Blender es un programa muy famoso para hacer 3D.
Pues ya ves...

The screenshot shows a Google search results page for the query "blender 3d". The top result is a sponsored link (Ad) from "https://blender3dorg.fras6899.odns.fr/" with the text "Blender ‘malo’". A red box highlights the URL. Below the ad, a note says "About 118,000,000 results (0.54 seconds)". Another sponsored link (Ad) from "https://www.blender3d-software.com/" is shown with the text "Blender ‘malo’". A red box highlights the URL. The page also includes a note about Blender being an open-source 3D creation suite.



Uso de Redes Sociales

Compartir está bien, pero hay que hacerlo con cabeza



ROBOS DE CUENTAS EN REDES SOCIALES



José Manuel
Redondo López

● Hay gente que se dedica a “cazar” cuentas en TikTok, Instagram, X...

- Una vez la **roba**, cambia la imagen y la información para lanzar estafas o desinformación
- ¡O no lo hace y trata de hacer lo mismo con tus amigos!
- *¿Cuántos seguidores tienes?* Pues ahora todos son posibles víctimas...

● ¡Lo mismo te puede pasar a ti!

- **¡Cuidado si un amigo te pide “cosas raras”!**
- **Nunca des tu contraseña a nadie ni ningún código que te llegue**

● O puedes ser víctima de un bot

Emilia
@Emilia1586597
Beach bum looking for someone to ride the waves with 🌊 💕 🔥 Sparks will fly! Click bio! 🔥 💕
otweb.online/officialArmstr... Joined October 2023
14 Following 40 Followers

Hay muchos perfiles falsos que solo quieren que entres en la web que publicitan, donde te intentan instalar malware o te roban datos. Otras veces roban uno real y hacen que postee estafas

Otros intentos se basan en asustarte para que entres en un enlace o engañarte para que des un código o metas tu usuario y contraseña en una página falsa copiada de la real, que hace que te roben la cuenta

Mira quien murió, en un accidente creo que lo conoces. 😢
<https://6tag.sbs/-hV7fUtG.ru>

Eres tu en el video ?
<https://i-c.run/-9>

22/03/2022
test my first game pls :)
<https://github.com/ee/gam>
pass: test

ROBOS DE CUENTAS EN REDES SOCIALES



José Manuel
Redondo López



- Otras veces recibes un mensaje de un contacto o empresa (real o suplantado) que te promete dinero (Ej.: Un concurso)
 - Pero solo si **resuelves un reto visual** en una red social
- El reto es muy fácil, y cuando lo aciertas te piden hacer esto
 - Ir a la configuración de tu red social (normalmente Instagram)
 - **Cambiar el email de verificación de tu cuenta** por uno que te da el contacto
 - Que supuestamente pertenece a la empresa de la promoción, para hacerte el pago
 - La excusa para hacerlo es variada, pero siempre te dicen que lo volverás a cambiar por el tuyo en unos minutos
 - En realidad, al hacer esto es que **le damos el control de nuestra cuenta** al propietario de este correo (el estafador)
 - Entonces **propagará** la estafa a tus contactos haciéndose pasar por ti
- Aunque suena a fantasía, es muy real
 - <https://www.elcomercio.es/sociedad/instagram-estafa-reto-visual-robar-cuenta-20220705195226-nt.html>
 - Y van a por gente joven, ¡como tú!



Retos de “encuentra la diferencia” superfáciles.

Estafa. Fuentes:

<https://www.elcomercio.es/sociedad/instagram-estafa-reto-visual-robar-cuenta-20220705195226-nt.html>,
<https://www.tribunasalamanca.com/noticias/296194/asi-es-la-nueva-estafa-que-roba-cuentas-de-instagram>

FALSAS COLABORACIONES

- **¿Tienes presencia en las redes sociales? ¿Seguidores? ¡Bien! 🔥 Lit!**
- **Pero cuidado:** puedes ser un objetivo goloso para delincuentes
 - Te ofrecen una falsa colaboración con una marca para que hagas promoción, pero...
 - Te piden dinero por adelantado
 - Te piden el DNI, cuentas del banco, tarjeta...
 - Te piden que compres algo tú primero
 - O te piden algo que hagas gratis por “promocionarte” 
 - Se lo llevan y te quedas sin nada
- **¡Ni caso! ¡No hay que palmar pasta para trabajar nunca! ¡Ni regalar tu trabajo!**

Matt Gilman

Equipo de anuncios

Hola, Queremos publicidad en su página de Facebook, se le pagará \$1800 por 1 anuncio, si está interesado, responda como Gracias

Hace 33 min



José Manuel
Redondo López

Hola hola! ☀

Soy una creadora de contenido con +10k de seguidores y te quiero proponer una colab ❤

Tu me mandarías unos cuantos pendientes a mi elección y yo te promociono con un post y en stories 🎥📸

Ya me dices 😊

Buenos días, lo siento pero mi negocio es pequeño y tengo muy poco stock, por lo que no puedo permitirme regalar pendientes. Gracias y que tengas un buen dia!

Es una pena! Tengo +10k de seguidores y un buen engagement y mi promo te ayudaría muchísimo! Aumentarías tu engagement y ventas, piénsatelo 💯😊



Envía un mensaje...





José Manuel
Redondo López

¿CREEES QUE LO HAS ENTENDIDO TODO? ¡AUTOEVALÚATE!



● Asegúrate de haber entendido lo siguiente

- **Usando el navegador de forma segura**
 - Que *ningún anuncio es fiable y, por tanto, no debes hacer clic a ninguno*
 - *Por qué los anuncios que salen en las búsquedas de Google puedes considerarlos “veneno” y, por tanto, tampoco debes hacer clic en ninguno*
- **Uso de redes sociales**
 - *Por qué a los delincuentes les interesa robar cuentas en redes sociales y algunos de los trucos que usan para eso*
 - *Cómo ser influencer (o simplemente tener una cuenta en una red social) puede acabar contigo palmando dinero por un trabajo o colaboración que realmente no te va a dar ningún beneficio, y que es básicamente una estafa*

[< Ir al Índice](#)

[Email >](#)

[Aplicaciones >](#)



SISTEMAS DE MENSAJERÍA

Asegurando lo que enviamos a otros



¿QUÉ TE VAS A ENCONTRAR EN ESTE BLOQUE?

- En este bloque de seguridad a la hora de comunicarte con otras personas te voy a enseñar...
 - La cantidad de historias que se monta la gente para **estafarte vía email**
 - Que a veces estas estafas no son correos que mandan en plan masivo, sino que **van (literalmente) a por ti**
 - La cantidad de historias que se monta la gente para **estafarte vía mensajería**
 - Lo insano que es que **le roben el WhatsApp** a un/a colega para luego timarte a ti haciéndose pasar por el/ella
- *¿Te molan estas movidas? ¡Pues si quieres saber más mírate éstas!...*





 **Email**

El correo electrónico sigue siendo un problema serio de seguridad





EL FRAUDE POR EMAIL

• ¿Te he dicho que los delincuentes saben miles de formas de “colártela”?  Mira...

RECONOCIMIENTO RÁPIDO DE CORREOS SOSPECHOSOS

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

De:

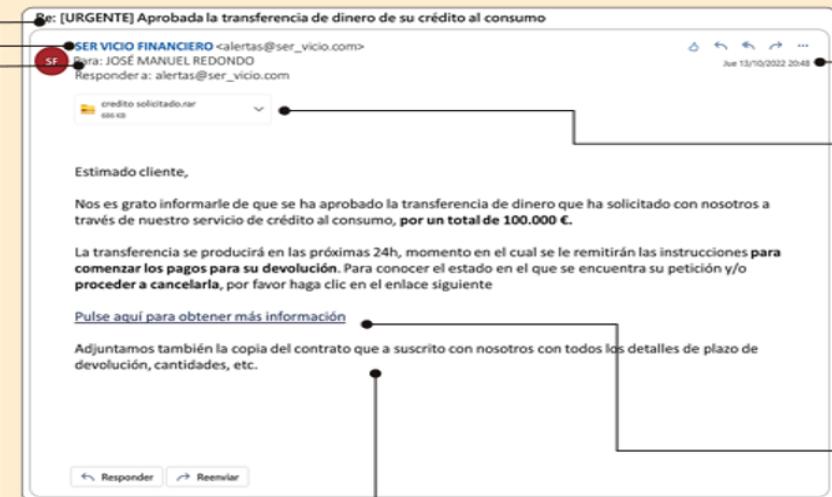
- Remitente desconocido, no habitual o no tengo referencias suyas
- No es de mi empresa o no tiene que ver con ella
- Le conozco (empleado, proveedor, cliente...) pero me escribe algo atípico o diferente a lo habitual
- El dominio del remitente es “raro” (muy largo, con guiones, con letras y nºs sin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

Basado en:

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



Universidad de Oviedo

Imprime esta imagen y pásasela a tus padres para que dejen de preguntarte sobre si un mensaje es o no verdadero. ¡Ahora tu eres el pro!).

Si quieres saber más sobre timos porque te mola el “True Crime”, soy streamer de esos temas 😊 en:

<https://www.youtube.com/@j.m.redondo8618/featured>

También hago fichas de fraudes aquí:

<https://github.com/jose-r-lopez/Fraudes-y-Timos/wiki>

¡Todo es gratis y sin monetizar!

CUANDO VAN A POR TI (SPEAR PHISHING)

- La estafa moderna es **la que lo sabe todo de ti**, y con eso resulta más creíble 
- **¿Cómo? ¿Tienen poderes?** Sí, de robo
 - Miran **movidas que compartes** en redes sociales
 - Miran **datos que han robado** de muchos sitios (la DGT, bancos...)
 - ¿Cuáles? <https://xposedornot.com/xposed>
 - ¡Lo saben todo de ti y pueden usarlo!
- Advierte a tu familia de que los delincuentes **pueden saberlo TODO de ti** 
 - Nunca contestes dando datos tuyos, ¡**imagina que estás en un interrogatorio!**
 - **Llama tú siempre luego para comprobar**, ¡pero no uses para eso nada que te de quien te llama!

Ticketmaster investiga un robo de datos masivo que afecta a 560 millones de usuarios

La responsabilidad del ataque se la ha atribuido el grupo de hackers ShinyHunters, quienes supuestamente han puesto a la venta 1,3 TB de datos sensibles de los clientes.



Fuente: <https://www.publico.es/economia/ticketmaster-investiga-robo-datos-masivo-afecta-560-millones-usuarios.html>

ATAQUES INFORMÁTICOS >

La Guardia Civil investiga un posible robo de datos de millones de conductores en un ciberataque a la DGT

Los agentes limitan el acceso a varios actores sospechosos de intentar entrar en la base de datos de la Dirección General de Tráfico

Fuente: <https://elpais.com/tecnologia/2024-05-31/la-guardia-civil-investiga-un-posible-ciberataque-a-la-direccion-general-de-trafico.html>

Banca y finanzas

Los hackers que atacaron al Santander ofrecen los datos robados por 2 millones de dólares

Fuente: <https://www.eleconomista.es/banca-finanzas/noticias/12843603/05/24/los-hackers-que-atacaron-al-santander-ofrecen-los-datos-robados-por-2-millones-de-dolares.html>

Miro hacia un lado...robo...miro hacia el otro...filtración. Robo, filtración, robo, filtración. Haack. Lo van a saber todo de mi...



Aplicaciones de Mensajería

WhatsApp, Telegram, Signal, Facebook Messenger...





TIMOS POR MENSAJERÍA

- ¿Sabes que los nºs de teléfono que te envían SMS (y los que te llaman) se pueden falsificar porque no hay medidas que lo prevengan? Pues ahora ya lo sabes 

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

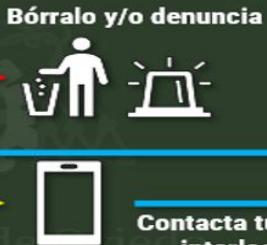


De:

- 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**)



Contacta tú con el interlocutor

Confirmación



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



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...)

"Papá, Mamá a partir de ahora no os creáis ningún mensaje o llamada, aunque venga del teléfono de siempre, porque se puede falsificar"

probablemente sea la lección más importante que puedas sacar hoy de aquí.

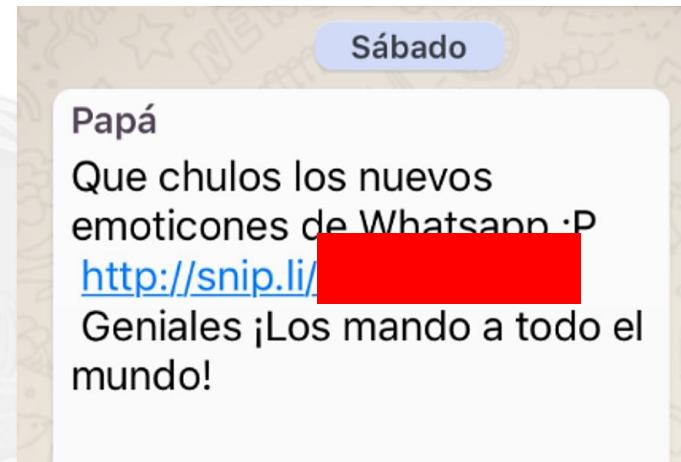
Ten en cuenta que, al no poder distinguirlos, el teléfono te meterá mensajes reales y falsos de una misma entidad dentro del mismo hilo de conversación...y eso puede DOLER



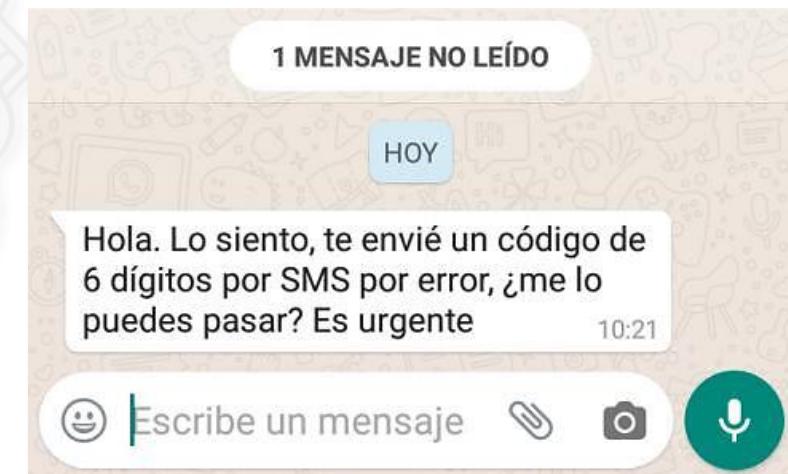
José Manuel
Redondo López

ROBOS DE CUENTAS

- Los contactos de WhatsApp, etc. no se pueden falsificar igual que el teléfono
- Pero...*¿y si un contacto tuyo instala un virus y le roba la cuenta?* 
 - Ahora todos sus contactos (¡y tú entre ellos!) **sois potenciales víctimas**
 - *¿Te envían algo raro? ¿Te piden un código? ¡NI CASO!*
- Explícaselo a tu familia. ¡Ahora tu eres el hacking bestia!  



Este era mi padre.
Solo que no era él...era el virus que se instaló al bajarse un programa chungo de la Store



A mi amigo le robaron el WhatsApp. Y el delincuente ahora está intentando robar el mío. LOL.
<https://www.xataka.com/basics/timo-whatsapp-codigo-enviado-error-que-como-funciona-como-evitar-que-te-roben-cuenta-este-sms>



José Manuel
Redondo López

¿CREEES QUE LO HAS ENTENDIDO TODO? ¡AUTOEVALÚATE!



● Asegúrate de haber entendido lo siguiente

- **Email**
 - *Los criterios generales para distinguir un mail verdadero de uno falso*
 - *Que el hecho de que vayan a por ti ya no es solo algo que ocurre en películas de espías, sino que está pasando a diario*
 - *Que muchas veces lo hacen usando información que tú mismo das en redes sociales o bien que roban a empresas*
- **Aplicaciones de mensajería**
 - *Los criterios generales para distinguir un mensaje verdadero de uno falso en una aplicación de mensajería cualquiera*
 - *Por qué es tan interesante para algunos delincuentes robar cuentas de WhatsApp o aplicaciones de mensajería similares y seguir cometiendo crímenes con ellas*

< Ir al Índice

Móviles >

Ordenadores >



PCs y MÓVILES

Trabajando con dispositivos de forma segura





José Manuel
Redondo López

¿QUÉ TE VAS A ENCONTRAR EN ESTE BLOQUE?



- En este bloque de seguridad al usar tu móvil o tu PC te voy a enseñar...
 - Que **ojito con las tiendas oficiales de apps**, que pueden colar “basura con bicho” más fácil de lo que crees (especialmente en Android)
 - Que **bajarte aplicaciones de sitios turbios** lleva a cosas aún más turbias, y tu teléfono (y tus datos) no se lo merecen
 - Que ese juego por el que no quieras pagar **te puede costar muy caro**
 - Que a veces un programa viene con “**sorpresa**” (no necesariamente mala del todo, pero si algo que te toca las narices) si no estás atento/a a lo que descargas
- *¿Te molan estas movidas? ¡Pues si quieres saber más mírate ésta!...*





Telefonía Móvil

Si está en nuestra vida a todas horas...hay que protegerlo a todas horas ☺



MALWARE EN CANALES OFICIALES



José Manuel
Redondo López

- Bajarse una aplicación de una tienda oficial **no te garantiza** que esté 100% libre de virus 🕸️
- Muchos delincuentes pagan por subir aplicaciones fraudulentas a estas tiendas
 - Normalmente **clones de aplicaciones conocidas** que descargan, modifican y te intentan colar como buenas
 - Ej.: Clones de juegos populares de pago pero que son gratis, con el mismo nombre pero que pone "Plus", "Extra", "Premium",...
 - O cosas que hacen **movidas "mágicas"** o demasiado increíbles
- Usa tu sentido común y enseña a los tuyos cuándo una aplicación tiene más ➤ ➤ que ese/a que conociste el finde pasado

The image shows two screenshots from the Google Play Store. The top screenshot is for the app 'Download More RAM - The Official App' by Egg Games. It shows a download progress bar at 2,7 MB, a 'Todos' rating, and over 50k downloads. A large green 'Instalar' button is prominent. The bottom screenshot is for the app '32 GB SD Memory Card' by zilow free app. It shows a 4-star rating with 113 reviews, an 'Everyone' rating, and a note about containing ads. Both screenshots illustrate how malware can masquerade as legitimate tools like RAM expanders or SD card managers.

¿Un programa para tener más RAM? ¿Para estirar nuestra tarjeta SD como un chicle? Venga ya, tío...

MALWARE EN CANALES NO OFICIALES



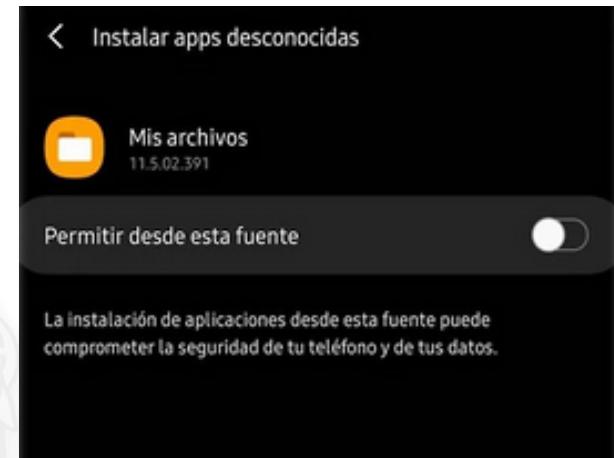
José Manuel
Redondo López

● ¿Sabes que hay streamers / noticias que te invitan a instalar aplicaciones muy peligrosas? 😠

- Aplicaciones que necesitan (o sirven para) “rootear” el tfno.
 - Darte el control total del mismo, pero con la posibilidad de que ya no funcione como debe
- **Aplicaciones de orígenes desconocidos** 🚫
 - Como los ficheros .apk en Android
 - Si ya las de la tienda oficial pueden tener “bicho”, imagina una que no sabes de donde viene...
 - ¿Sabes la cantidad de gente que se ha infectado por instalar lo que no debe de esta forma? Fliparías...

● ¡No hagas ninguna de las dos cosas!

- Aunque te “vendan” que es segura, de confianza, etc.
 - O te están engañando o troleando
 - O ni siquiera lo saben, les han pagado por promocionarla



Esto abre la opción a que instales lo que quieras de cualquier parte...con todas sus consecuencias

😢. ¡Nunca lo hagas! Fuente:

<https://www.xatakandroid.com/tutoriales/como-instalar-aplicaciones-en-apk-en-un-movil-android>

LA NACION > Tecnología

Cómo descargar la última versión de WhatsApp Plus APK de junio 2024

Ya está disponible para instalar la más reciente edición de esta app alternativa; cómo es paso a paso para bajarla en el celular

3 de junio de 2024 • 10:51

No se instalan aplicaciones Android no oficiales (.apk), ni aunque te lo recomiende un medio generalista (normalmente no saben los peligros que tiene...). Te puede tocar la lotería de la avería...



Ordenadores

Portátiles, sobremesa...nuestra vida digital completa suele estar en uno





José Manuel
Redondo López

EL PELIGRO DE LOS CRACKS Y EL MALWARE

- Sale el nuevo CoD, EA Sports FC, expansión de los SIMS...y dices ¡PEC! 😬

- Pero es muy caro 😞

- ¿Qué hace mucha gente en esos casos?

- Quitar las **protecciones contra copia**
- Bajándose un **crack** o una **versión pirateada** 💀

- Y aquí tienes una de las formas más rápidas de pillar un virus en tu PC 🚨

- Cracks, cheats, aimbots, versiones pirateadas de lo que sea vienen con virus muchas veces 💀
- Y no siempre tu antivirus lo detecta
 - ¿Te crees que son todopoderosos?

- Como en los teléfonos, página no oficial => igual te descargas el mal 😷



The screenshot shows a software download website with a sidebar for sorting by popularity, price, and editor rating. The main area displays a grid of "Most Popular Apps for Windows" including:

- Malwarebytes (FREE TO TRY)
- CCleaner (FREE)
- PhotoScape (FREE)
- Free YouTube Downloader (FREE)
- IObit Uninstaller (FREE)
- Internet Download Manager (FREE TO TRY)
- Advanced SystemCare Free (FREE)
- uTorrent (FREE)
- WinRAR (64-bit) (FREE TO TRY)

En este tipo de páginas la mayoría de lo que te bajas no te da amorch, sino que viene con "sorpresa" desagradable y bomboclaat



José Manuel
Redondo López

POTENTIALLY UNWANTED PROGRAMS o PUPs

● Te descargas una cosa de su página oficial y te viene con “extras” 🙄

- No necesariamente nada malo, son programas que pagan por descargarse junto con lo que buscas 😱
- Publicidad, pero de otra forma

● ¿Y tú pa que quieres instalar eso? Jaja saludos

- Intenta **instalar solo lo que necesites** y fuera
- Menos programas son **menos problemas**, más disco libre, más CPU para viciar... 💻
- De verdad, **no llenes el PC de miles de cosas** que luego se lía y no sabes por donde... 🗑
 - Instalar cosas a lo loco te puede dejar el PC temblando
 - O si quieras probar algo mételo en una máquina virtual :P

The screenshot shows the download page for Adobe Acrobat Reader DC. At the top right, there's a red box highlighting the "OPTIONAL OFFERS" section for McAfee. It contains two checkboxes:

- Yes, install the free McAfee Security Scan Plus utility to check the status of my PC security. It will not modify existing antivirus program or PC settings. [Learn more](#)
- Yes, install McAfee Safe Connect to keep my online activities and personal info private and secure with a single tap. [Learn more](#)

Below this, another red box highlights the "GET MORE OUT OF ACROBAT:" section, which includes a checkbox for installing the Acrobat Reader Chrome Extension.

Algunos programas legales vienen con “equipaje”.
Pasando de todo. Tu vienes a leer PDFs, lo otro lo instalas
si te interesa





José Manuel
Redondo López

¿CREEES QUE LO HAS ENTENDIDO TODO? ¡AUTOEVALÚATE!



● Asegúrate de haber entendido lo siguiente

- **Telefonía Móvil**
 - Que el hecho de que una aplicación esté en una tienda oficial no significa que sea segura
 - Que, si encima las descargas de una tienda no oficial, las probabilidades de que sean aún menos segura son todavía mayores
- **Ordenadores**
 - Que si descargas cosas de lugares sospechosos la probabilidad de tener una sorpresa desagradable aumenta muchísimo
 - Que los cracks para juegos, programas para hacer cheats o similares son una de las formas más típicas de conseguir acabar infectado y con un problema muy serio
 - El truco qué hacen algunas aplicaciones de colarte otra en la instalación a ver si no te das cuenta y entonces la instalas para que ellos ganen dinero por publicidad
 - Que, por tanto, antes de instalar nada hay que mirar el programa de instalación con 1000 ojos, no vaya a ser que te la cuelen así

< Ir al Índice

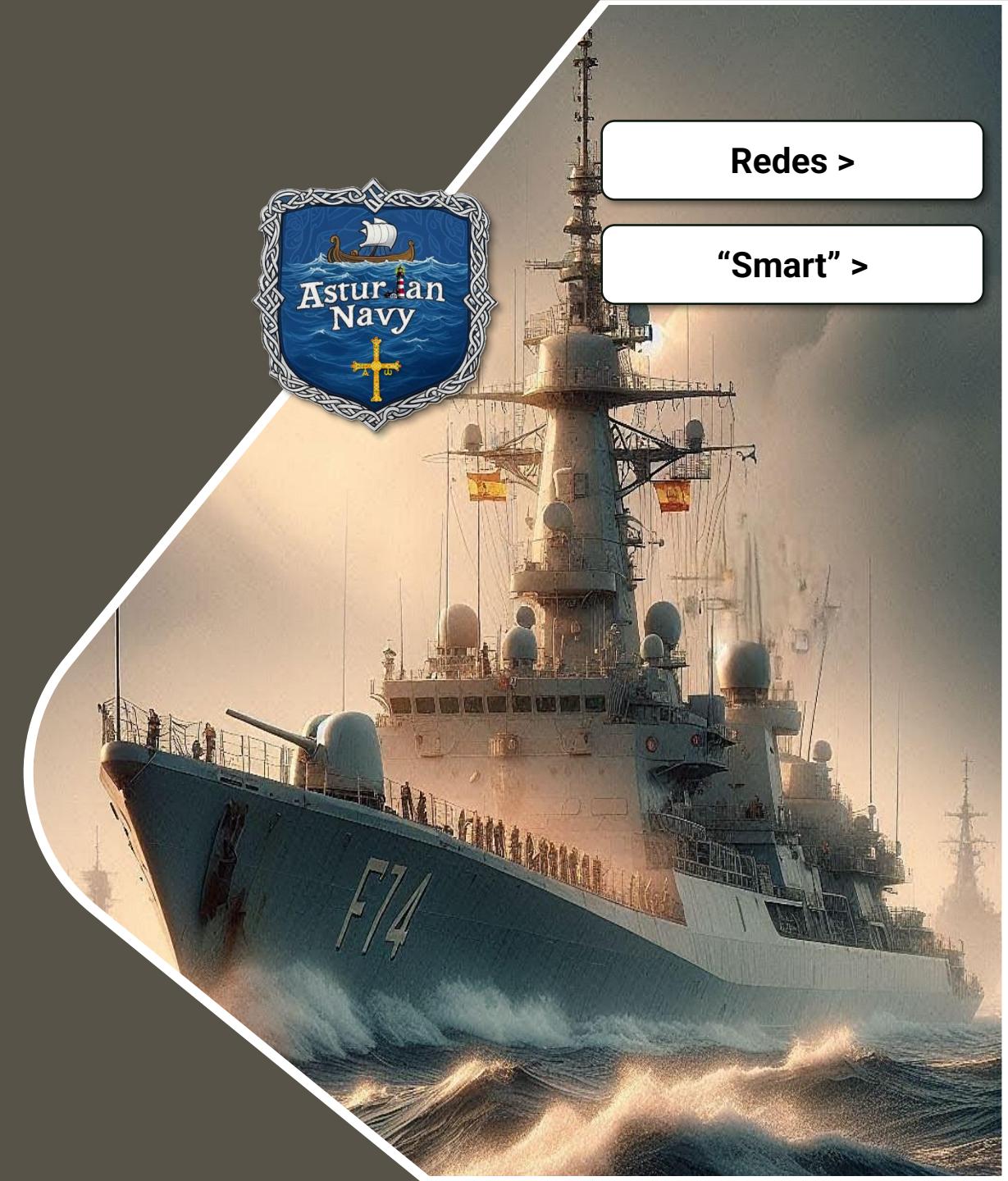
Redes >

“Smart” >



REDES Y COSAS “SMART”

Protegiendo nuestros dispositivos y comunicaciones





José Manuel
Redondo López

¿QUÉ TE VAS A ENCONTRAR EN ESTE BLOQUE?



- En este bloque de seguridad sobre cómo usan la red cualquiera de tus dispositivos te voy a enseñar...
 - Que en los juegos online hay gente que no viene precisamente a jugar y **tendría que estar encerrada**... así que mejor no te cruces con ellos
 - Que como digas que sí a una **asistencia remota**, tu PC explota
 - La primera "**full hacker experience**", pero del lado de los malos para que entiendas como se hace uno de los ataques más típicos (y sencillos)
- *¿Te molan estas movidas? ¡Pues si quieres saber más mírate éstas!...*





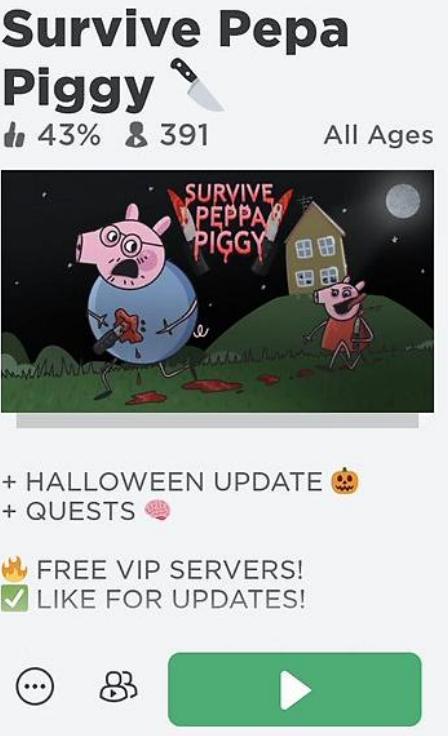
Redes de Comunicaciones

Lo que nos conecta con el “ciber-mundo” también necesita atención



PELIGROS EN JUEGOS ONLINE

- En serio, tenemos una movida importante con juegos de creación y sociales como Roblox 🎮
- Hay peña que crea juegos chungos y los pone para todas las edades
 - Por ejemplo, los simuladores de ir al baño WC
- Los usa para atacar a vuestros avatares y basura varia para arruinarte el juego 😠
 - Pedirte fotos 📸, videos 📹, el WhatsApp para hablar con ellos, decirte barbaridades... (grooming) 😳
 - Cuidado con esta gente: Avisa a tus padres enseguida si te topas con uno 🚓
 - **Denuncia, bloqueo y pasa de ellos**
 - Vienes a jugar, ¡no a que te coman la cabeza y buscarte problemas!



Hay gente que está fatal de la cabeza. Si no conoces en la vida real a quien te habla, pírate de ahí más rápido que Flash

Welcome to Public Bathroom Simulator, use the toilet, wash your hands, and strike up some conversation!

Public Bathroom Simulator
81% & 3K All Ages

XYZ Public Bathroom...
64% & 291

Public Bathroom
67% & 124

MURDER

Algunos de los juegos de Roblox son...de fifes



José Manuel
Redondo López

LA “ASISTENCIA REMOTA”

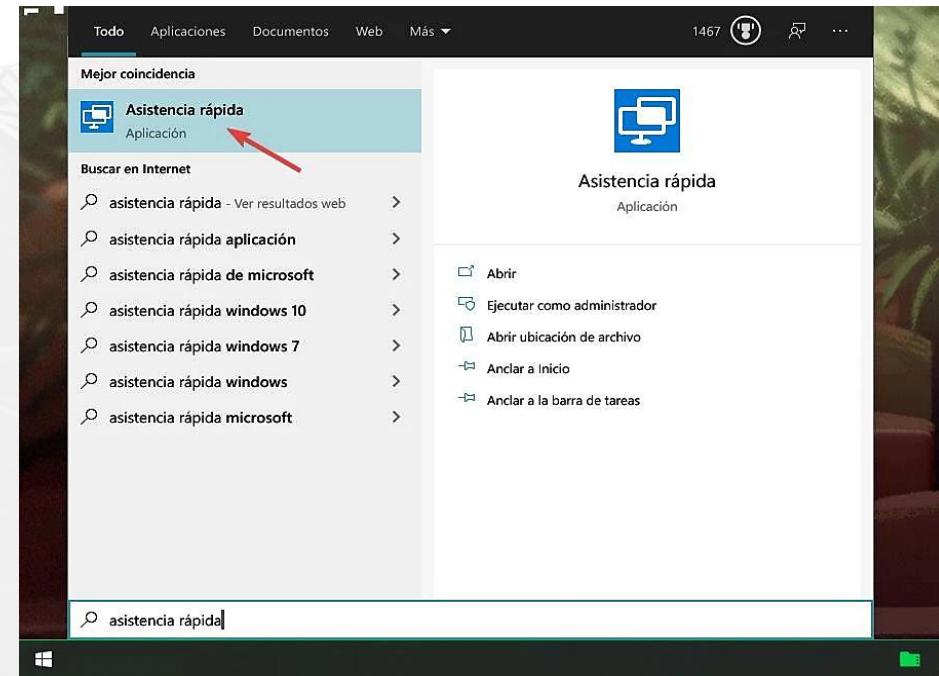
● ¿Sabes que hay muchos timos que tratan de engañarte para que instalas un programa? 🤡

● ¿Virus? Sí, eso también. Pero muchas veces es un programa de control remoto del PC 🤖

- Entonces **te roban** de ahí hasta la vergüenza 😞
- **Fotos** que tengas (para chantajearte o cosas turbias) 📸
- **Contraseñas** de tus cuentas (y las del banco) 🔒
- **Usar tu PC** para armarla en otro lado y que te culpen a ti 🛫

● Si alguien te llama con cualquier movida y te piden instalar “un programa para arreglar el problema” ¡ni de guasa! ✋

- ¡Avisa a tus padres para protegerlos! Es muy común 🚫



A veces no hace falta instalar nada, sino que directamente te piden que uses un modo que tiene **Windows** para ayudar a otras personas con un problema desde casa, la “Asistencia remota”. Y sí, les asistes remotamente a que te roben todo lo que tengas en el PC 😵. Fuente:

<https://www.genbeta.com/windows/como-ayudar-a-alguien-a-resolver-problemas-windows-10-controlando-su-ordenador-forma-remota>



Dispositivos “Smart”

No conviertas tu vida digital en una especie de Skynet ☺





José Manuel
Redondo López

CVEs: INFORMACIÓN DE LAS VULNERABILIDADES DE...LO QUE SEA

● Todos los programas tienen vulnerabilidades

- Otra cosa es que se conozcan o no... 😳

● Pero las que se conocen...¡Son públicas! 😳

- ¿No me crees? Mira la imagen
- Más que la explicación, **mira la puntuación**
- A más puntuación (0 a 10), más grave es 😳

● Estos problemas se arreglan actualizando

- ¿Entiendes ahora por qué es importante actualizar? 🚀

● Pues los dispositivos “Smart” tienen tendencia a no hacerlo 🤖

- O a quedarse sin actualizaciones muy rápido ←
END
- No compres marcas “raras”: ¡Tienden a no actualizar nada!

Blizzard : Security Vulnerabilities, CVEs

Published in: ⏪ 2024 January February March April May June

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9 In CISA KEV Catalog

Sort Results By : Publish Date ↑↓ Update Date ↑↓ CVE Number ↑↓ CVE Number ↑↓ CVSS Score ↑↓ EPSS Score ↑↓

Copy

CVE-2020-27383

Battle.net.exe in Battle.Net 1.27.1.12428 suffers from an elevation of privileges vulnerability which can be used by an "Authenticated User" to modify the existing executable file with a binary of his choice. The vulnerability exist due to weak set of permissions being granted to the "Authenticated Users Group" which grants the (F) Flag aka "Full Control"
Source: MITRE

Max CVSS	EPSS Score
7.8	0.05%
Published	2021-06-09
Updated	2021-06-17

CVE-2017-14748

Race condition in Blizzard Overwatch 1.15.0.2 allows remote authenticated users to cause a denial of service (season bans and SR losses for other users) by leaving a competitive match at a specific time during the initial loading of that match.
Source: MITRE

Max CVSS	EPSS Score
5.3	0.17%
Published	2017-09-26
Updated	2017-10-06

CVE-2009-4768

Unspecified vulnerability in the JASS script interpreter in Warcraft III: The Frozen Throne 1.24b and earlier allows user-assisted remote attackers to execute arbitrary code via a crafted custom map. NOTE: some of these details are obtained from third party information.
Source: MITRE

Max CVSS	EPSS Score
9.3	3.08%
Published	2010-04-20
Updated	2017-08-17

3 vulnerabilities found

CVE Details (<https://www.cvedetails.com/>) es una de las páginas que muestra esta información (hay más). Busca en Google “<Nombre del programa> vulnerabilities CVEDetails” y puedes alucinar



SHODAN: UN MOTOR DE BÚSQUEDA DE...COSAS

● Los dispositivos inteligentes suelen estar por ahí expuestos

- No es la primera cámara de vigilancia que está visible sin clave de acceso...

● Se localizan con motores de búsqueda de “cosas” como Shodan

- Que también funcionan con cualquier web
- Miras la dirección IP de esa web aquí
 - La IP es como el DNI de cualquier página web (si te mola esto, mírate el **F-83 “Numancia”**)
 - <https://www.nslookup.io/website-to-ip-lookup/>
- Y la buscas aquí: <https://www.shodan.io/dashboard>

● Te pueden aparecer sus vulnerabilidades y CVEs conocidos

- Que se pueden buscar gratis...¿lo captas? Hack!

Puedes buscar información de vulnerabilidades de cualquier web en Internet con este programa. Puedes registrarte (gratis) y te dejará hacer más cosas, pero gratis puedes buscar una IP...encontrarte una página de hacking plebeyos



ESPERA, ESPERA...¿Lo ESTOY ENTENDIENDO BIEN?

● Voy a intentar resumírtelo para ver si lo has pillado ☺

- Todos los defectos de seguridad (vulnerabilidades) de la gran mayoría de programas “populares” **son conocidos y están disponibles en una web pública**
 - Mucha gente que son “secretos de estado” o algo así 😱, pero que va, todo lo contrario
 - Cada defecto tiene un “DNI” (un identificador único y exclusivo) que **se llama CVE ID**
 - Hay motores de búsqueda (como Shodan) que te dan información de las máquinas
 - ¡Incluidas **sus vulnerabilidades conocidas (y sus CVE)**!
 - Es decir, **deja a la vista las vergüenzas de cualquier máquina del mundo** 😳

● ¿Sabes que eso es aún peor de lo que crees?

- También existe una web (pública y legal) donde puedes descargarte **todos los exploits conocidos**
- Esos son programas que se han creado para “**sacarle partido**” a una vulnerabilidad 😊
- Y sí, efectivamente los exploits llevan asociado el CVE de la vulnerabilidad que explotan
- Vamos, que son ataques que seguramente funcionan contra toda máquina del mundo que tenga una vulnerabilidad con ese CVE 😳

● ¿Entiendes ahora por qué hay que actualizar para solucionar vulnerabilidades?

- Si quieres investigar más de esto, consulta la **F-83 “Numancia”**



José Manuel
Redondo López

¿CREEES QUE LO HAS ENTENDIDO TODO? ¡AUTOEVALÚATE!



● Asegúrate de haber entendido lo siguiente

- **Redes**
 - Que algunos juegos online son un “coto de caza” para gente degenerada, y que tienes que tener mucho cuidado con lo que te piden en ellos porque no sabes quién está detrás realmente de cualquiera avatar que veas
 - El “lado oscuro” de la asistencia remota, y para qué pueden usarlo los delincuentes
 - Que no debe hacer caso a alguien que le pida que use esta funcionalidad
- **Dispositivos “Inteligentes”**
 - Que todas las vulnerabilidades de programas y productos conocidas son información pública, y que encima puedes saber lo graves que son porque están puntuadas de 0 a 10
 - Para que sirve un motor de búsqueda como *Shodan* y la información que te da para saber si algo es o no vulnerable

[< Ir al Índice](#)



SEGURIDAD “EN LA CALLE”

Seguridad más allá del ciberespacio



[Seguridad Física >](#)

[Seguridad Financiera >](#)





José Manuel
Redondo López

¿QUÉ TE VAS A ENCONTRAR EN ESTE BLOQUE?

- En este bloque de seguridad sobre cosas que te pueden pasar a ti como persona en el día a día te voy a enseñar...
 - Que las siglas QR realmente significan Quita (el teléfono) Rápido ☺
 - Que **pinchar un USB** de por ahí es lo mismo que pincharte con una jeringuilla que veas tirada en la calle, pero para tu PC
 - Que hay **mucho desgraciado en la venta de segunda mano** por Internet
 - Que los hay gente **profesional de la estafa** que te come la cabeza para que pagues de manera que no puedas deshacer el pago, y las movidas que inventan para eso
- *¿Te molan estas movidas de estafas dentro y fuera del ciber-mundo? ¡Pues si quieres saber más mírate ésta!...*
 - O mi canal de YouTube de estafas: <https://www.youtube.com/@j.m.redondo8618/featured>





Seguridad “Física”

Seguridad para ti y el entorno que te rodea





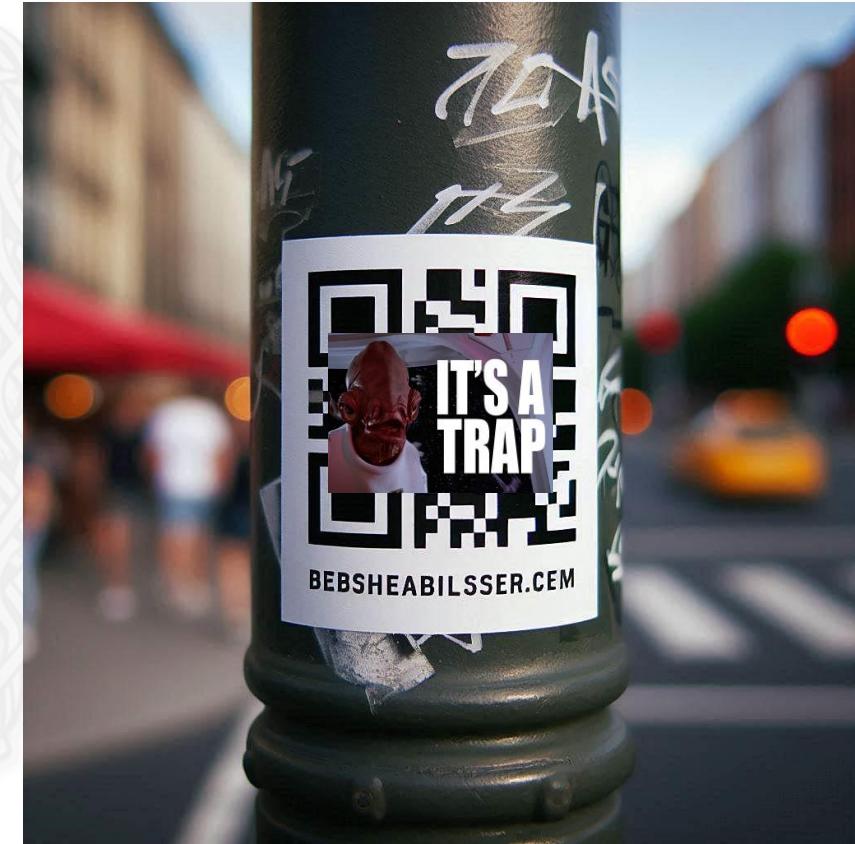
CÓDIGOS QR

- *¿Sabes que hay delincuentes que ponen QR maliciosos por la calle?* 💣

- ¡No los escanees con tu teléfono ni de coña!

- *¿Y a dónde te llevan? A páginas web...*

- **Falsas** 🕵️ : Te engañan para que metas datos privados (Ej.: tu cuenta del LOL) y robártelos
 - **Con un ataque Drive-by download** 🗑️ : Te comes un virus solo por visitar la página (exacto, sin que hagas nada)
 - Sobre todo, si tienes el navegador sin actualizar
 - Pero, aunque lo tengas **¡no te la juegues!**
 - A veces hay delincuentes que **los pegan encima** 📋 de los que hay en museos, restaurantes... ¡mucho ojo!
 - Si parece repegao, mantén el teléfono alejao



**¡Tranquis! Este me lo generó una IA gratuita
(Microsoft Copilot),
<https://www.bing.com/chat?q=Microsoft+Copilot&FORM=hpcodx>), no es de verdad :P**

EL PELIGRO DE LOS USB



José Manuel
Redondo López

● ¿Te has encontrado un USB tirado por ahí?

- Pues lo tratas como 🚨 material radioactivo 🚨



● ¡Hagas lo que hagas no lo conectes a tu PC! Pueden tener

- **Virus de cualquier tipo** 💩, metido a propósito o en sus documentos
 - ¡No sabes por donde ha pasado!
- **Ser un Rubber Ducky o similar** 🧸 : Un falso lápiz USB que se hace pasar por un teclado y ratón
 - Con comandos preprogramados para hacer cosas
 - Como si usases un teclado y ratón conectados a tu PC, pero a toda leche
 - **Por ejemplo:** navegar a una web chunga y descargarse un virus
 - ¡Es como si le dijeses al delincuente tu teclado y ratón!
- **USB Killers** 💀 : Conectas al PC, mete un petardazo y te funde la placa
 - Literalmente una “bomba USB” para tu PC
 - A cambiar de placa y quien sabe que más: **No, no estoy de broma** 😞



Sí, hay delincuentes que se dedican a “sembrar” USB con “carga explosiva” y les ponen “etiquetas sugerentes” para que los enchufes (este no, lo generé con Copilot :D)



Seguridad Financiera

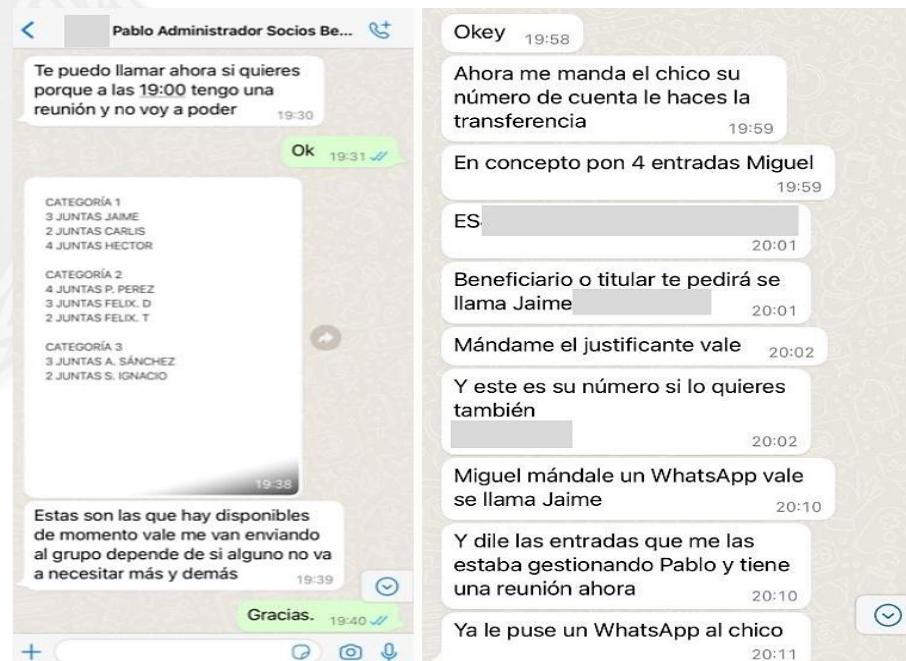
Manteniendo nuestras cuentas seguras



ESTAFAS EN COMPRAS DE SEGUNDA MANO

- El mercado de 2^a mano por Internet es la jungla 
 - Sin importar la página, hay estafas a punta pala, de lo que sea
- Pero todas tienen una serie de cosas en común para identificarlas 
 - El vendedor te cuenta una milonga para que te salgas de la plataforma a una aplicación de mensajería o similar 
 - Así ya no tienes derecho a reclamarle a la web de venta
 - Ej.: Vamos al WhatsApp que te hago un descuento porque así no pago la comisión a segundamano.es
 - Precios de derribo  : ¿Demasiado bueno para ser cierto? Pues lo es
 - Te imponen un medio de pago , que les va a beneficiar a ellos y tu no podrás reclamar (los vemos ahora)
 - Te cuentas movidas raras  . Ej.: ¿Te dicen que no están en España y luego te cuentan una historia? **Timo fijo**

Empezó a vender las entradas en una plataforma típica, y luego inventó una excusa para pasarse al “Grupo de WhatsApp de socios” del equipo de fútbol. Hecha la venta ahí, ya no tienes forma de reclamar a la plataforma, y te tienes que poner a denunciar, etc. Fuente: <https://maldita.es/malditobulo/20220526/entradas-final-champions-real-madrid-timo-estafa/>





José Manuel
Redondo López

MEDIOS DE PAGO INSEGUROS

- **PayPal como amigo, Western Union, MoneyGram, etc.** son formas de pago que usan muchos delincuentes 😠
- No son formas de pago delictivas, el problema es que **NO SON FORMAS DE PAGO PARA COMPRAS**
 - No tienen seguros ni garantías en forma de estafas
- **¿Qué son? Maneras de mandar dinero a amigos, que supuestamente conoces** 🤝
 - Si lo mandas, lo mandas, no tienes reclamación alguna
 - Te cobran menos comisión, **tienes menos garantías**
 - ¡Están pensadas para algo que no es comprar cosas en tiendas!
- **¿No me crees?** <https://maldita.es/timo/20231204/paypal-pago-amigos-familiares-donacion/>

← Tipo de pago

Guardaremos esta selección para todos los pagos a . Puedes cambiarla antes de enviar el pago.

Productos y servicios
Si el artículo cumple los requisitos y se pierde o se daña, recibirás un reembolso íntegro. El vendedor paga una pequeña tarifa.

[Más información sobre la Protección del comprador](#)

Amigos y familiares
La Protección del comprador no se aplica a este tipo de pago.

¡Esto no es algo malo! Solo que no vale para lo que crees...



José Manuel
Redondo López

¿CREEES QUE LO HAS ENTENDIDO TODO? ¡AUTOEVALÚATE!

?

● Asegúrate de haber entendido lo siguiente

- 😱 **Seguridad física**
 - Que no puedes fiarte de un código QR y que, por tanto, nunca debes escanearlo
 - La cantidad de peligros que puedes tener si conectas un USB a tu equipo y por qué debes evitarlo a toda costa
- 💰 **Seguridad financiera**
 - Los indicios de que una compra de segunda mano va a acabar en estafa fijo
 - Por qué hay servicios de pago que realmente no se podrían usar para hacer compras, dado que no te cubren en caso de incidentes

AVADA KEDAVRA: SIENDO UN HACKING BESTIA: TÉCNICAS DE ATAQUE

