

SOBREVIVIENDO EN LAS REDES SOCIALES



Campus Tecnológico-Deportivo para
Jóvenes

Universidad de Oviedo



JOSÉ MANUEL REDONDO LÓPEZ PROYECTO "F-31 'DESCUBIERTA'" v1.3



Organiza:
 Escuela de
Ingeniería
Informática
Universidad de Oviedo

Colaboran:

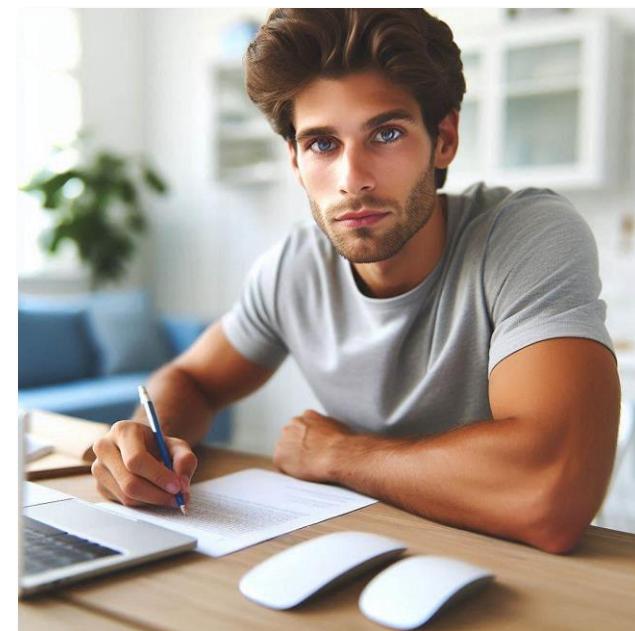
 CITIPA
Colegio Oficial de Graduados
en Ingeniería Informática e
Ingenieros Técnicos en Informática
Principado de Asturias

 COITPA
Colegio Oficial de
Ingenieros en Informática
Principado de Asturias

 Cátedra CAPGEMINI
PARA LA TRANSFORMACIÓN
DIGITAL SOSTENIBLE

¡BIENVENIDO!

- Esta es una presentación pensada para quien hace poco que se han metido en RRSS y no saben exactamente qué hacer
 - En ella te voy a intentar exponer los **peligros** a los que te puedes enfrentar
 - Y también formas de **defenderte** contra ellos
 - De manera que puedas **investigar contenidos y personas** y protegerte
- Las RRSS pueden ser un sitio donde aprendas y compartas mucho, hagas amigos y tengas muchos efectos positivos
 - ¡Pero no debes dejar que ningún incidente te arruine la experiencia!
- Ante todo, debes recordar que es una “ventana al mundo”
 - Y en el mundo hay muchos tipos de personas
 - Unos querrás tenerlos cerca...y **otros querrás espantarlos lo más lejos posible**



¿Estás listo para tomar nota y aprender? ☺



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"



Protección de Servidores y Aplicaciones Web

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

Rango 1
(Sargento)



Defensa contra el Cibercrimen

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



Rango 2
(Suboficial Mayor)



Identificación y Análisis de Vulnerabilidades en Web

Seguridad ofensiva:
Reconocimiento y Explotación
MUINGWEB, Microcredenciales.
TK-210 "красный октябрь"
(Octubre Rojo)



Protección de Servidores Web

Seguridad de infraestructuras para startups
Guías INCIBE, F-103 "Blas de Lezo"



Rango 3
(Capitán de Fragata)



Desarrollo Seguro de Software

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

Rango 4
(Almirante)





José Manuel
Redondo López

¿Y TODO EL RESTO DE MATERIAL?

- Durante este curso se hará mención a otros cursos complementarios que te regalo y que forman parte de la misma iniciativa
- Puedes encontrarlos todos aquí:
 - [https://github.com/jose-r-lopez/Formacion_-Seguridad_Joven/wiki/Contenidos-de-la-Iniciativa-%22Cobra-Kali%22-\(Capacitaci%C3%B3n-B%C3%A1sica\)](https://github.com/jose-r-lopez/Formacion_-Seguridad_Joven/wiki/Contenidos-de-la-Iniciativa-%22Cobra-Kali%22-(Capacitaci%C3%B3n-B%C3%A1sica))
- También tengo pensado en el futuro subir videos explicando cada curso en mi canal de YouTube
 - <https://www.youtube.com/@JoseRedondo-dj7xk>



ÍNDICE

- 🧟 [¿Para qué vale una red social?](#)
- 💰 [¿Es realmente gratis una red social?](#)
- 😬 [¿Cómo me “enfrento” a una red social?](#)
 - 🖊 [Configurar una red social](#)
 - 😷 [Precauciones usando una red social](#)
- 😕 [¿Qué pasa con la información que pongo en RRSS?](#)
 - 😢 [La persona detrás de una cuenta de una red social](#)
- 🚪 [Precios en la dark web de los datos que nos roban](#)
- ➔ [Más información...](#)



👻 ¿PARA QUÉ VALE UNA RED SOCIAL?

Pensemos en los usos que le podemos dar...



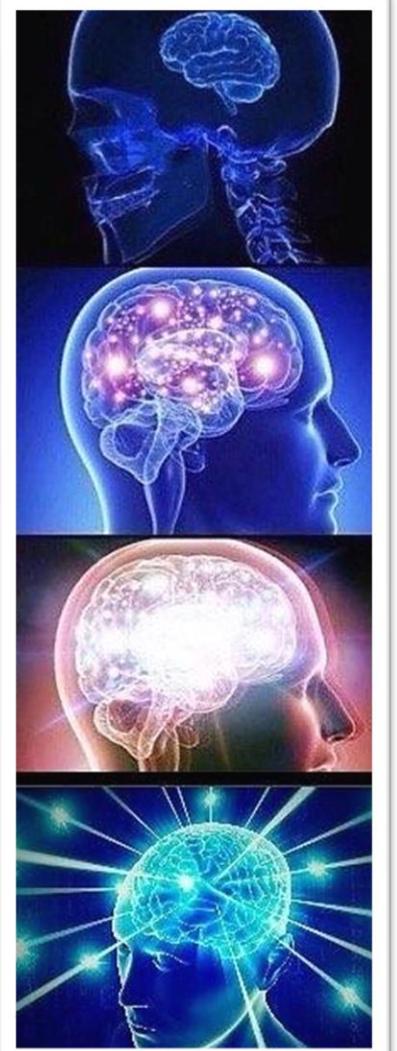
¿QUÉ TE VAS A ENCONTRAR EN ESTE BLOQUE?



- *• ¿Alguna vez te has parado a pensar en los pros y contras de una red social?*
 - Pues yo te los voy a explicar aquí ☺
- *• ¿Te has parado a pensar que en las redes sociales hay tanto gente buena como gente mala, que aparentemente quiere ser amigo tuyo, pero su intención es otra?*
- Pues en esta sección te quiero poner un poco al tanto de qué tipo de gente solo te quiere por el interés y lo que puede sacar de ti
- Además de advertirte de que con esto de la inteligencia artificial vas a tener que mirar todo varias veces
 - ¡Porque las formas de engañarnos están avanzando mucho!

¿PARA QUÉ VALE UNA RED SOCIAL?

- *¿Alguna vez os habéis parado a pensar para qué vale una red social?*
- ¡Seguro que sí! Pero...igual no habéis pensado en todos los “usos” que se le pueden dar
- Vamos a repasar los más típicos...
- ...y también vamos a ver cómo cada uso positivo tiene un...“lado oscuro” (**¡para saber cómo protegernos!**)



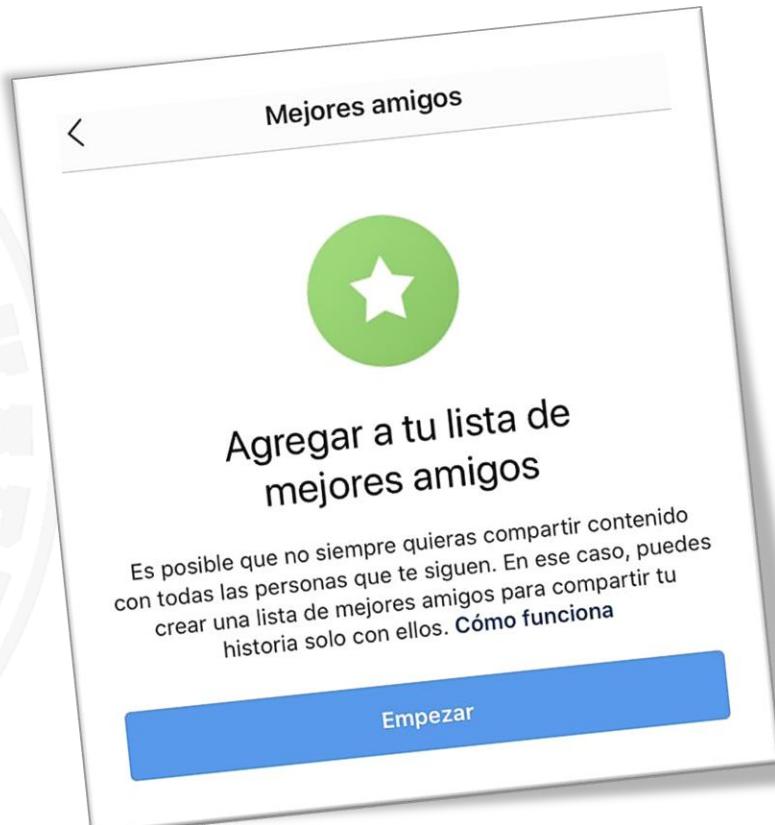
¡HACER AMIGOS!



José Manuel
Redondo López

- Darte a conocer a otras personas es el principal uso de una red social
- ¡Puedes tener amigos en todo el mundo!
 - En mi época (cuando los dinosaurios dominaban la tierra) eso se hacía en un banco de un parque
- Conoces a otras personas con gustos, aficiones, hobbies... en común contigo

¡Y eso es genial!

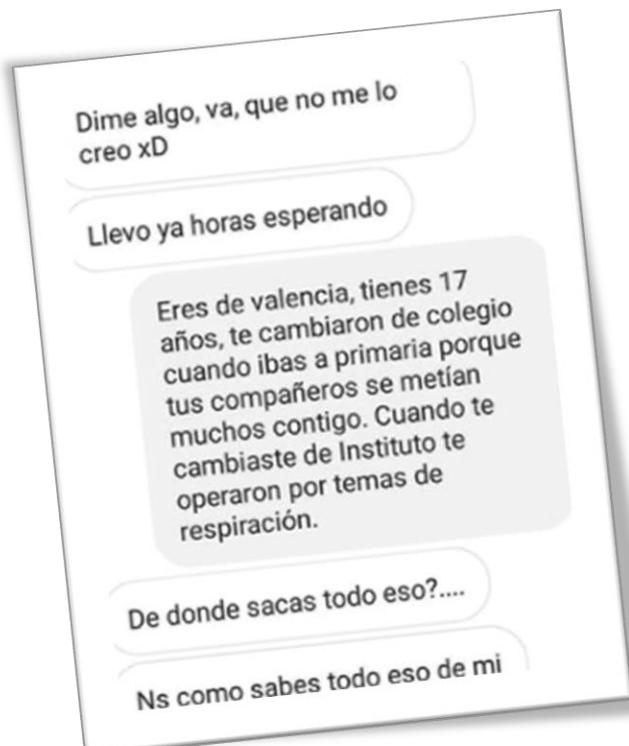


¿HACER “AMIGOS”?



José Manuel
Redondo López

- Pero poder hacer amigos en todas partes tiene también su parte menos buena
- A veces hay cierto tipo de gente no recomendable...
 - No son quienes dicen ser (**suplantan** a otras personas)
 - Son bromistas / trolls /
 - Ofrecen una imagen de sí mismos que no es la real
 - No conoces a una persona, **¡conoces a un personaje!**
 - O, en realidad sólo quieren “**venderte**” algo
 - No necesariamente que compres cosas (loot boxes, gachas,...)
 - También que pienses como él/ella...



¡Que no te “coman la cabeza”!

¡COMPARTIR IDEAS, TRABAJOS...!

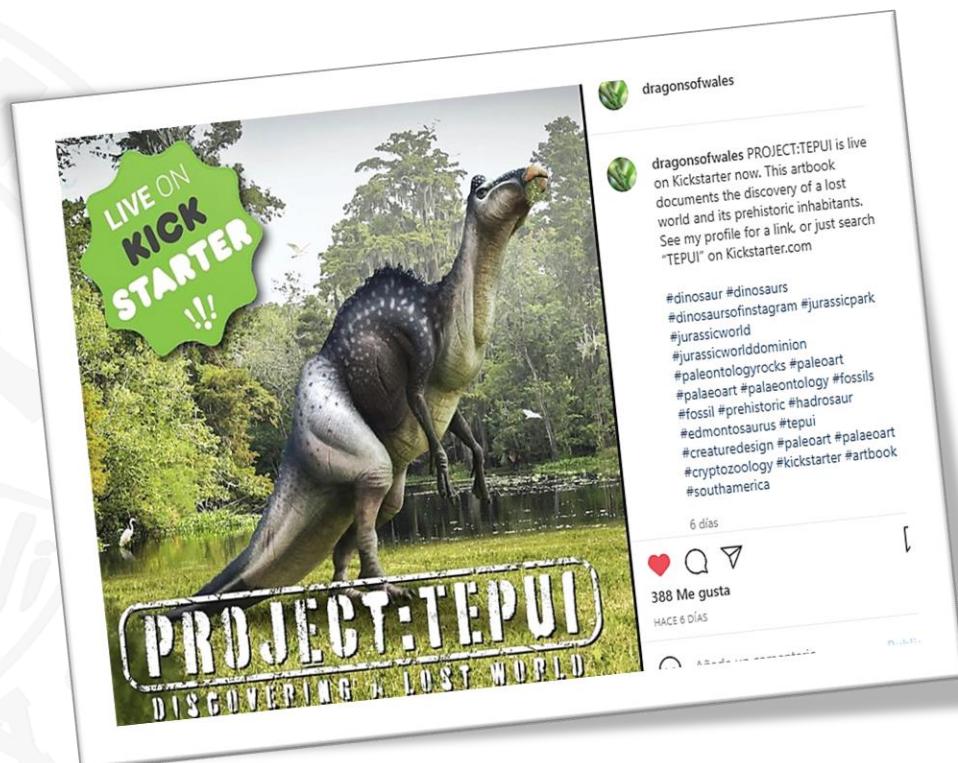


José Manuel
Redondo López

- Seguro que eres alguien con cosas que decirle a los demás, expresarte, compartir...

- Ideas
- Trabajos artísticos o de cualquier tipo
- Tus hobbies (y lo que haces)
- Tus deportes / aficiones y cómo las practicas (resultados, premios...)
- ...

¡Y eso es genial!



¿“COMPARTIR” IDEAS, TRABAJOS...?



José Manuel
Redondo López

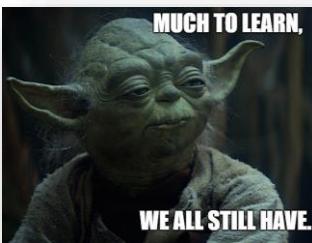
- Pero si compartes cosas de ti mismo, hay que tener en cuenta que...

- Si son obras artísticas de cualquier clase, alguien se las puede **apropiar, robar, decir que son tuyas...**
 - Es importante firmar cada cosa que uno hace
 - ¡Investiga las marcas de agua!
- Los **trolls y las críticas** pueden aparecer fácilmente
 - Hay gente **MUY ABURRIDA** en la vida
 - Criticar por deporte, placer o porque necesita “casito”

¡Hay que estar preparado para resistir a los envidiosos! (de tu Nvidia nace mi fuerza ;))



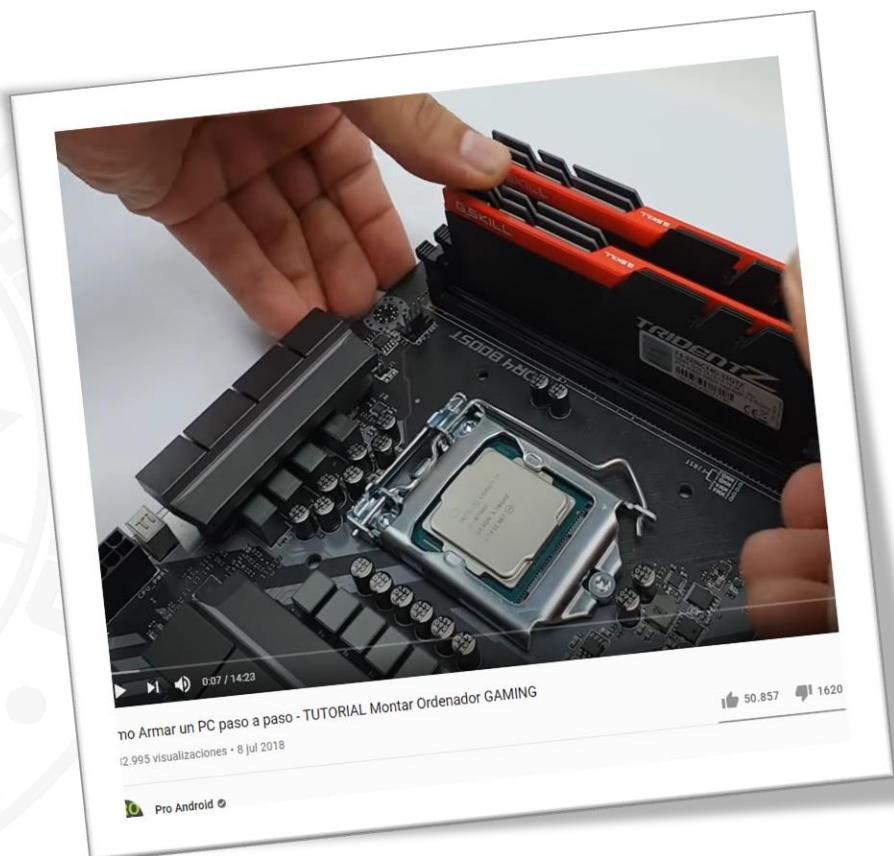
¡APRENDER COSAS NUEVAS!



José Manuel
Redondo López

- Internet es **EL SITIO** para aprender cosas nuevas
- Wikipedia, YouTube...**TODA** la información de **TODAS** las cosas que puedes imaginar...
 - ¡Está ahí, a tu alcance!
- Hay cursos y tutoriales en video de lo que quieras, cuando quieras...
- Normalmente, es mucho más fácil de aprender que leerlo en un libro ☺

¡Y eso es genial!



“APRENDER” COSAS ¿NUEVAS?



José Manuel
Redondo López

- El problema es que tienes que fiarte de tus “maestros”
- En Internet hay mucho “maestrillo” que te cuenta una historia
 - O se hace pasar por experto y en realidad... **a lo mejor no lo es**
- No han pasado un proceso de selección...
- También hay mucha “noticia falsa” (fake news) para que te creas bulos
 - ¡Y así conseguir manipularte! ¡NO LO PERMITAS!



¡No hay que creer todo lo que uno lee, hay que contrastar las cosas y, si tienes dudas, pregunta a tu familia/ profes siempre!

¿Cómo se pueden detectar?

LAS FAKE NEWS

Compartimos una serie de buenas prácticas con las que detectar los bulos y noticias falsas:

1| Busca la fuente y contrasta

Una noticia real siempre va a estar bien redactada. Se identificará al autor y tendrá fuentes en las que apoyarse para sustentar la noticia.

Si recibimos una noticia sin fuente o con una de poca fiabilidad, lo mejor será desconfiar. **¡Sin fuente, no compartas!**

Una buena práctica es comprobar la noticia a través de un buscador y contrastar con otras fuentes.



2| Revisa la URL

A veces este tipo de noticias falsas puede llegar a través de enlaces que se deben revisar:

- **Analiza la URL** para ver si se trata de un servicio legítimo o por el contrario se trata de una suplantación.



- Comprueba que la URL dispone de **certificado de seguridad** que se corresponde con la página y empieza por **HTTPS**.

3| Mira más allá del titular

Los titulares de las noticias falsas suelen ser sensacionalistas y muy llamativos.

Suelen apelar a las emociones para generar interés en redes sociales. Un rápido vistazo al interior del contenido servirá para desenmascararlas.



4| Comprueba el formato

El cuerpo de la noticia puede estar mal redactado, con faltas de ortografía y fotografías o imágenes de mala calidad.

Una **búsqueda inversa** de las imágenes puede desvelar manipulación o un mal uso de estas.



is4k INTERNET SEGURA FORKIDS

Si quieras poner a prueba tu radar, en la campaña sobre alfabetización mediática publicada en la web de is4k, encontrarás varios recursos que podrás utilizar.

www.is4k.es

5| Aplica el sentido común

Lo más importante es ser **neutral** y no dejarse llevar por la temática ni por el contexto. Es fácil dejarse llevar por las emociones a la hora de interpretar una noticia.



6| Analiza si es una broma

En ocasiones se confunden con bulos aquellas noticias satíricas que buscan parodiar un hecho.

Si busca ironizar una noticia o burlarse de algo en tono de humor, probablemente sea una broma y no un bulo real.



OSI Oficina de Seguridad del Internauta

En la web de la OSI, encontrarás ejemplos de **fake news** reales que han circulado por Internet, como es el caso de los **anuncios con imágenes de famosos**.

www.osi.es

¿Cómo denunciar?

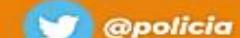
LAS FAKE NEWS

Existen diversas herramientas, páginas web e incluso bots en aplicaciones de mensajería instantánea que se dedican a **desmentir este tipo de bulos** y que también pueden utilizarse para contrastar la información.



Las redes sociales incorporan sus propios medios para luchar contra las noticias falsas y el contenido inapropiado.

También se puede consultar y denunciar a través de los perfiles en Twitter de la Policía Nacional o de la Guardia Civil.



Finalmente, **INCIBE** pone al servicio de los usuarios su **Línea de Ayuda en Ciberseguridad 017**, un teléfono gratuito y confidencial disponible todos los días del año al que puedes llamar en caso de duda.



¿LO DE LAS FAKE NEWS NO SE VA A VOLVER UNA JUNGLA CON LA IA?

- Me temo que sí 😞, es la era de los **deepfakes**
- Las IAs ya permiten generar videos de quien quieras, haciendo lo que quitas y hablando con el tono de voz que quieras...
 - Si un conocido te pide algo raro, llámale y confírmalo ¡Se paranoico/a!
 - Mucha gente tiene **una “contraseña” con sus amigos** para prevenir estas cosas
 - Si el que te llama no la sabe, no es él, aunque tus ojos y oídos de elfo te engañen (sí, estamos así ya...)



Pistas para detectar una deepfake

incibe OSi Oficina de Seguridad del Internet

- Desconfía de videos con efectos sensacionalistas, alarmantes o que apelan a las emociones
- Busca cosas extrañas, como sombras que no cuadren con la iluminación
- Examina el rostro, la piel o la frecuencia del parpadeo del personaje
- Sospecha si el audio no concuerda con lo que transmite la imagen, no corresponde con la persona que habla o no está sincronizado
- Fijate en la duración, suelen ser cortos para minimizar los posibles errores de edición

! No compartas nunca sin antes contrastar

#OSiconsejo www.incibe.es/ciudadania

Financiado por la Unión Europea NextGenerationEU

Gobierno de España Ministerio de Ciencia, Innovación y la Función Pública

Plan de Recuperación, Transformación y Resiliencia

España | digital 20/26 017

Pistas para identificar fake news

incibe OSi Oficina de Seguridad del Internet

- Verifica la fuente y busca la noticia en otras fuentes para corroborarla
- Examina la URL para comprobar si se trata de un sitio seguro
- No te dejes llevar por títulos sensacionalistas, alarmantes o que apelan a las emociones
- Revisa el formato del contenido en busca de errores ortográficos e imágenes de mala calidad
- Apóyate en herramientas de verificación para comprobar (fact-checking) la autenticidad de la noticia

! No compartas nunca sin antes contrastar

#OSiconsejo www.incibe.es/ciudadania

Financiado por la Unión Europea NextGenerationEU

Gobierno de España Ministerio de Ciencia, Innovación y la Función Pública

Plan de Recuperación, Transformación y Resiliencia

España | digital 20/26 017

"APRENDER" A SER ¿UN GANADOR? COACHES ONLINE

● Últimamente circula por RRSS este perfil de "coach"

- Persona de (supuesto) **éxito** que critica "al sistema"
 - Todo es un engaño para mantenerte pobre...menos él/ella
- Te promete salir de él **haciéndote rico** con alguna historia
- **Te vende un curso** o pertenecer a un "club" o "universidad" que te enseñará "cosas que te sacarán de la Matrix"
- Te dicen que tú también puedes ser de su "**élite**" y salirte de la masa social de "plebeyos"

● Pero algunos son "fake news"

- **No son ricos**, es todo apariencia / alquiler
- Su sistema realmente **no funciona**, solo es una forma de hacerse rico vendiéndote un curso
 - Son **esquemas piramidales** que "revientan" pasado un tiempo
- **Te aíslan** de tu familia/amigos/toda "la plebe" que no tenga "mentalidad de ganador"
 - Y "te critique por envidia / no vibra con tu frecuencia / etc."
 - Solo vas a ser su víctima más fácilmente



Los coches, las casas y las apariencias se pueden alquilar. Si es rico ¿Por qué vende cursos? ¿Por ayudarte? Entonces no te cobraría (yo no soy rico, no tengo Lambos, y no te cobro por este curso ☺)



José Manuel
Redondo López

¿QUÉ ES ESO DE UN ESQUEMA PIRAMIDAL?

- *¿En pocas palabras?* Un sistema donde para ganar algo tienes que convencer a otros para que se metan en él
- Porque lo que tú ganas se paga con lo que otros pagan (en FIAT o en criptos...)
 - “Revientan” en cuanto deja de haber nuevos ingresos (y pasa siempre)
- Solo ganan unos pocos de la pirámide
 - Los de la “cabeza” (los que la crearon, vamos)
- *¿Te ofrecen muchas ganancias, pago por “reclutar”, pagar por trabajar o te intentan deslumbrar con promesas?*
 - Es un esquema de estos, ¡no tengo pruebas ni tampoco dudas!

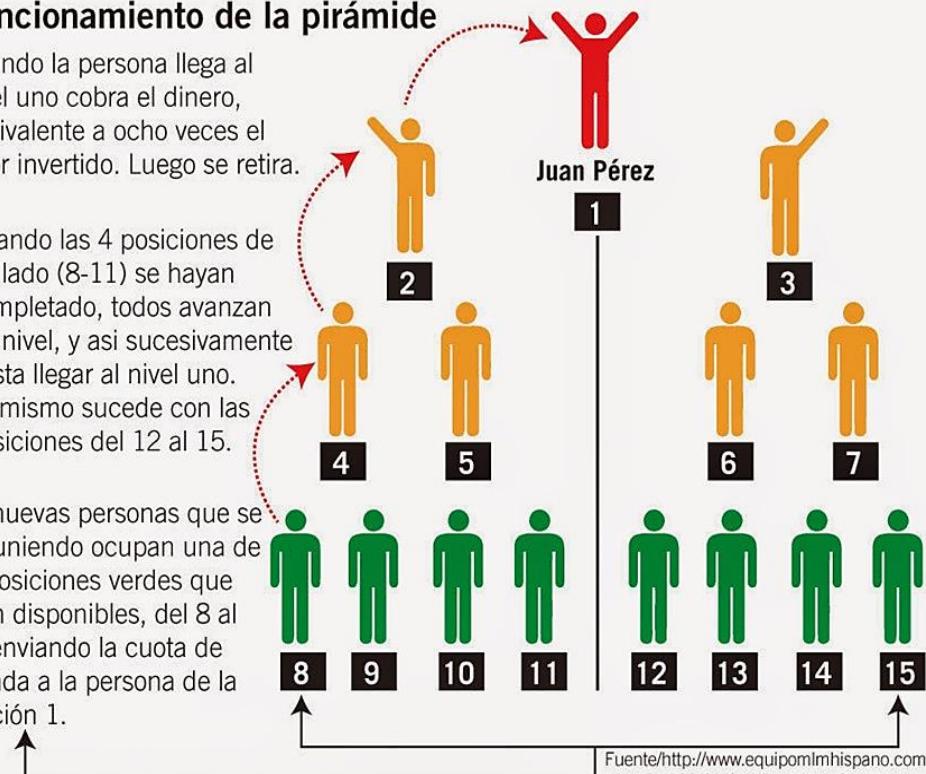


El funcionamiento de la pirámide

C Cuando la persona llega al nivel uno cobra el dinero, equivalente a ocho veces el valor invertido. Luego se retira.

B Cuando las 4 posiciones de un lado (8-11) se hayan completado, todos avanzan un nivel, y así sucesivamente hasta llegar al nivel uno. Lo mismo sucede con las posiciones del 12 al 15.

A Las nuevas personas que se van uniendo ocupan una de las posiciones verdes que estén disponibles, del 8 al 15, enviando la cuota de entrada a la persona de la posición 1.



Fuente/<http://www.equipomlhispano.com/gc/angel100/Gráfico/Ramón L. Sandoval>

Estos esquemas siempre acaban mal, y para que unos ganen tiene que estafar a otros. Fuente:
<https://es.linkedin.com/pulse/estafa-con-esquema-piramidal-tragos-en-c%C3%A1psulas-alejandro-falco>

¿CREEES QUE LO HAS ENTENDIDO TODO? ¡AUTOEVALÚATE!

?

- *¿Te ha quedado claro para qué puedes usar una red social en tu día a día, y que sea algo útil y productivo?*
- *¿Te ha quedado claro también qué tipo de contenidos son perjudiciales o pueden suponerte un problema?*
- *Has entendido que la desinformación o fake news hoy en día es un problema muy grave?*
- *Y que este problema se va a ver agravado todavía más por la aparición de los deepfakes?*
- *Entiendes que toda persona que te oferte algo donde tengas que pagar, o suscribir a más gente, es un esquema que te mete en una estafa?*



¿ES REALMENTE GRATIS UNA RED SOCIAL?

¿De verdad todo esto no cuesta dinero?



¿QUÉ TE VAS A ENCONTRAR EN ESTE BLOQUE?

- *¿Nunca te has parado a pensar por qué descargar una aplicación de una red social es gratis?*
 - Sobre todo, teniendo en cuenta lo que debe costar mantener algo con tantísimos usuarios en marcha...
- En esta sección te voy a intentar explicar cómo pagas por el uso de estas redes sociales, aunque no salga ni un euro de tu bolsillo
 - En realidad, sale ¡pero no como te imaginas!
- Y es que al final lo que vendemos en las redes sociales es a nosotros mismos y nuestros gustos, y aquí verás por qué
- También te enseñaré cómo algunos intentan provocarte para generar visualizaciones y dinero



LAS REDES SOCIALES... ¿SON GRATIS?



José Manuel
Redondo López



• ¿En el sentido de no pagar por usarlas? La mayoría sí, son gratis

- Pero el motivo es que “**cobran**” de otro sitio...
- Aunque últimamente hay mucha **suscripción “premium”** con diferentes excusas o supuestas ventajas

• ¿Cómo dices?

- Sí, en realidad ganan cantidades **ENORMES** de dinero

• ¿Pero cómo? ¿De manera ilegal?

- ¡NOOO! **Con tus datos**, vendiéndolos a **empresas de anuncios**

• ¡Eh! ¡Pero yo nunca les di permiso para eso!

- En realidad, **sí lo hiciste**, al hacerte una cuenta...
- ¿Te leíste el “tocho” que te salió de “términos y condiciones”? (No, yo tampoco ☺)



COMO CONOCÍ A VUESTRA MADRE, PADRE, AFICIONES, AMIGOS...

- Veamos ahora de donde viene la frase “**Si algo es gratis, tú eres el producto**” aplicada a las RRSS
- Lo primero de todo, voy a enseñaros un anuncio de mi propio Instagram
 - Se trata de una figura ultra-realista (bueno, vale, el color no...) de un Smilodon Populator, un tigre de dientes de sable



COMO CONOCÍ A VUESTRA MADRE, PADRE, AFICIONES, AMIGOS...

• *¿Cómo sabe mi Instagram que me gusta la prehistoria?*

- Mucho, la verdad, ¡ha acertado de pleno! ☺

• Lo primero...

- Los asistentes como Siri, el asistente de voz de Google, Cortana, Alexa... **SI TE ESCUCHAN** (En tu teléfono, PC, aparatos varios en casa...)

- Pero es que lo necesitan para funcionar (se activan con “frases clave”)
- ...y para **mostrarte anuncios**

- <https://www.lavanguardia.com/tecnologia/20180504/443209404047/google-escuchas-telefono-espionaje-privacidad.html>

- Puedes **desactivarlos, pero perderás opciones**

- <https://www.xatakandroid.com/tutoriales/como-desactivar-asistente-google>

- Otras aplicaciones del móvil **NO TE ESCUCHAN**

- Salvo que les **permitas usar tu micrófono** (permisos concedidos al instalarla)

- No, no le grito al móvil “¡me gustan los animales prehistóricos!”
 - ¡Pero es que no lo necesitan!

- Y entonces...*¿cómo lo hacen las empresas?*



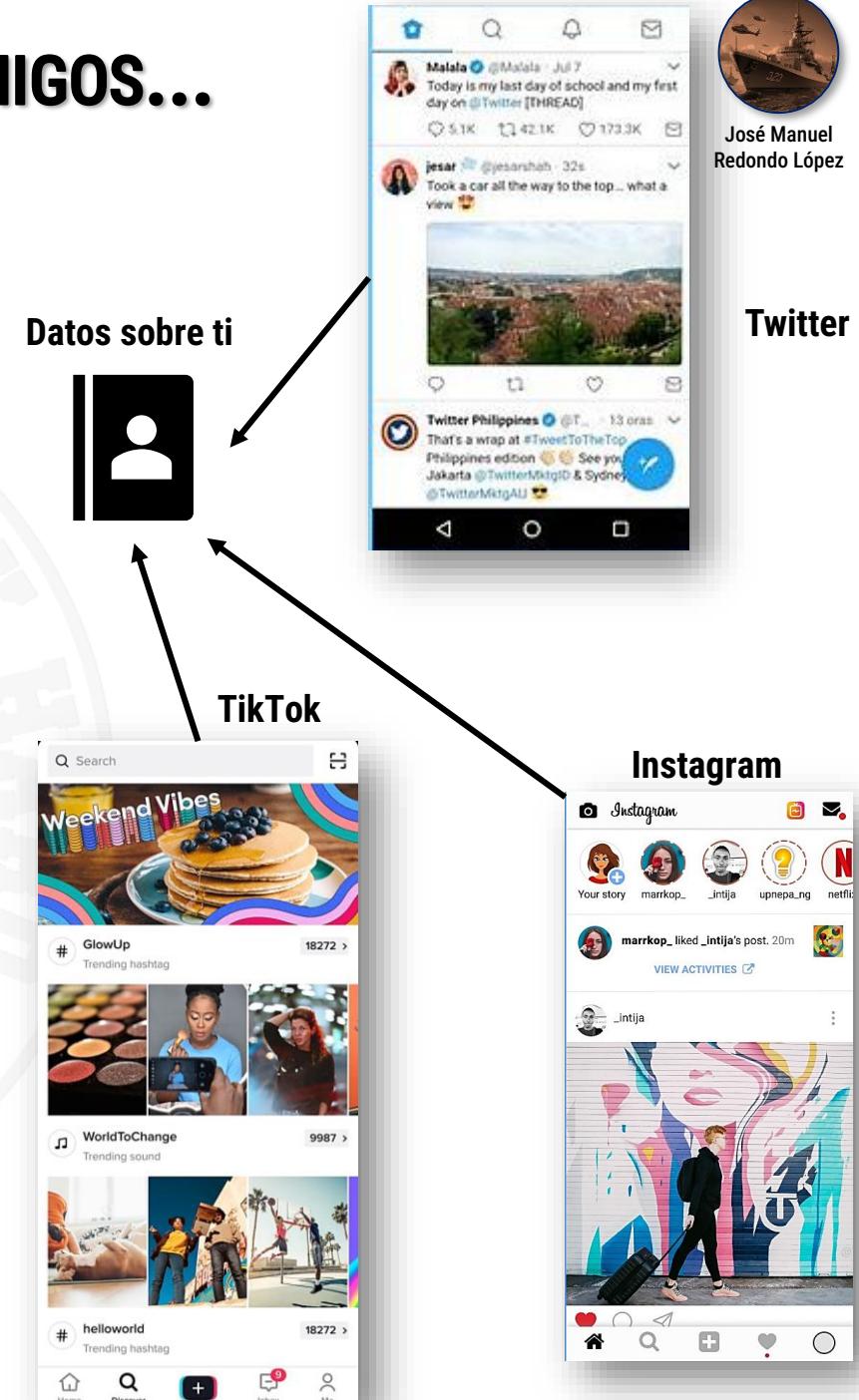
COMO CONOCÍ A VUESTRA MADRE, PADRE, AFICIONES, AMIGOS...



José Manuel
Redondo López

• **TODAS** las aplicaciones de redes sociales recogen datos de tu teléfono

- Tantos como permisos les des...
 - Pero, aunque les des los mínimos, lo hacen ☹
- **Tu ID de teléfono** (todos los teléfonos tienen un ID distinto)
 - Sí, no eres tú directamente, pero es TÚ teléfono ¿me sigues?
- **Tu localización** (más o menos aproximada)
- **Predice tu rango de edad**
 - Por lo que haces / sigues / “faveas”...
 - Hay **muchísima investigación en esto**, lo creáis o no...
- ... (muchos más datos útiles para identificarte, imposibles de listar aquí todos)





José Manuel
Redondo López

COMO CONOCÍ A VUESTRA MADRE, PADRE, AFICIONES, AMIGOS...

- Hay una serie de empresas que trabajan de “aspiradoras de datos” (como Kirby ☺)

- Se les suele llamar “data brokers”
- A esta venta de datos se la llama “data capitalism”

- Pagan por sacar datos de DONDE SEA

- Participas en un concurso, te suscribes a algo, usas un descuento, canjeas un vale...
- Cualquiera de esas acciones genera datos que reciben y tratan de asociarlos a ti
 - Cuando digo DONDE SEA es realmente DONDE SEA, en serio, ¡es alucinante!

- ¿Pero cómo? Ahí está el truco, TODAS las empresas les VENDEN esos datos

- Y luego los “cruzan”...y con eso ¡SABEN UN MONTÓN DE COSAS DE TI!

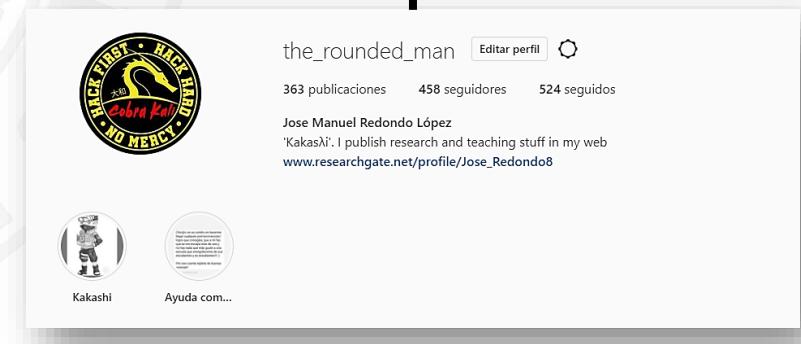
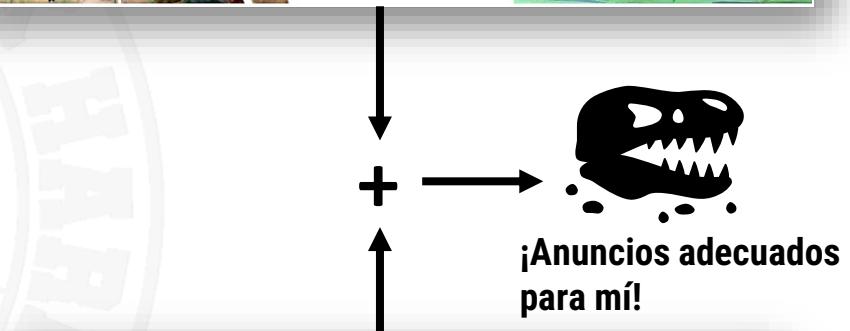


COMO CONOCÍ A VUESTRA MADRE, PADRE, AFICIONES, AMIGOS...

- *¿Y cómo saben que a mí me gustan las figuras prehistóricas ultra-realistas?*

- Pues porque de vez en cuando **compro alguna** a alguna tienda...
- En esta tienda **he dado mi dirección de correo electrónico** en el registro
 - (Y acepté los términos y condiciones)
- Y esa dirección es justo **la misma** que usé en Instagram (¿tenéis muchas direcciones? Yo no...)
- Y muchas empresas tienen “sondas” para **saber por qué webs navego** y lo que miro en ellas
- Y entonces la app Instagram sabe que ese usuario “anónimo” del teléfono cuyo ID es X y su correo es Y (anonimizado), compra figuras prehistóricas
 - ¡Todo juntando datos míos de distintos sitios!

Las webs a las que navego...



Las cosas que posteo en RRSS...

COMO CONOCÍ A VUESTRA MADRE, PADRE, AFICIONES, AMIGOS...

● Pero...¡hay más, mucho más!

- Yo **sigo a cuentas** de marcas de estas figuras, y faveo / retwitteo cosas que me gustan
 - Y de gente que habla sobre sus nuevos lanzamientos, hacen críticas de ellos...
- Y me gustan **sólo de ciertas marcas**, porque es fácil saberlo si analizas lo que hago
- Y como lo hago en mi Twitter / Instagram...ellos tienen estos datos (¡son tuyos!)

● ¿Qué anuncios me vas a poner entonces?

- De figuras prehistóricas
- De las marcas que más me gustan
- Pero no es necesariamente “malo”, ¿sabéis?
 - Así me entero de las novedades
 - Y de vez en cuando compro...
 - ¡La marca de figuras **ha pagado a la red social** para colocar esos anuncios “inteligentes”!
- **Y así...ganen dinero** (porque se hace con todo el mundo en todo el mundo ☺)
- Esta “**publicidad dirigida a cada persona individual**” funciona **MUY BIEN**, y las marcas lo saben
 - ¡Este es el imperio que rige Internet hoy en día! 😊

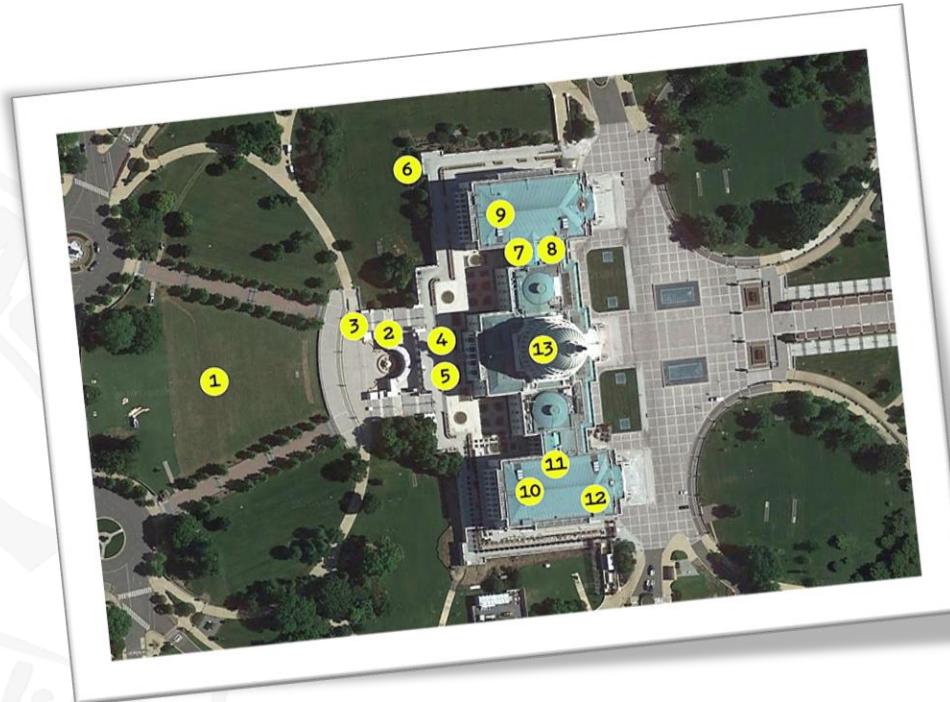




José Manuel
Redondo López

COMO CONOCÍ A VUESTRA MADRE, PADRE, AFICIONES, AMIGOS...

- ¿Te parece alucinante? Espera...
- Antes he dicho que pueden saber tu **geolocalización** (dónde estás en el mundo)
 - Pero también saben la de **TODOS** los móviles...
 - Y con eso, por increíble que parezca, pueden saber qué teléfonos están regularmente cerca de ti
- Y si es en una casa, en un colegio, en un gimnasio...porque...**¡Google Maps!** ☺
 - Es decir, ¡pueden reconstruir todo mi entorno social y mis rutinas!
 - Familia, amigos, compañeros de clase...



Esta imagen es real, y corresponde a personas durante el asalto al capitolio según sus móviles. ¡Supieron por dónde se movían en todo momento! ¿Cómo creías que los asistentes saben cosas como "tu casa", "tu instituto", etc.?

COMO CONOCÍ A VUESTRA MADRE, PADRE, AFICIONES, AMIGOS...

- Y con eso, las RRSS empezarán a mostrarme a mí anuncios de cosas que le interesan a “mi gente”
 - Sí, ya sé que lo que les interesa a tus colegas no tiene por qué interesarte a ti...
 - Y gente que me stalkee sabe por dónde me muevo, lo que me gusta, mis rutinas, mis colegas...
 - ¡Depende de cuanto posteé!
- Pero...igual así un día hablo de ello con alguien de mi entorno al que **SÍ LE INTERESA**
 - ¡Y le hago “publi” gratis!
 - Is this...¿*publicidad subliminal*?
 - ¡**NO**! Pero...a lo mejor sin querer te conviertes en “embajador” de una marca





José Manuel
Redondo López

COMO CONOCÍ A VUESTRA MADRE, PADRE, AFICIONES, AMIGOS...

● Pero ¿creéis que solo pasa en las redes sociales?

- ¡NO! ¡Prácticamente cualquier web con anuncios lo hace!
- Y ¿no te aparecen en las RRSS “post promocionados”?
- ¿De dónde crees que salen? ¡Ahora lo sabes!

● ¿Y esto no le importa a nadie?

- Pues en realidad, parece que no...
- Tiene nombres “guays” para que la gente lo vea como algo “moderno y cool”: “Targeted marketing”, “Smart Ads”

● ¿Y realmente las empresas pagan por eso?

- Sí, por que se ha demostrado que **FUNCIONA** y **MUY BIEN**

TAG Heuer @TAGHeuer
Next #CR7Time contest is coming soon! Follow @TagHeuer to get a chance to win exclusive #TagHeuer bags and wallets! pic.twitter.com/FAN9JxjUT0

TAG Heuer
Promocionado

A alguien de mi entorno le gustan los relojes Tag Heuer (yo no soy 😊)

Así que no...NO ES “GRATIS” como parece 😊

EL CONFLICTO Y LAS RRSS

- Y, para sacar información, las RRSS quiere que **interacciones**

- Vamos, que “escribas cosas”

- Para ello, los algoritmos de las RRSS **fomentan el conflicto**

- Te dejan ver mensajes de **gente que opina de manera contraria** a ti
 - O son muy polémicos
 - Con tal de que interactúes con ellos y “escribas cosas”
 - Si un influencer cobra por “visitas” e “interacciones” **le da igual que sean positivas o negativas**
 - Muchos crean flames para cobrar así... 😞

- ¡Están diseñadas para cabrearte y “comerte la cabeza”!

- **No hagas RT, comentes ni compartas “basuras”, bloquea y denuncia**
 - ¡Hacerles “casito” es bueno para ellos! ¿No me crees?
 - <https://www.newtral.es/algoritmo-twitter-como-funciona-marcelino-madrigal/20210525/>
 - <https://www.newtral.es/opinion-discurso-ira-online-echo-marcelino-madrigal-redes-sociales/20210614/>



En serio, esto no merece la pena, por muchas ganas que te den...be water, my friend. No interacciones, no compartas, denuncia y bloquea, como buen Jedi 😊

EJEMPLOS DE ALGUNOS TIPOS DE PUBLICACIONES PARA GENERAR “ENGAGEMENT” EN CUALQUIER RRSS

- Cobrar por interacción en muchas RRSS hacen proliferar contenidos “discutibles”
 - Si le unes equipos o herramientas de moderación insuficientes, la RRSS se degrada
 - La parte social queda en un segundo plano, y solo queda la parte económica

Hola buenas, hoy vamos a ver el origen una de las tradiciones más bonitas del verano

Vamos a tomar el fresco

[Abro hilo]



Hilos extra-largos (muchos hechos con IA) que se repiten cada X tiempo. Al menos algunos son interesantes...

El perfecto **imbécil** de Jota Pe Hernández no tiene ninguna prueba en contra de la vicepresidenta Francia Márquez. Nuevamente este mamarracho quedó en ridículo como siempre.



Faltosidades, racistadas y salvajadas varias, muchas de ellas denunciables (lo veremos luego)

Reply this tweet with your most **unpopular opinion** of Dragon Ball



Generación de polémicas intencionadamente y “sealioning”: <https://es.wikipedia.org/wiki/Sealioning>



José Manuel
Redondo López

ONLYFANS: TÚ ERES EL PRODUCTO A LA VENTA

- Se que OnlyFans está prohibida a menores de 18
 - Pero también sé que gente menor se salta esos controles
- Se supone que tus fans pagan por tus contenidos
 - Pero no te engañes: OnlyFans hoy en día se usa para **vender contenido sexual** mayoritariamente
 - Y muchos de tus seguidores que no conoces **te lo van a exigir**
 - Aunque eso reporte beneficios económicos hoy, **te puede estar perjudicando tu futuro**
 - Es frecuente ser **víctima de ciberacoso** o contactar con **groomers, coaccionadores o extorsionadores sexuales** (mira P-74 "Atalaya")
 - Por favor, **no te metas ahí siendo menor**

● Más información

- <https://www.incibe.es/ciudadania/blog/onlyfans-la-nueva-red-social-para-vender-tu-privacidad>
- <https://www.incibe.es/menores/blog/al-dia-en-onlyfans>
- <https://www.incibe.es/menores/blog/historia-real-mi-hijo-a-ha-compartido-contenido-sexual-en-onlyfans>

OnlyFans 300 Posts • 71.5K Likes

OnlyFans @onlyfans

OnlyFans is a subscription social platform revolutionizing creator and fan relationships

SUBSCRIPTION

SUBSCRIBE FOR FREE

300 POSTS 300 MEDIA 1 ARCHIVED

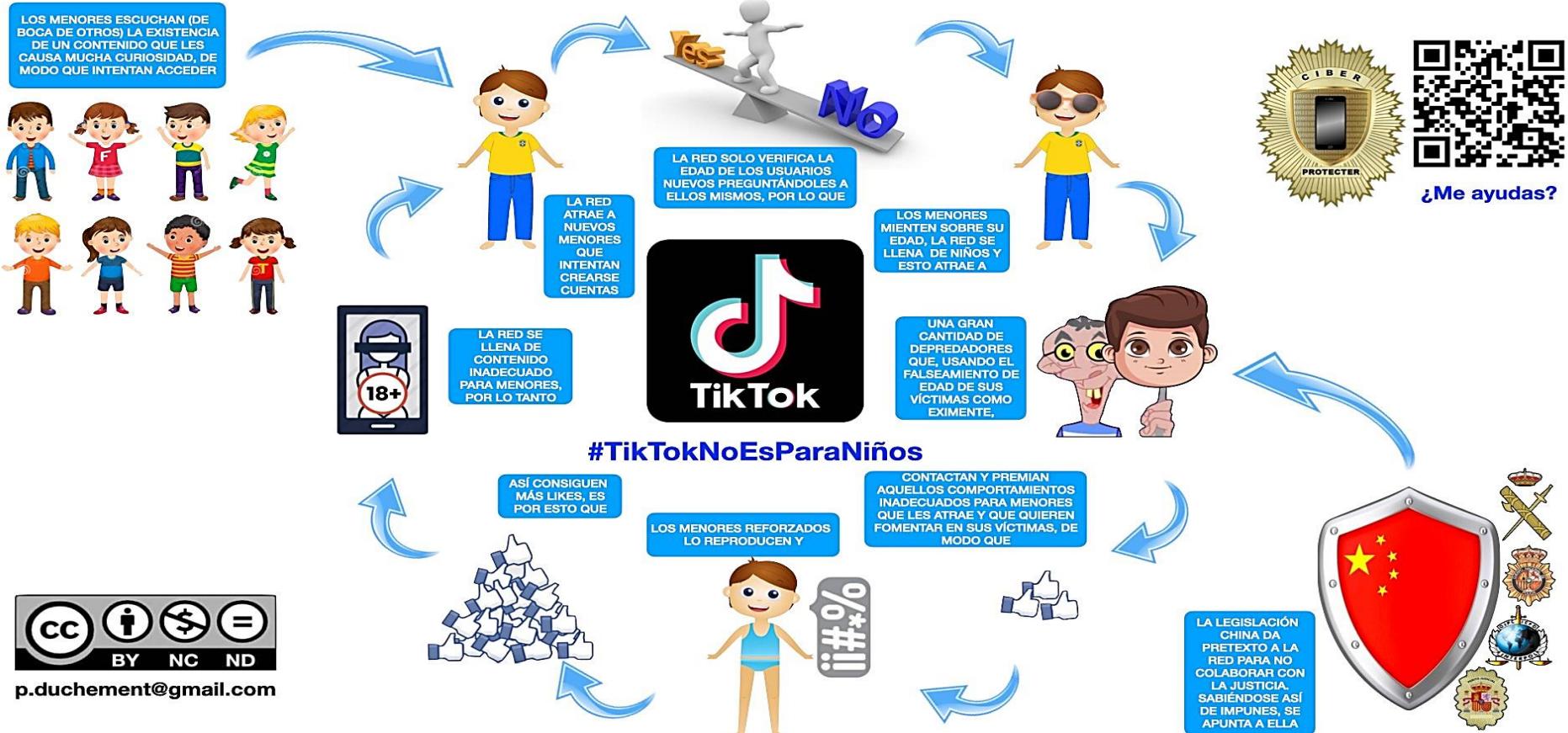
LATEST POSTS

El dinero que (a lo mejor) ganes hoy, te lo puedes tener que gastar en sicólogos o demandas mañana...

TIKTOK: TÚ PODRÍAS SER EL PRODUCTO “A LA VENTA”

● TikTok también es una red peligrosa para menores

- No solo hay sospechas de venta excesiva de tus datos, sino de tener muchos groomers (**P-74 “Atalaya”**)
- ¿Ya tienes cuenta? Mira esto: <https://www.incibe.es/menores/familias/control-parental/tiktok>



¿CREEES QUE LO HAS ENTENDIDO TODO? ¡AUTOEVALÚATE!



- *¿Comprendes cómo una red social cualquiera saca partido de todo lo que hagas en ella, aunque no pagues dinero directamente?*
- *¿Te ha quedado claro que cuanto más compartas en una red social más beneficio le reportas, de manera directa o indirecta, gracias al mundo de la publicidad?*
- *¿Eres consciente de que lo que pones en una RRSS puede usarse en tu contra, especialmente por gente que te stalkee y sepa lo que haces o dónde vas?*
- *¿Y que las cosas que se presentan en las redes sociales están influenciadas por tus gustos y preferencias, tanto para sugerirte contenido como para fomentar interacciones, aunque sea basándose en la polémica?*
- *¿Te ha quedado claro que interaccionar, aunque sea para criticar, beneficia al que pone el contenido polémico?*



¿CÓMO ME “ENFRENTO” A UNA RED SOCIAL?

¿Qué debo tener en cuenta cuando estoy en una?



¿QUÉ TE VAS A ENCONTRAR EN ESTE BLOQUE?

- 
- *¿Te da miedo entrar en una red social por la de cosas que hay?*
 - No te preocupes, yo te enseño una estrategia para entrar con menos riesgo
 - *¿Te has parado a pensar que estar en una red social no deja de ser algo similar a estar en la calle, y que se aplican las mismas normas?*
 - *¿Hablarías con un desconocido?* Pues en las redes social tampoco...
 - *¿Harías amistad con gente que no conoces, o sólo con gente que sean amistades o populares?* Pues aquí es lo mismo...
 - **Y también voy a tratar de explicarte que tu perfil en las redes sociales eres “tú en Internet” para bien y para mal**
 - Y que el hecho de que te suplanen puede ser un verdadero problema
 - Así que tienes que evitarlo y también te voy a explicar cómo
 - Lo que incluye cuidar también tu imagen personal
 - **Y por supuesto evitar fraudes comunes a través de redes sociales**
 - Y de los que podrías ser víctima solo por el hecho de estar ahí

¿QUÉ TENGO QUE SABER CUÁNDO ESTOY EN UNA RED SOCIAL?

● Lo primero es **USAR LA CABEZA** y **PENSAR**

- ¿VAS A DEJAR QUE TE ENGAÑEN? ¡**NUNCA!**

● *¿Te dan Información?. Contrástala (fact check)*

- Opiniones /noticias (ojo, que también las hay falsas)
 - <https://twitter.com/malditobulo> (también tienen web)
- Usa **TU** criterio y toma **TUS** decisiones
- Cuando termines de analizarlo, consulta a tu familia/profesores y explícales lo que has visto y “cómo te lo has currado”

● *¿Te piden que compres algo? CUIDADO*

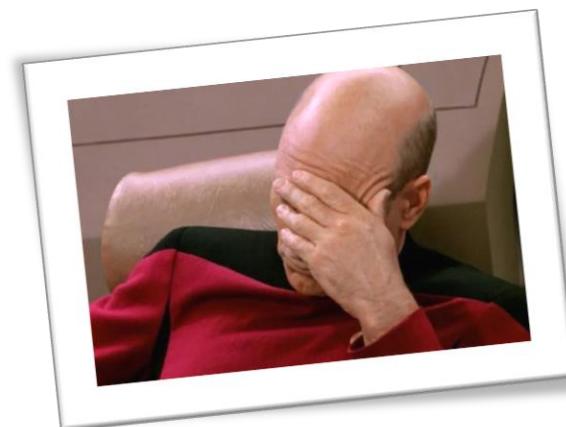
- A un influencer podría haberle **pagado** una compañía para promocionar que compres cosas en sus juegos...
 - Y simplemente “venderlo” sin haber probado nada de lo que vende...
- *¿Realmente las necesitas? ¿no estás haciendo trampa? ¿de verdad quieres pagar aún más dinero por el juego?*



¿QUÉ TENGO QUE SABER CUÁNDO ESTOY EN UNA RED SOCIAL?

● ¿Te has equivocado / te han engañado? Lo siento ☹

- No te preocupes, si lo has pensado antes lo has hecho bien, **es aprendizaje** (para la próxima te espero!)
- Pero...¡**Nunca juegues con cosas que no tienes!** (apuestas, compras in-game...todo lo que requiera dinero tuyo o de tu familia)
 - **Sí, eso incluye micro-transacciones, loot boxes, gachas, cromos del FIFA, etc. (aunque te lo diga tu influencer favorito)**
 - ¡Quieren que gastéis (y les regaléis) dinero a las compañías de videojuegos! (¡y ya habéis pagado por él!), pero...¡controla!
- Y sobre todo ¡**nunca mandes fotos ni datos personales de cualquier clase a nadie** (direcciones, nºs de tarjetas de crédito...!)!



● ¿Tienes dudas? En seguridad siempre tenemos un dicho:

Si dudas o sospechas, la única respuesta segura es decir NO

¿CÓMO ENTRO EN UNA RED SOCIAL?

● Empieza restringiendo quién puede añadirte

- Y añadiendo tú a quién **VERDADERAMENTE** conozcas
 - Déjate de cuentas “raras”, desconocidas...
 - Tus compañeros de clase, tus amigos, tu gente, tu cole, tu equipo de deportes, influencers conocidos que hablen de lo que te interesa... ¡anda que no hay gente interesante!

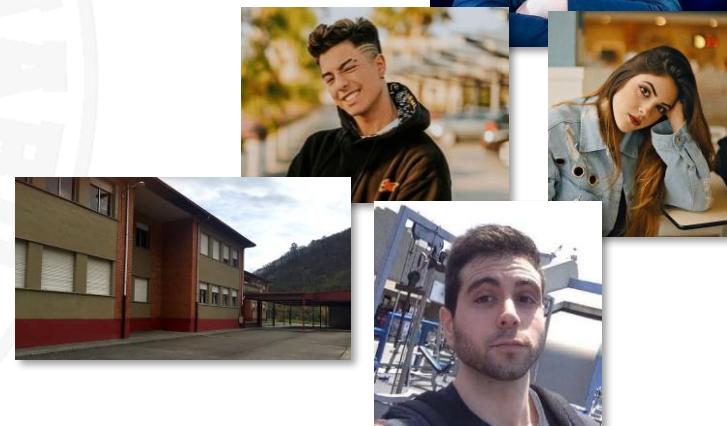
● “Ábrete al mundo” a medida que pilles confianza y te familiarices

- O tus contactos te recomiendan gente buena y de confianza...
- **Pero NUNCA aceptes NADA de desconocidos**



● Controla para quién publicas las cosas

- Todo el mundo, grupos concretos, “mejores amigos”...
- ¡Todas las redes sociales tienen opciones de esta clase!
- Tienes que analizarlas y dominarlas como un pro ☺



● **Ojo con los mensajes directos:** ¡Asegúrate de que se los mandas a quien de verdad quieres y no los aceptes de desconocidos! ☺

COSAS QUE TIENES QUE SABER DE LAS RRSS

- Lo primero que tienes que hacer es tener **una contraseña decente**
- Y luego tratar tu perfil, tus datos, tu localización (desde dónde publicas) adecuadamente
- Os voy a dar algunos ejemplos en redes sociales conocidas
- ¡Pero que sepáis que **TODAS tienen opciones parecidas!**
 - Así que... ¡echa un rato en buscarlas para estar más seguro!
- **¿Te sientes hakin bestia? ¡Puedes ir más allá activando un 2FA!**
 - Aquí te lo explican: <https://www.incibe.es/ciudadania/tematicas/contrasenas-seguras/autenticacion-de-dos-factores>

Crea tu contraseña segura

PASO A PASO

PASO 1

Pensar una frase

Puede tener significado para nosotros o simplemente unir 2 o 3 palabras al azar, pero que nadie más conozca. La longitud mínima recomendada es de 10 caracteres.



Mi cuenta segura

PASO 2

Alternar mayúsculas y minúsculas
Unimos las palabras y resaltamos las iniciales con mayúsculas.

MiCuentaSegura

PASO 3

Sustituir letras por números
Un truco es intercambiar algunas letras por cifras, como "o" por 0, "i" por 1, "e" por 3 o "a" por 4.

M1Cu3nt4S3gur4

PASO 4

Añadir caracteres especiales
Solo queda incluir algún símbolo (~ ! @ # \$ % ^ & * - + | \ \ () { } [] ; : " < > . ? , !).

M1Cu3nt4S3gur4!

PASO 5

Personalizar la clave para cada servicio
Podemos utilizar las dos primeras letras del servicio y una la ponemos al principio y otra al final de la clave, ambas en mayúsculas. Ejemplo: si el servicio se llama "Mailbook", usaremos la M y la A.



MM1Cu3nt4S3gur4!A

¡Y listo! Así de sencillo hemos creado nuestra contraseña robusta, segura y fácil de recordar.



Y como medida de seguridad extra, sigue estos consejos y los ciberdelincuentes no tendrán nada que hacer:

Utiliza gestores de contraseñas para controlar todas tus claves.

No repitas las mismas contraseñas en distintas cuentas.

Cambia las cada cierto tiempo (3 meses).

No las compartas con nadie, ni amigos ni familiares.

Utiliza la verificación en dos pasos siempre que sea posible.

Configura tu móvil para que, al recibir una notificación, no se muestren los caracteres que pulsas.



Recuerda que tienes a tu disposición la Línea de Ayuda en Ciberseguridad de INCIBE, gratuita y confidencial, para cualquier consulta relacionada con la ciberseguridad.

www.incibe.es | www.osi.es

GOBIERNO
DE ESPAÑA
VICERRENDERIA
TERCIERA DEL GOBBERO
MINISTERIO DE ASUNTOS ECONOMICOS
Y CONSEJERIA DE INVESTIGACIONES
Y INTELIGENCIA ANTICRIMEN

SECRETARIA DE ESTADO
DE INVESTIGACIONES
Y INTELIGENCIA ANTICRIMEN

INSTITUTO NACIONAL DE CIBERSEGURIDAD

017

Oficina de Seguridad
del Internauta



@INCIBE @osiseguridad



Configurar una red social

No es “crear una cuenta y ya” precisamente...



¿POR QUÉ CONFIGURARLAS?



José Manuel
Redondo López

- Tristemente, estar en una red social te hace objetivo de muchos tipos de fraudes
- Muchos usuarios en una red social no son reales, sino bots
 - Están ahí para escribir mensajes falsos y sacar algún beneficio
 - Desinformación, estafas, troleo...
- Muchas veces usando la información que tú mismo/a das (Ej.: Robando tus fotos)
- Configurando bien tu RRSS puedes parar muchos de estos problemas

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 | www.osi.es

GOBiERNO DE ESPAÑA
VICEREJERÍA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN Y TRANSFORMACIÓN DIGITAL

incibe
INSTITUTO NACIONAL DE CIBERSEGURIDAD
017
OSI
Oficina de Seguridad del Internauta

@INCIBE @osiseguridad

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.**Más información en "Sorteos y premios online, un reclamo para hacerse con nuestros datos".**
- 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.**Más información en "¡Socorro, me han secuestrado WhatsApp!".**
- 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 videos 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".**



José Manuel
Redondo López

PRIVACIDAD

- **Alguna gente dice que la privacidad no es importante**

- Afirman que “no son delincuentes y no tienen nada que ocultar”

- **Esto es falso:** Tu falta privacidad puede ser usada en tu contra en muchos casos

- Ej.: *¿Qué pasa si alguien te suplanta en un grupo que tienes con tus amigos/as?*
- Es imposible calcularlos todos
- Por lo que puedes tener un problema si no la cuidas en cualquier momento

- **Tus pensamientos, fotos, etc. son tuyos,**

- ¡No dudes en protegerlos en cualquier RRSS!

The infographic is titled "Tu privacidad sí importa, ¡protégela!" and is produced by incibe_ (Instituto Nacional de Ciberseguridad) and OSi (Oficina de Seguridad del Internauta). It includes several tips for protecting privacy:

- Protege la información almacenada en tus cuentas usando contraseñas seguras y distintas para cada servicio online.**
- Activa la autenticación en dos pasos para dotar de mayor seguridad el acceso a tus cuentas online.**
- Limita la información que compartes en redes sociales u otros canales para prevenir el robo y suplantación de identidad.**
- Lee las políticas de privacidad de las webs en las que estás registrado para conocer cómo protegerán tus datos y qué uso harán de ellos.**
- Cierra siempre la sesión cuando termines de hacer uso de un servicio en dispositivos compartidos o públicos.**
- Revisa qué permisos concedes a las aplicaciones que tienes instaladas.**

#OSIconsejo
www.incibe.es/ciudadania



REPUTACIÓN

- La privacidad va de la mano con tu **reputación online**
- Si algo no lo harías en persona, no lo hagas en RRSS
 - La culpa **siempre es de quien acosa**, extorsiona, etc.
 - Pero las consecuencias chungas de primeras **te las llevas tú** 😞
- Como dijimos antes, en la RRSS se busca “guerra”: No caigas en la trampa
- Cuidado con lo que dices, o con lo que le dicen a la gente de tu entorno
 - Es importante **combatir el ciberbullying**: Mira la P-74 “Atalaya”
 - ¡Tú puedes ayudar a quien lo necesita!

The infographic is titled "¿Cómo cuido mi reputación online?" and is produced by incibe (Instituto Nacional de Ciberseguridad) and OSi (Oficina de Seguridad del Internauta). It features a woman in an orange jacket holding a smartphone, looking at a magnifying glass icon over a profile picture. The background is orange with white text and icons. The text provides five tips for managing online reputation:

- Indaga sobre ti en motores de búsqueda.** Si encuentras contenido que no te gusta, elimínalo si tienes permisos para ello. En caso contrario, solicita su eliminación a la plataforma donde está publicado.
- Piensa antes de publicar contenido en Internet** si puede malinterpretarse, disgustar y ofender a otros usuarios si no se conoce el contexto.
- Interactúa de forma positiva en línea.** Respeta las opiniones de los demás y evita discusiones innecesarias que perjudiquen tu imagen.
- Utiliza las opciones de privacidad** que proporcionan las redes sociales y otros sitios web para controlar quién puede ver lo que publicas.
- Si alguien publica algo negativo sobre ti,** trata de resolver el problema de manera privada y cordial para solicitar su retirada. Si no atiende a tus peticiones, solicita a la plataforma su eliminación.

#OSIconsejo
www.incibe.es/ciudadania



José Manuel
Redondo López

OK, PERO...¿CÓMO LO HAGO?

- Por suerte para nosotros, el INCIBE tiene guías fáciles de seguir
 - ¡Para todas las RRSS!
 - <https://www.incibe.es/ciudadania/tematicas/privacidad/configuraciones-redes-sociales>
- Te incluimos aquí unas imágenes resumen
 - Y luego usaremos Twitter/X como ejemplo de por qué ciertas configuraciones son importantes
 - Así puedes buscar **opciones parecidas en otras RRSS** que tengas

No dejes que X (Twitter) te delate, configura tu privacidad

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD 017 OSi Oficina de Seguridad del Internauta

Abre la aplicación.

Accede al **menú principal** pulsando sobre la imagen de tu perfil.

A continuación, dirígete al apartado **"Configuración y privacidad"**.

Una vez ahí, desde el apartado **"Privacidad y seguridad"** podrás configurar cuestiones como:

- Controlar quien puede ver y responder a tus tuits.
- Bloquear y silenciar palabras, usuarios, listas, notificaciones, etc.
- Establecer las **preferencias de anuncios**, la forma en la que se comparte la **información** con terceros, datos de **ubicación** y la **política de privacidad** de la aplicación.

#OSiconsejo
www.incibe.es/ciudadania

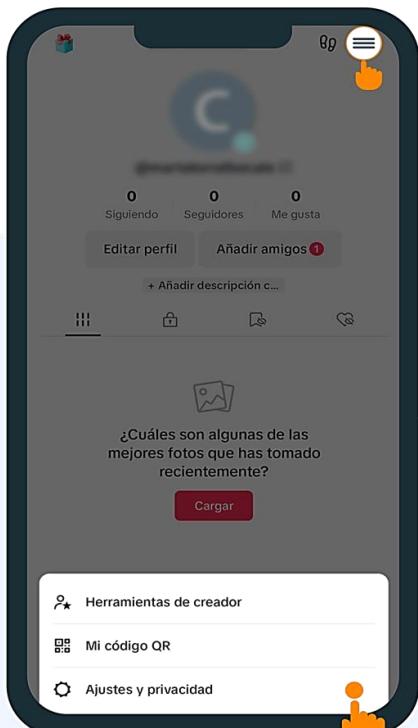


José Manuel
Redondo López

OK, PERO...¿CÓMO LO HAGO?

incibe_ 017 OSI Oficina de Seguridad del Internauta

¿Cómo protejo mi privacidad en TikTok?



Entra en tu perfil y haz clic en las tres rayas.

Accede a 'Ajustes y privacidad'.

Revisa dentro de 'Privacidad' cuestiones relevantes como:

- Si la cuenta es privada.
- Si estás compartiendo tu ubicación.
- Quién puede enviarte mensajes.
- Usuarios bloqueados.

Ajustes y privacidad

- Cuenta
- Privacidad
- Seguridad
- Saldo
- Compartir perfil

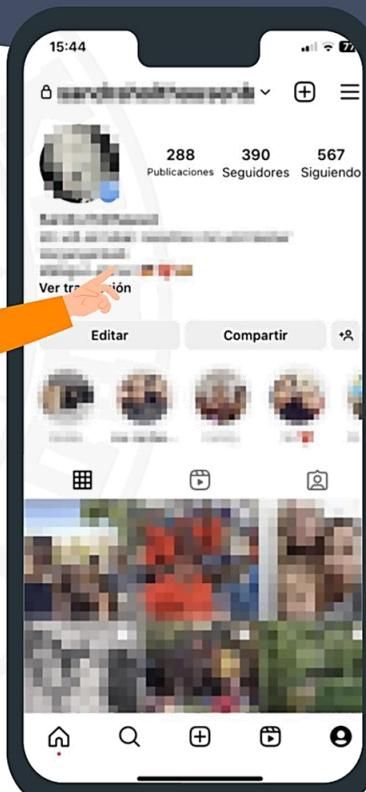


Configura la aplicación y ten bajo control tu información!

#OSIconsejo
www.incibe.es/ciudadania

incibe_ 017 OSI Oficina de Seguridad del Internauta

Configura tu privacidad de Instagram en 5 pasos



Abre la aplicación de Instagram



Entra en tu perfil



Pulsa en las tres líneas horizontales de arriba a la derecha.



Dirígete a 'Configuración y privacidad'.

A continuación, podrás:

Revisar la configuración de la cuenta: datos personales, contraseña, permisos así como las preferencias de los anuncios.

Establecer quién puede ver tus contenidos.

1. Privacidad de la cuenta.
2. Bloquear cuentas de usuarios.
3. Ocultar historias y directos a usuarios concretos.

Indicar cómo pueden interactuar contigo los demás.

1. Bloquear comentarios, quién puede etiquetarte, etc.

#OSIconsejo

www.incibe.es/ciudadania

Pasos a seguir en iPhone. En dispositivos Android, en el paso 4 habrá que seleccionar 'Configuración' y después 'Privacidad' para encontrar las distintas opciones.



José Manuel
Redondo López

EJEMPLO DE OPCIONES DE UNA RED SOCIAL: TWITTER/X

The image shows the Twitter/X mobile application's settings menu. On the left, a sidebar lists various account management options. The 'Configuración y privacidad' option is highlighted with a red box and has a red arrow pointing to the main content area. The main content area is divided into two sections: 'Configuración' and 'Privacidad y seguridad'. The 'Configuración' section contains links for 'Tu cuenta', 'Seguridad y acceso a la cuenta', 'Privacidad y seguridad', 'Notificaciones', 'Accesibilidad, pantalla e idiomas', and 'Recursos adicionales'. The 'Privacidad y seguridad' section contains links for 'Tu actividad en Twitter', 'Audiencia y etiquetas', 'Tus Tweets', 'Contenido que ves', 'Silenciar y bloquear', 'Mensajes Directos', and 'Visibilidad y contactos'.

Solicitudes de seguimiento 20+

Temas

Momentos

Boletines informativos

Twitter Ads

Analytics

Configuración y privacidad

Centro de ayuda

Mostrar

Atajos de teclado

Configuración

- Tu cuenta >
- Seguridad y acceso a la cuenta >
- Privacidad y seguridad >
- Notificaciones >
- Accesibilidad, pantalla e idiomas >
- Recursos adicionales >

Privacidad y seguridad

Administra qué información ves y compartes en Twitter.

Tu actividad en Twitter

- Audiencia y etiquetas >
- Tus Tweets >
- Contenido que ves >
- Silenciar y bloquear >
- Mensajes Directos >
- Visibilidad y contactos >

¡PROTEGE TU CUENTA! (SOBRE TODO AL PRINCIPIO)

- Tu cuenta > Ve la información de la cuenta, descarga un archivo con tus datos u obtén más información acerca de las opciones de desactivación de la cuenta
- Seguridad y acceso a la cuenta > **Información de la cuenta**
 - Ve la información de tu cuenta como el número de teléfono y la dirección de correo electrónico.
- Privacidad y seguridad >
- Notificaciones > Cambia tu contraseña
Cambia tu contraseña en cualquier momento.
- Accesibilidad, pantalla e idiomas >
- Recursos adicionales > Descargar un archivo con tus datos
Hazte una idea del tipo de información que se almacena de tu cuenta.
Teams de TweetDeck
Invita a cualquier persona a twittear desde esta cuenta con la función Teams de TweetDeck.
Desactiva tu cuenta
Averigua cómo puedes desactivar tu cuenta.

Esto es el “tick” azul, pero solo se lo dan a famosos, a empresas (tick amarillo) o a quienes pagan

← **Información de la cuenta**

- Nombre de usuario
@The_Rounded_Man >
- Teléfono >
- Correo electrónico
 >
- Verificado
No. Solicitar verificación >
- Tweets protegidos
 >

Superimportante, esto hace que solo quien te siga (y tú aceptes primero) vea lo que publicas

¡Búscalos en todas tus RRSS!



José Manuel
Redondo López

¡NO DES DEMASIADA INFORMACIÓN Y VIGILA TU CUENTA!

Configuración

- Tu cuenta >
- Seguridad y acceso a la cuenta** > (highlighted)
- Privacidad y seguridad >
- Notificaciones >
- Accesibilidad, pantalla e idiomas >
- Recursos adicionales >

Seguridad y acceso a la cuenta

Administra la seguridad de tu cuenta y lleva un control de su uso, incluidas las aplicaciones que conectaste a ella.

- Seguridad** > (highlighted)
- Aplicaciones y sesiones** > (highlighted)

Seguridad
Administra la seguridad de tu cuenta.

Aplicaciones y sesiones
Consulta la información sobre cuándo iniciaste sesión en tu cuenta y las aplicaciones que conectaste a ella.

¿Sospechas que alguien te entra en la cuenta? Aquí puedes ver desde dónde se entró últimamente...

¡Revísalo a menudo por si hay algo sospechoso!

Configuración

- Tu cuenta >
- Seguridad y acceso a la cuenta** > (highlighted)
- Privacidad y seguridad >
- Notificaciones >
- Accesibilidad, pantalla e idiomas >
- Recursos adicionales >

Tus Tweets

Administra la información asociada a tus Tweets.

Marcar el contenido multimedia que twitteas para indicar que contiene material que puede herir la sensibilidad de algunas personas

Si activas esta opción, las imágenes y los videos que twitteas se marcarán como delicados para las personas que no deseen ver ese tipo de contenido. [Más información](#)

Agregar información de ubicación a tus Tweets > (highlighted)

Entra aquí y DESACTIVA la ubicación para tus Tweets

¡A nadie le interesa saber desde donde Twitteas! (demasiada información a la que dar mal uso)

¿No te interesa cierto contenido? ¡PUES NO LO VEAS!

Configuración	Privacidad y seguridad
Tu cuenta	Administra qué información ves y compartes en Twitter.
Seguridad y acceso a la cuenta	
Privacidad y seguridad	Audiencia y etiquetas Administra qué información permite que vean otras personas en Twitter.
Notificaciones	
Accesibilidad, pantalla e idiomas	
Recursos adicionales	Contenido que ves Decide qué ver en Twitter en función de los temas e intereses de tu preferencia. Silenciar y bloquear Administra las cuentas, palabras y notificaciones que silenciaste o bloqueaste.

[← Contenido que ves](#)

Decide qué ver en Twitter en función de los temas e intereses de tu preferencia.

- Mostrar contenido multimedia que pueda contener material delicado
- [Temas](#)
- [Intereses](#)
- [Configuración de Explorar](#)
- [Configuración de búsqueda](#)

Indica lo que te interesa y así tu red te mostrará cosas más interesantes...

¡También puedes bloquear videos o imágenes catalogadas como ofensivas (hay gente que se cree muy graciosa 😊)

[← Silenciar y bloquear](#)

Configuración	
Tu cuenta	Administra las cuentas, palabras y notificaciones...
Seguridad y acceso a la cuenta	
Privacidad y seguridad	
Notificaciones	
Accesibilidad, pantalla e idiomas	
Recursos adicionales	

- [Cuentas bloqueadas](#)
- [Cuentas silenciadas](#)
- [Palabras silenciadas](#)
- [Notificaciones silenciadas](#)

Aquí puedes bloquear o silenciar gente (más de eso después)

¡Pero lo más importante es que si estás harto de un TT o tema, puedes silenciar palabras y no volverán a salirte más mensajes que las contengan!



José Manuel
Redondo López

¡EN INSTAGRAM HAY OPCIONES MUY SIMILARES!

Editar perfil

Cambiar contraseña

Aplicaciones y sitios web

Correo electrónico y SMS

Notificaciones push

Administrar contactos

Privacidad y seguridad

Actividad de inicio de sesión

Correos electrónicos de Instagram

[Cambiar a cuenta profesional](#)

Privacidad de la cuenta

Cuenta privada

Si tu cuenta es privada, solo las personas que apruebes podrán ver tus fotos y vídeos en Instagram. Esto no afectará a tus seguidores actuales.

Estado de actividad

Mostrar estado de actividad

Permite que las cuentas que sigues y las personas a las que has enviado mensajes puedan ver la última vez que has estado activo en las aplicaciones de Instagram. Si desactivas esta opción, no podrás ver el estado de actividad de otras cuentas.

Compartir las historias

Permitir compartir

Permite que las personas comparten tu historia como mensajes.

Comentarios

[Editar configuración de los comentarios](#)

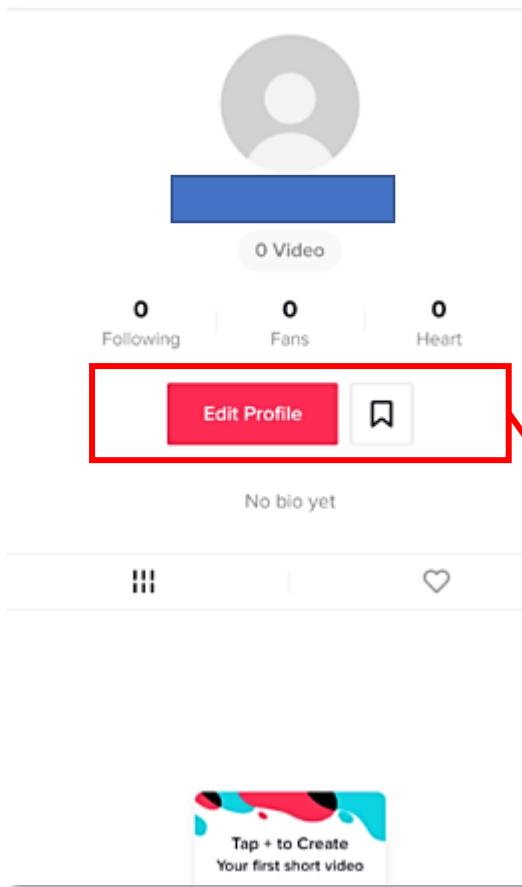
¡Merece MUCHO la pena dedicar un rato a leer opciones de privacidad y seguridad y activarlas en TODAS tus redes sociales!

¡Hay cosas muy útiles que seguramente no conozcas!



José Manuel
Redondo López

¿Y EN TIKTOK?



Privacy and Settings

- Digital Wellbeing
- Live Photo
- General Settings

ABOUT

- Help Center
- Terms of Use
- Privacy Policy
- Copyright Poli
- Report a Problem
- Clear Cache

Log Out

v9.9.0(2019011531)

Privacy and Safety

Discoverability

- Allow Others to Find Me
- Private Account

Personalization

Safety

- Who Can Send Me Comments
- Who Can React to Me
- Who Can Duet With Me
- Who can send me messages
- Allow Download
- Block List

Aunque...TikTok es una red que ahora mismo está rodeada de polémicas (tratamiento de tus datos, privacidad...)

¿CREEES QUE LO HAS ENTENDIDO TODO? ¡AUTOEVALÚATE!

?

- *¿Te ha quedado claro que la mejor forma de entrar en una red social es limitando tu cuenta solo a personas que conozcas en la vida real?*
- *¿Entiendes que el consejo de no “hables con desconocidos” se aplica tanto en la calle como en las redes sociales?*
- *¿Te ha quedado claro que tener una buena contraseña es clave para proteger tu cuenta en una red social?*
- *¿Te das cuenta de que las redes sociales tienen muchas configuraciones que te permiten dejarla en un estado mucho más seguro que recién creada tu cuenta?*
- *¿Eres consciente de que todas las redes sociales más o menos comparten las mismas opciones de privacidad y seguridad, y que una vez vistas en una puedes encontrar el equivalente en las demás?*



Precauciones usando una red social

Cosas que no debes hacer o debes tener especial cuidado





José Manuel
Redondo López

¿QUÉ COSAS TENGO QUE VIGILAR CUANTO ESTOY EN UNA RRSS?

- Como te comentaba antes, estar en RRSS te somete a nuevos peligros (mira la imagen)

- Todos están en todas las RRSS

- Pero algunos son más frecuentes en unas que en otras

- La de **bulos** conspiranóicos para mayores que hay en Facebook mete miedo (recuerda: algunas personas se creen eso...)
- Los **challengues** de Insta son muy peligrosos
- Ya vimos lo que pasaba en TikTok 😞
- Cuidado con las **funas** (hacerlas (¡es bullying!) y que te las hagan) y con quedarte “enganchado”
 - No solo a la red, hay mucho **juego online encubierto** (o no)
- ...

- Es necesario que sepas lo que son y tengas bien entrenado tu “sentido arácnido”

Top 10 de los principales peligros de las redes sociales para los jóvenes

	Problemas para la privacidad
	Suplantación de identidad
	Adicción a las RRSS
	Ciberbullying
	Contacto con desconocidos que pueden ser peligrosos
	Grooming
	Sexting
	Sextorsión
	Fake news y la distorsión de la realidad
	Challenge o retos muy peligrosos, en ocasiones delictivos

Fuente: <https://protecciondatos-lopd.com/empresas/peligros-redes-sociales/>



José Manuel
Redondo López

APLICACIONES QUE SE INSTALAN EN TUS RRSS

● ¿Este tipo de aplicaciones “graciosas” te suena?

- Son simpáticas y tienen funcionalidades bastante interesantes, pero...
- ...¡Algunas veces resultan ser timos!
- **¡Lo mismo pasa con algunos anuncios en RRSS!**

● Solo quieren que hagas clic y acceder a tu cuenta para...

- Mostrarte **publicidad** (¡que jeta!)
- Postear como su fuera tú, es decir, **suplantarte** (¡impostor!)
- **Borrarte** mensajes (¡lo que faltaba!)
- ¡O **robarte** la cuenta! (Oh, oh...)

● El daño que pueden hacer depende de los permisos que les concedas



The image contains two screenshots of mobile applications. The top screenshot is for a Facebook app titled "¿Quien visita tu perfil?". It shows a blue header, a progress bar "Paso 1 de 4", and a text explaining how to find visitors to your profile. The bottom screenshot is for a Twitter app titled "WHO VISITS YOUR TWITTER PROFILE?". It shows a similar layout with a grid of user profile pictures.



José Manuel
Redondo López

APLICACIONES QUE FUNCIONAN CON TU CUENTA DE RRSS

● Tu cuenta es tuya

- No la cedas a nadie... ¡ni a nada!
- Lo mejor es **NO** instalarse estas aplicaciones
- Si ya lo has hecho
 - Vete a las opciones y busca el apartado de aplicaciones
 - Una vez allí, elimínala o quítale permisos
 - ¡Todas las RRSS tienen una opción así!

¡Está intentando instalarse en tu cuenta de Twitter!

The screenshot shows a Twitter application authorization dialog. At the top, it says "Authorize Seesmic Web to use your account?". Below that, it lists permissions: "This application will be able to: Read Tweets from your timeline, See who you follow, and follow new people, Update your profile, Post Tweets on your behalf, Access your direct messages." At the bottom, there are two buttons: "Authorize app" (in blue) and "No, thanks". To the right, there's a sidebar with the Seesmic Web logo and some text: "Seesmic Web By Seesmic seesmic.com/app Seesmic Web is a web application helping to easily manage and build your community directly in your browser." Below the main dialog, it says "This application will not be able to: See your Twitter password." and "You can revoke access to any application at any time from the Applications tab of your Settings page. By authorizing an application you continue to operate under Twitter's Terms of Service. In particular, some usage information will be shared back with Twitter. For more, see our Privacy Policy."

● Lo mismo con anuncios

- Mejor **no hagas clic** en ninguno
- Te pueden llevar a páginas de fraudes o que te instalen algo automáticamente
 - Y ya no te digo si te piden que te lo instalas tú
- **No te instales cosas de cualquier sitio**, ¡que es lo que buscan para liártela!

The screenshot shows the Instagram settings page under "Authorized Applications". It lists two apps: "Buffer" and "WordPress.com". For Buffer, it says "Production environment client for Buffer" and has a "Revoke Access" button. For WordPress.com, it says "Display your latest Instagram photos on your WordPress.com site." and also has a "Revoke Access" button. To the right, there is a large red block of text: "¿No sabes qué hace aquí o no te interesa? ¡Cárgatela!".

¡ALGUIEN HA POSTEADO UNA BURRADA!



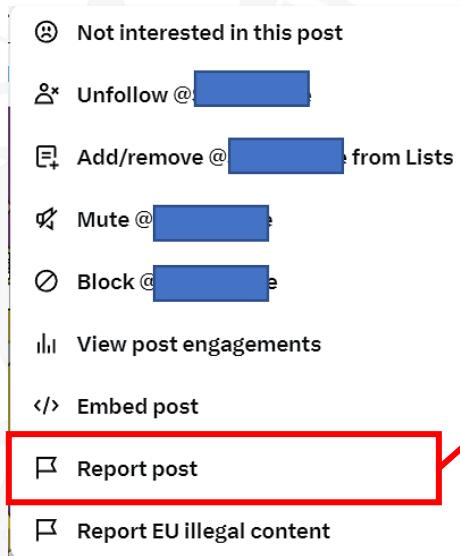
José Manuel
Redondo López

● *¿Alguien ha posteado una burrada, algo ofensivo o similar?*

- ¡Tú puedes ayudar a “limpiar” la red!
- Se puede **denunciar un mensaje** alegando una razón
- La red social te pregunta **por qué crees que es ofensivo**
- Examina lo que dices y, si hay más gente que ha hecho lo mismo y/o es verdad, puede borrar el mensaje o suspender / cancelar la cuenta

● Así las redes auto-regulan sus contenidos

● **Siempre es anónimo** (nadie sabrá que le has denunciado)



Cada RRSS tiene sus normas y “contenidos prohibidos”, pero en general acaban más o menos siendo estos en todas

X Gathering info

What type of issue are you reporting?

Why are we asking this?

Hate

Slurs, Racist or sexist stereotypes, Dehumanization, Incitement of fear or discrimination, Hateful references, Hateful symbols & logos

Abuse & Harassment

Insults, Unwanted Sexual Content & Graphic Objectification, Unwanted NSFW & Graphic Content, Violent Event Denial, Targeted Harassment and Inciting Harassment

Violent Speech

Violent Threats, Wish of Harm, Glorification of Violence, Incitement of Violence, Coded Incitement of Violence

Child Safety

Child sexual exploitation, grooming, physical child abuse, underage user

Privacy

Sharing private information, threatening to share/expose private information, sharing non-consensual intimate images, sharing images of me that I don't want on the platform

Spam

Fake engagement, scams, fake accounts, malicious links

Suicide or self-harm

Encouraging, promoting, providing instructions or sharing strategies for self-harm.

Sensitive or disturbing media

Graphic Content, Gratuitous Gore, Adult Nudity & Sexual Behavior, Violent Sexual Conduct, Bestiality & Necrophilia, Media depicting a deceased individual

Impersonation

Pretending to be someone else, including non-compliant parody/fan accounts

Violent & hateful entities

Violent extremism and terrorism, hate groups & networks

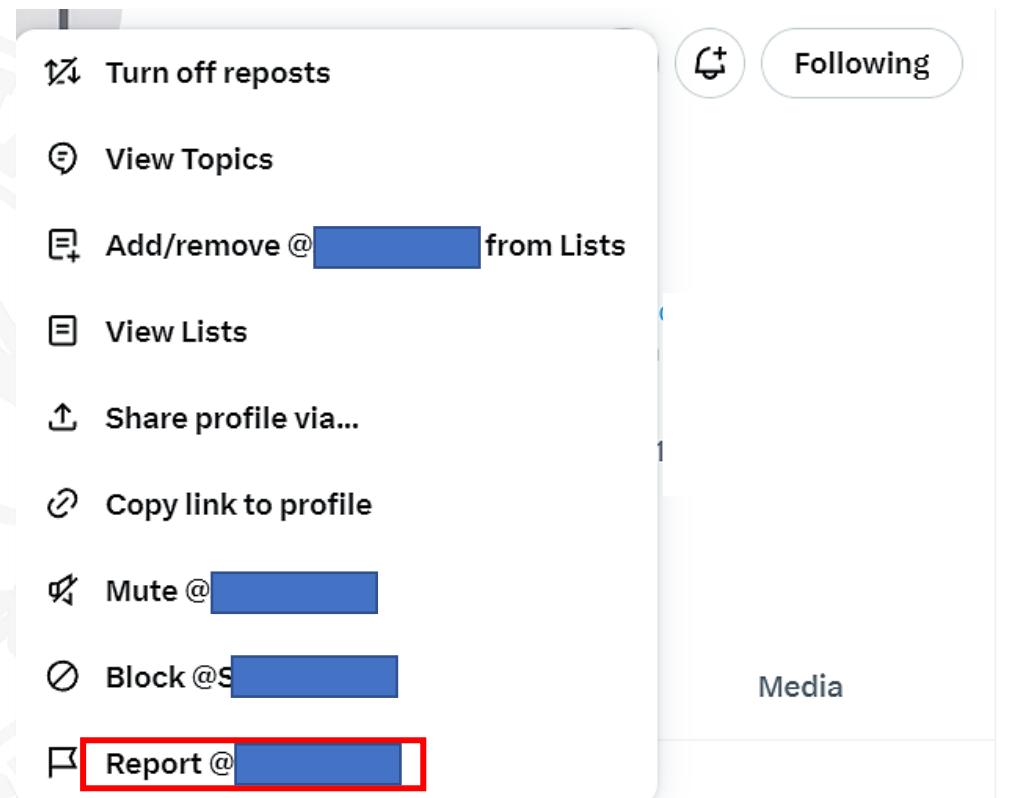
Next



José Manuel
Redondo López

¡UNA CUENTA SOLO POSTEA BURRADAS!

- ¿Ves que una cuenta solo postea burradas / intentos de estafa / mensajes automáticos / engaños / etc.?
- Se puede hacer lo mismo: **denunciar una cuenta completa**
- Nuevamente te preguntará una razón
 - Que suelen ser las mismas que a la hora de denunciar un post, como en el caso anterior
 - Y si hay varias denuncias / comprueban que es cierto, ¡adiós cuenta troll!
 - La suspensión puede ser temporal o total



Bloquear a un troll está bien, pero ¿denunciarlo y que le tiren la cuenta por tóxico/cafre? Otro rollo 😊

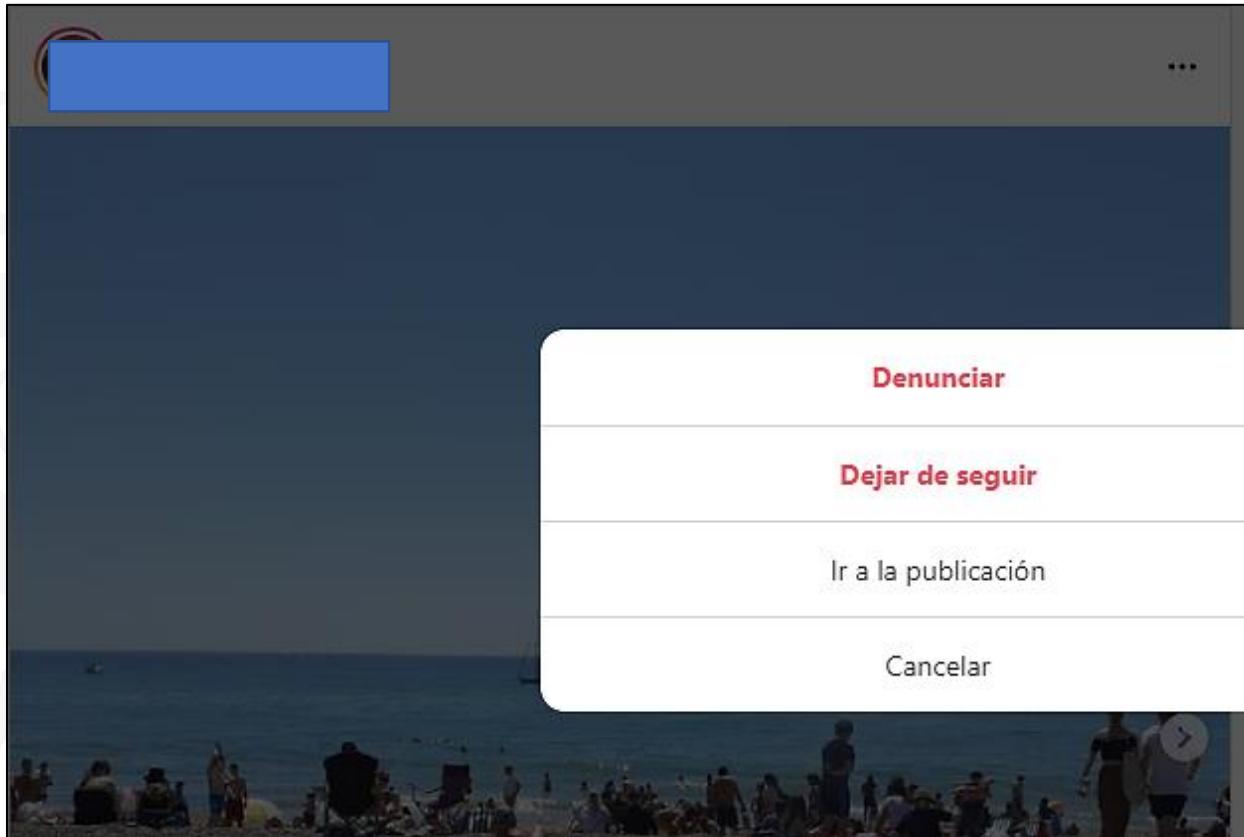
¿ESTO SE PUEDE HACER EN TODAS? ¡SÍ!

- Instagram u otras redes no son una excepción a este sistema de auto-regulación

- Haciendo esto ayudas a “limpiar” la red social de trolls
- Tampoco desesperes si la RRSS no te hace caso
 - Les interesa tener usuarios porque da dinero
- Pero a fuerza de denunciar burradas acaban cediendo

- **Recuerda:** Las denuncias son anónimas en la mayoría de las redes sociales

- **¡Pero no denuncies “por los loles” o puedes acabar tú eliminado!**
- **¡Asegúrate de tener una razón!**



- **Dejar de seguir:** Alguien que no quieras ver, pero no quieras que sepa que ya no le ves
- **Bloquear:** Alguien que no quieras ver, y quieras que sepa que te ha ofendido/hecho daño, etc.
- **Denunciar:** Alguien tan burro que no quieras que nadie más lo vea por las barbaridades que pone (diciendo a la red cuáles son)



José Manuel
Redondo López

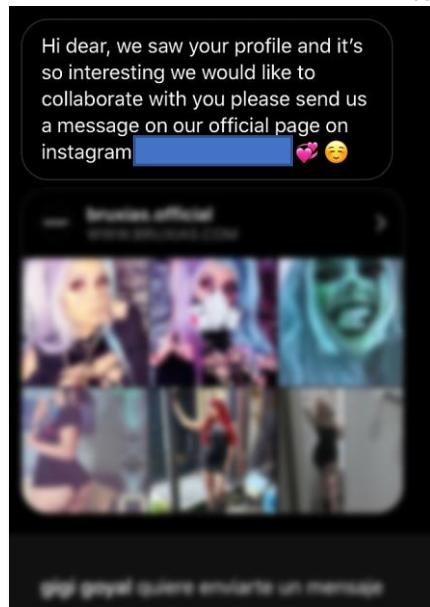
TIMOS Y ESTAFAS...¡USA LA CABEZA!

● Desgraciadamente las redes sociales están llenas de intentos de timos y estafas...y debes tener cuidado

- Cuentas falsas, Anuncios, mensajes privados...¿qué persiguen?
 - **TU DINERO** (o el de tu familia)
 - Dar datos bancarios para que te hagan una transferencia por algún concepto
 - Comprar productos o servicios que sean timos, falsos o no hagan lo que prometen
 - Esquemas tipo piramidal y otras formas similares de estafa
 - **TUS DATOS PERSONALES**: Como parte de supuestas colaboraciones, pago por un producto o servicio...
 - **TUS LIKES / FOLLOWS**
 - **¡TU CUENTA DE USUARIO ENTERA!**: Para cometer más estafas ¡en tu nombre!
- *¿Quieres conocer un testimonio sobre esto de alguien que lo ha visto de primera mano en Instagram / Bookstagram?*
 - <https://www.youtube.com/watch?v=0OAXfk1x5-s>

● Tengo un canal de YouTube (y un curso gratis, el P-45 “Audaz”) sobre estafas

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



TENED CUIDADO CON LOS PERFILES FALSOS

Han comenzado a aparecer numerosas cuentas falsas que solo buscan estafar al pedir datos bancarios con la excusa de que habéis ganado un sorteo.

Este perfil es el único oficial, y todos los sorteos se anuncian públicamente. NUNCA solicitaremos datos bancarios.

»PUCK«

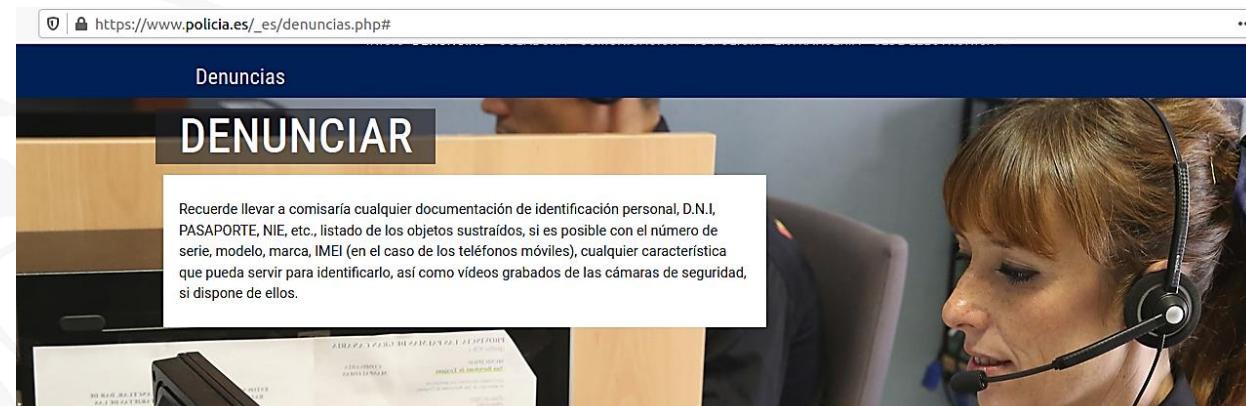
Heart icon, Search icon, Share icon, Home icon

DENUNCIAR A LA POLICÍA / GUARDIA CIVIL



José Manuel
Redondo López

- Y si ya tienes un problema...hablar con tu familia y **DENUNCIAR**
- Por ejemplo, en la página de la policía hay opciones para denunciar online
 - Y una batería de preguntas que te pueden guiar en casos comunes
- También puedes informar de muchas cosas que veas en RRSS o en Internet en general
 - https://www.policia.es/_es/colabora_informar.php?strTipo=CGSCPN#
- ¡Están para ayudarte!



DÓNDE Y CÓMO DENUNCIAR

Siempre puedes acudir a cualquier comisaría, abiertas las 24 horas del día, los 7 días de la semana.

[Ver dependencias policiales](#)

De igual manera te facilitamos la denuncia, pudiéndola hacer también por teléfono e internet.

Tramitar

Consejos de seguridad.

Programa Colectivos Ciudadanos

Comercio Seguro

Consejos en la vivienda

¿CREEES QUE LO HAS ENTENDIDO TODO? ¡AUTOEVALÚATE!

?

- *¿Entiendes que estar en redes sociales tiene en una serie de peligros, y que ciertas redes son más propensas que otras a ciertos tipos de ellos?*
- *¿Comprendes que las aplicaciones que se pueden instalar asociadas a redes sociales pueden usarse para robarte tu cuenta, y que no debes instalar cualquier cosa, aunque te la recomiende un amigo?*
- *¿Comprendes que el mecanismo de denuncia es tu principal defensa contra la aparición de contenidos o personas que sean ofensivos?*
- *¿Entiendes también que la red es uno de los principales canales de distribución de estafas?*
- *¿Y dónde debes denunciar todas las que te encuentres?*



¿QUÉ PASA CON MI INFORMACIÓN EN UNA RRSS?

Lo que tienes que saber cuando subes cosas



¿QUÉ TE VAS A ENCONTRAR EN ESTE BLOQUE?

- *• ¿Alguna vez te has planteado qué pasa con todas las cosas que subes en una red social?*
 - Pues yo te lo voy a explicar en esta sección
 - Y con lo mismo que puedes aplicarlo a tu información, también puedes estudiar la que suben los demás...
- *• ¿Te has parado a pensar que una simple foto de un lugar puede usarse para mucho más?*
 - Pues hasta te voy a poner un ejemplo de eso
 - Y de qué cosas no deberías nunca subir para que las vea todo el mundo
 - Además de otra serie de trucos para que estés más seguro
- *• Finalizando con una serie de trucos para identificar trolls, mentirosos y otro tipo de gente no recomendable*
 - Y así te puedas defender contra ellos



“SI LO SUBES A UNA RED SOCIAL, DEJA DE SER TUYO”

- La idea de que algo que subes a una red social "deja de ser tuyo" es un tema complejo con varias aristas que hay que considerar
 - Es cierto que al subir contenido a redes sociales cedes ciertos derechos
 - Pero no significa que pierdas la propiedad intelectual del mismo
- Hay que tener en cuenta lo siguiente
 - **Términos de servicio y condiciones de uso:** Al crear una cuenta en una red social, los aceptas
 - En ellos se suele incluir una sección que otorga a la red social una licencia no exclusiva, mundial y gratuita para usar, reproducir, modificar, distribuir y mostrar el contenido que subes
 - **Alcance de la licencia:** La licencia que concedes a la red social es limitada
 - La plataforma no puede usar tu contenido para lo que le de la gana, solo para los fines previstos en sus términos de servicio
 - Ej.: Mostrarlo a otros usuarios, mejorar sus servicios, promocionar la plataforma...
 - **Conservas la propiedad intelectual:** Sigues siendo el dueño de los derechos de autor de tu contenido
 - Tienes el derecho exclusivo de reproducir, distribuir, modificar y crear obras derivadas de tu contenido

“SI LO SUBES A UNA RED SOCIAL, DEJA DE SER TUYO”

- **Limitaciones a tus derechos:** Debes tener en cuenta que hay algunas limitaciones a tus derechos
 - Por ejemplo, no puedes usar tu contenido para infringir los derechos de autor de otros
 - O, por ejemplo, podrías no tener la opción de eliminarlo de la red social una vez que lo has subido

● Recomendaciones si vas a subir obras originales tuyas o contenido muy personal

- **Lee los términos de servicio** y condiciones de uso antes de crear una cuenta
 - Ya sé que es un rollo, pero hay páginas que te los resumen...
- **Comprueba la configuración de privacidad** de tu cuenta para controlar quién puede ver tu contenido
 - Lo vimos en una sección anterior
- Marca tu contenido como con **derechos de autor** si lo deseas
- **Ten cuidado al compartir contenido de terceros**, y siempre cita la fuente
- **Guarda copias de tu contenido** en un lugar seguro
 - Te pueden cerrar la cuenta, y con ello perderías acceso a todo lo que has subido
- Y recuerda que **alguien podría usar tu propio contenido contra ti** si no cuidas lo que subes
 - Veamos este último aspecto a continuación

¿QUÉ PASA CON LAS FOTOS QUE SUBIMOS?

- Más allá de lo que ya hablamos de la publicidad: lo que subes puede dar información a otras personas que lo leen...a veces demasiada
- Especialmente fotos o videos (fotogramas de ellos)...
 - Con ellos puedes hacer **búsqueda inversa** -> obtener el sitio **dónde se hizo** la foto
 - Si posteas muchas fotos, con eso pueden saber tus **rutas habituales** (dónde vives, colegio, gimnasio,...) -> **tus costumbres**
 - Si posteas con quien estás -> **amigos** -> **grupos** -> **tu clase**
- ¡Analiza lo que subes como si fueras el profesor Layton!: Cómo mirar con “ojos de hacker”
- *¿No me crees? Espera...*





BÚSQUEDA INVERSA EN GOOGLE

¡Vale para cualquier imagen sospechosa!: persona, producto, piso, calle, ...

¡ASÍ PODEMOS DETECTAR PERFILES FALSOS! (Catfishing)

¡Puedes “Recortar” cualquier imagen de la pantalla con la herramienta “Recortes” de Windows!

La guardamos en un fichero, y arrastramos y soltamos el fichero en la búsqueda de Google

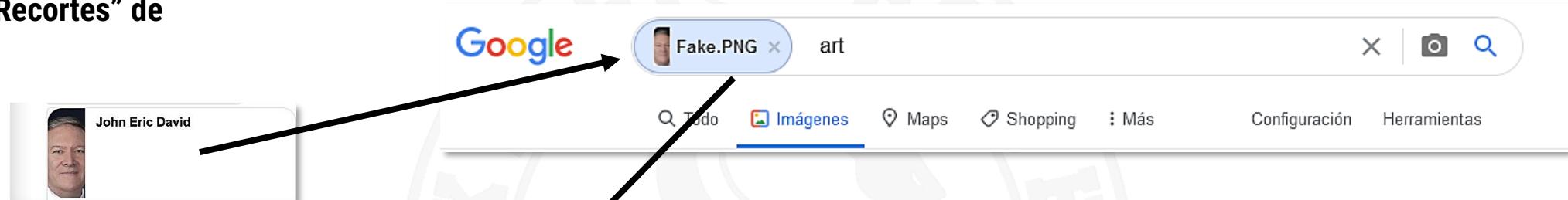


Imagen de perfil recortada
Y “sospechosa”

Aparece un artículo con esa imagen más completa escrita por Mike Pompeo (ex-Secretario de Estado de EEUU)

Sanciones en Siria - Prisionero en Argentina

 150 × 150 - 30 jul. 2020 - Por Michael R. Pompeo, Secretario de Estado de Estados Unidos de América Hoy, el Departamento de Estado y el Departamento del Tesoro ...

<https://www.osi.es/es/actualidad/blog/2018/06/06/detectando-fraudes-me-suena-esta-foto>

Efectivamente, es él y la imagen del perfil es **FALSA**





IMÁGENES QUE DICEN SER DE ALGO...PERO ES MENTIRA



"Chilling with the bros in the mountain"

- Cualquier imagen de una web que te resulte sospechosa admite este tratamiento
- ¿Encuentras imágenes falsas? No te fíes de esa web

Tamaño de imagen:
1116 x 513
No se ha encontrado esta imagen en otros tamaños.

Posible búsqueda relacionada: [tree](#)

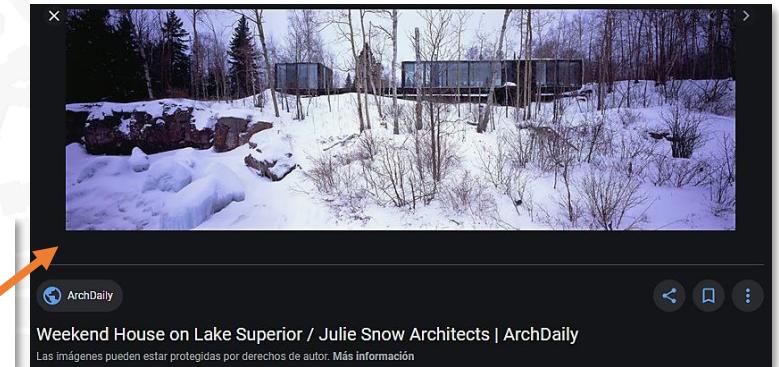
Búsqueda en Google Images

[en.wikipedia.org › wiki › Tree](#) Traducir esta página
[Tree - Wikipedia](#)
In botany, a **tree** is a perennial plant with an elongated stem, or trunk, supporting branches and leaves in most species. In some usages, the definition of a **tree** ...

[en.wikipedia.org › wiki › Tree_\(da...\)](#) Traducir esta página
[Tree \(data structure\) - Wikipedia](#)
In computer science, a **tree** is a widely used abstract data type that simulates a hierarchical **tree** structure, with a root value and subtrees of children with a parent ...

Imágenes visualmente similares

¡La foto!



Todo es mentira, es una casa de un estudio de arquitectura. Esto es más frecuente de lo que te crees en páginas de alquileres de pisos. ¡Díselo a tus padres!



José Manuel
Redondo López

¡MIRA COMO DISFRUTO EN ESTE SITIO!...MMM ¿SEGURO?



"De vacaciones por la sierra de Andalucía"

<https://www.turismoasturias.es/rutas/senderismo/ruta-del-cares> ▾

Ruta del Cares. Rutas en Asturias - Turismo Asturias

Ruta del Cares. Rutas en Asturias ... A pie 6 h. 15 min. ... Hacer la ruta, Poncebos-Caín ida y vuelta, supone caminar unos 22 km, distancia que no es apta para ...

<https://www.escapadarural.com/planes/rutas/ruta-del-cares> ▾

Todo lo que necesitas saber para hacer la Ruta del Cares

12 jul 2016 — Longitud: 12 km (24 km ida y vuelta). · Duración: 6 horas aproximadamente. · Dificultad: medi.a · Desnivel: Prácticamente llano todo el recorrido, ...

Imágenes visualmente similares





José Manuel
Redondo López

¡MIRA COMO DISFRUTO EN ESTE SITIO!...MMM ¿SEGURO?



"¡De vacaciones por Toledo!"

<https://buendiatours.com/guias/casco-antiguo> ▾

Casco antiguo de Oviedo | Buendía Tours

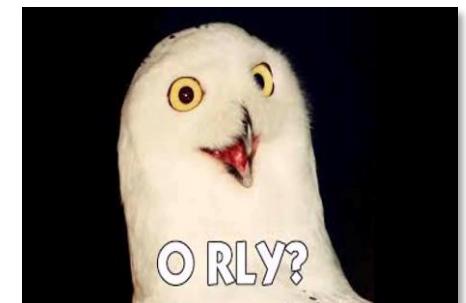
Casco antiguo de Oviedo. El casco antiguo, o el "Oviedo antiguo" como se le llama en la ciudad, es la ciudad medieval que estaba dentro de la ...

<https://asturias.com/el-casco-historico-de-oviedo> ▾

El casco histórico de Oviedo. Qué ver en Oviedo Asturias ...

4 feb 2021 — La vamos dejando a nuestra derecha y tomamos la calle Magdalena camino ya de El Fontán, plaza emblemática del Oviedo Antiguo que se ha ...

Imágenes visualmente similares



¡Te saca hasta las imágenes similares del sitio! (lo cual te da aún más contexto para "investigar")



IMÁGENES QUE DICEN MÁS DE LO QUE PARECE...

- Este método no es en absoluto infalible
 - Pero probar a ver qué pasa no está mal... ☺
- Como os decía, si se publican varias imágenes, se puede llegar a “triangular” a la persona
 - Averiguar su rutina, gustos, aficiones, rutas... (hay gente que postea su vida)
 - Incluso muchas veces la propia persona geolocaliza la imagen, así que no hace falta investigar nada
 - Por eso todo este tema de “cuidado con lo que se publica” ☺



"Vistas desde mi casa"

Aproximadamente 299 resultados (1,08 segundos)



Tamaño de imagen:
1200 × 900

Buscar esta imagen en otros tamaños:
[Todos los tamaños](#) - [Pequeño](#) - [Mediano](#) - [Grande](#)

Possible búsqueda relacionada: [puertollano españa](#)

Ups...ahora ya
saben dónde
vives...



IMÁGENES QUE DICEN MÁS DE LO QUE PARECE...

- Google Earth puede hacer magia...



¿QUÉ ES LO QUE NUNCA DEBEMOS SUBIR?

● Nunca subas

- **Billetes de tren, avión:** con la numeración pueden saber demasiado
- **Tarjetas de crédito o nºs de cuenta** (compras fraudulentas)
- **El ID de una avión o medio de transporte grande** (¡pueden saber tu ruta exacta!)
- **Cosas demasiado personales / que alguien pueda usar en tu contra**
- **Si te vas de casa / vacaciones**, etc... (casas deshabitadas)
 - A posteriori lo que quieras. ¿Mientras estás? ¡NO!
- ...

Piensa “**como un malo**” y responde la siguiente pregunta
¿*Cómo podría usar yo esto que voy a subir para el mal?*

Si tienes una respuesta, NO lo hagas (y, sino sabes, pregunta a tu familia / profesores)

Fuente: <https://www.incibe.es/ciudadania/formacion/infografias/7-datos-que-nunca-debes-compartir-en-internet>



¿QUÉ ES LO QUE NUNCA DEBEMOS SUBIR?

● ¿Crees que esto solo aplica a menores?

- ¡No! También a cualquier mayor de edad
- Por temas personales, laborales, etc.

● Los de cierta generación son quizá los que más problemas dan en ese sentido

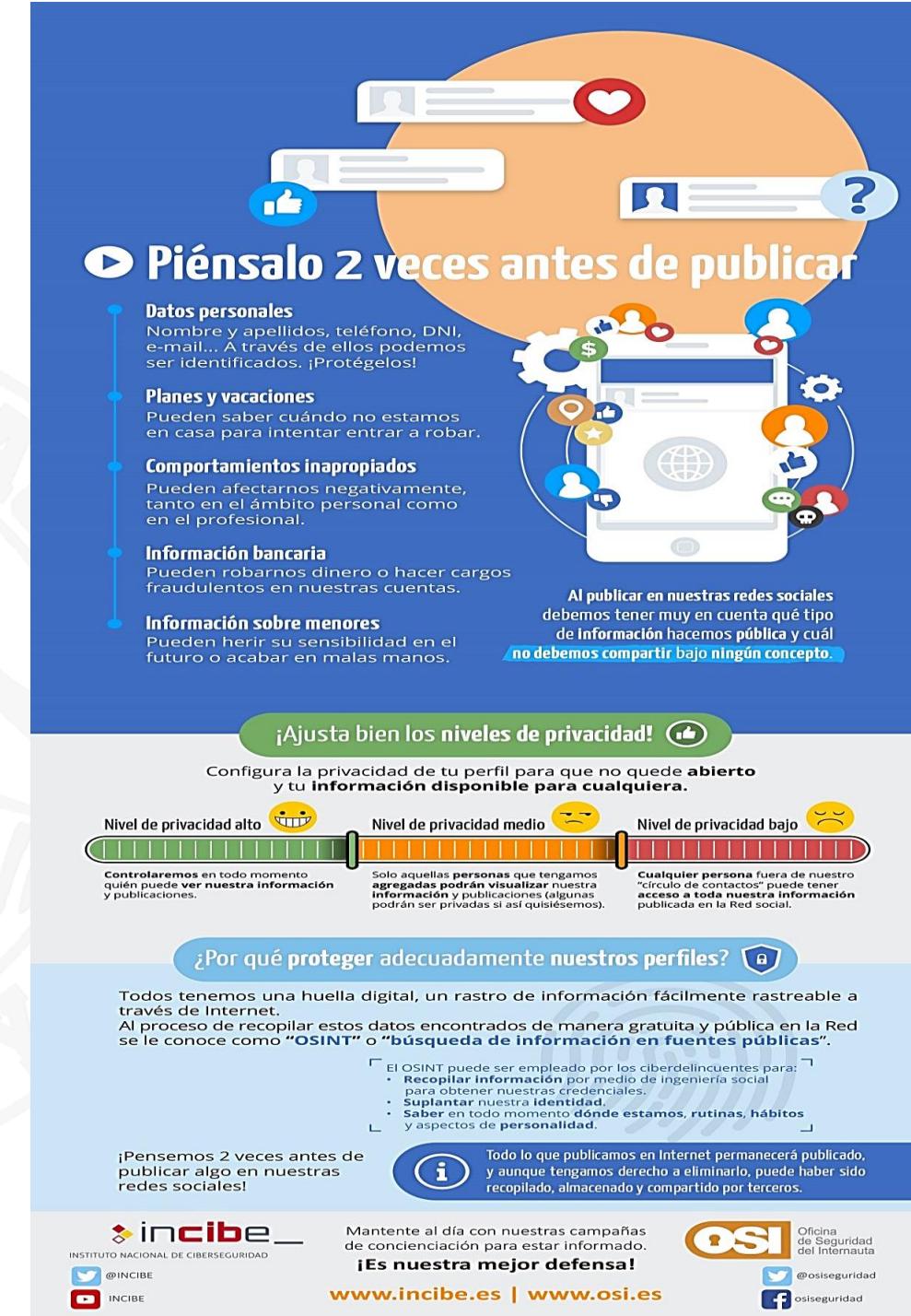
- ¡Les encanta postear de todo, sin entender las consecuencias!
- Y es una generación poco sospechosa de ser menor ;)

● ¡Pon sentido común en tu casa y edúcales!

● Este video de Sarina Abdullah sobre el tema es muy revelador

- <https://www.youtube.com/watch?v=35caskf6YJg>

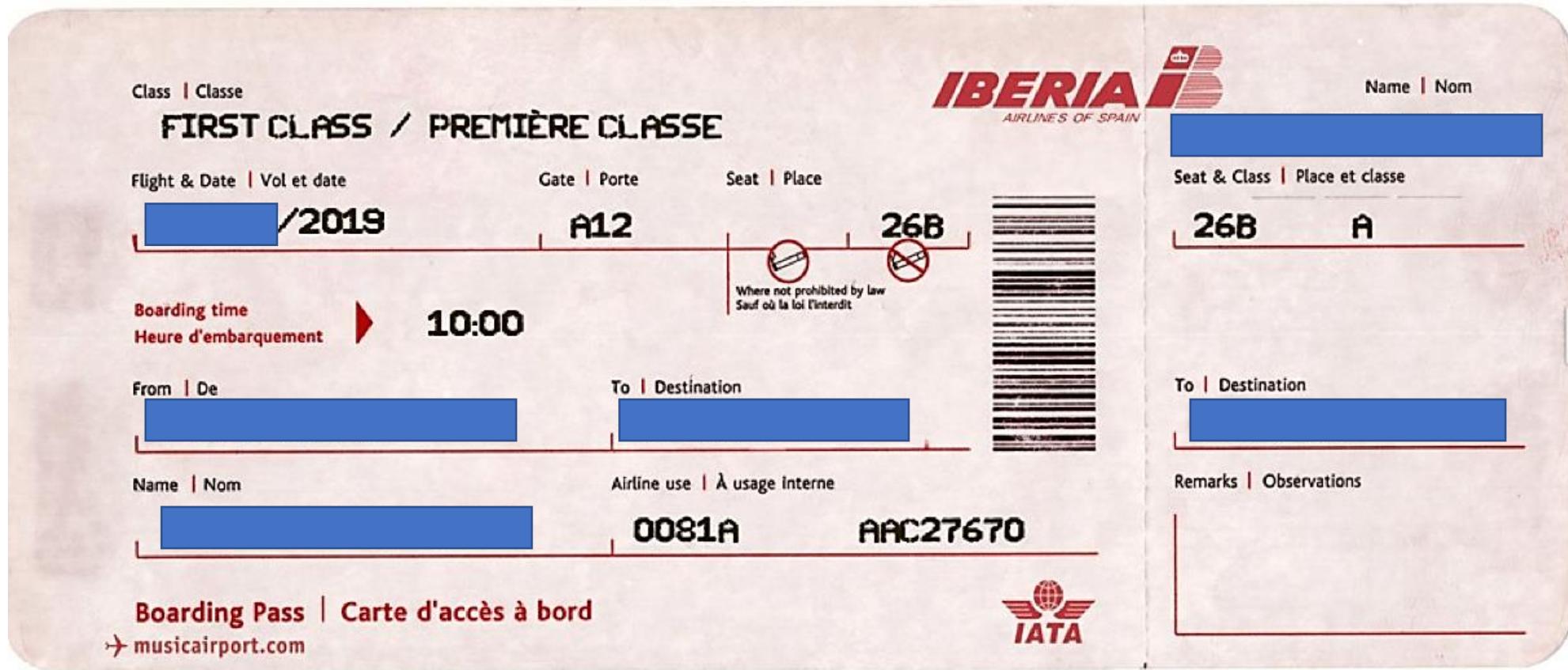
Fuente: <https://www.incibe.es/ciudadania/formacion/infografias/piensalo-2-veces>





José Manuel
Redondo López

EJEMPLO: BILLETE DE AVIÓN



Cuando te vas, dónde te vas, cómo te vas...



NºS DE VEHÍCULOS DE TRANSPORTE

- Saber el identificador de un avión y el día aproximado de un viaje da mucha información a quien quiera saberla
- Hay páginas que muestran toda esa información... ¡gratis!
 - ¡Sabrán todo de tu viaje! ¡Hasta si has llegado tarde!
- Otros medios de transporte pueden tener el mismo problema
 - Así que **¡no lo hagas!**
- Otras cosas que **nunca debes postear**: Tu DNI, tus tarjetas, entradas de conciertos...



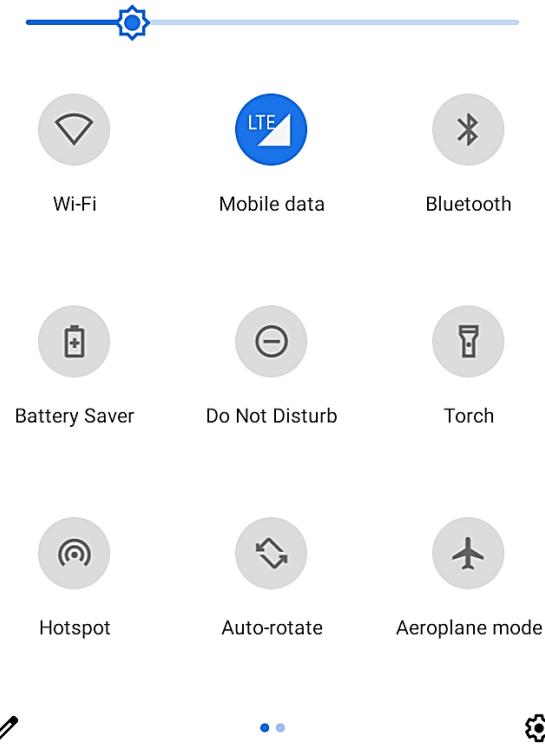


José Manuel
Redondo López

¿Y QUÉ MÁS PUEDO HACER?

● Se un usuario **ACTIVO** de tu teléfono

- Desactiva lo que no uses (datos cuando uses Wifi, Bluetooth si no lo usas, tu posición si estás en casa, etc.)
 - Es ecológico ☺ (ahorras batería)
- Pero evita problemas de que “se filtren” cosas



● Dile a tu familia donde vas a estar, por si acaso

- Lo que vas a hacer, depende ya de ti ☺
- Mejor que sepan donde buscarte, ¿no?
- ¡Confiar en alguien estas cosas es una buena forma de evitar problemas!

● Usa las redes sociales vía navegador web mejor que usando su app (si te dejan)

- Se filtran menos datos tuyos de esta forma, ¡créeme!
- ¿Por qué crees que te insisten tanto en que te la instales? ;)

¿CREEES QUE LO HAS ENTENDIDO TODO? ¡AUTOEVALÚATE!



- *¿Entiendes que una vez que subes algo a una red social deja de ser tuyo?*
- *¿Has comprendido el peligro que tiene subir ciertas cosas a las redes sociales, por la información que pueden sacar de ellas?*
- *¿Te das cuenta de que hay que mantener una serie de medidas de “higiene” a la hora de manejar tanto las redes sociales como tus teléfonos móviles?*



🤔 La persona detrás de una cuenta de una red social

¿Se pueden averiguar cosas, aunque la cuenta no refleje una identidad real?



¿Y QUÉ HAGO CON LOS TROLLS?

- En las redes sociales hay bots o trolls. Es un hecho, no algo cuestionable
 - La forma más rápida de intentar averiguar si una cuenta es falsa es la búsqueda en Google Images de la foto de perfil que vimos en la presentación anterior
 - *¿Es la imagen de otra persona? ¿de un catálogo?* **FALSO**
 - El problema es que ahora **muchas son generadas por IA**, y no se pueden distinguir de esta forma
- Por otro lado, si alguien así te está acosando, lo mejor es **denunciarlo a la policía** en caso de que cometa un delito
 - Si publica **fotos de sitios y lugares** (o fotogramas de un video), una búsqueda de imágenes saca fotos visualmente similares...que podrían ser del mismo sitio y estar geolocalizadas
 - Lo vimos antes
 - Con ello, averiguarás más o menos por dónde vive o por dónde pasa
 - Y probablemente así sepas más fácilmente quién puede ser (**datos para la denuncia**)
 - No obstante, esto es más frecuente usarlo **para detectar fraudes**

TÉCNICAS BÁSICAS PARA IDENTIFICAR “TROLLS”

● *¿Y si esto no funciona?*

- A veces en la **información extendida pública** de la cuenta aparece el identificador original que se usó para crearla
 - Que puede ser el nombre real de la persona (que luego cambió por otro anónimo)
- **El mismo id de usuario** se puede usar en distintas redes sociales / foros / perfiles de juegos
 - Y en algún sitio de ellos puede aparecer su nombre real (mención de un amigo, foto...)
 - Lo veremos en la siguiente hoja
- **El nombre de su web personal** (si tiene) puede delatarlo
- **Inferencia por lo que escribe:** provocar que diga un dato que solo poca gente sabe
 - Deducción detectivesca over 9000 😊
- **Con quién se relaciona:** ¿hay confianza con alguno de sus allegados? Pregunta
- **A quien le da/no le da like:** Muchos se dan like a si mismo cuando postean con otra cuenta “pública”
 - **Si critica a una persona mucho**, no descartes que sea él mismo (para desviar la atención)
 - **Si defiende a ultranza a otra persona** aparentemente sin relación, es probable que estés a ante una “cuenta B” de esa persona (muchos streamers famosos lo hacen 😊)
- O también puedes identificarlo por **cómo se comporta...**

EL IDENTIFICADOR DE UNA RED SOCIAL PUEDE DECIR MUCHO

- El identificador que alguien usa en las redes sociales puede ser delator

- Puede usar el mismo en muchas redes distintas, unas protegidas y otras no
- Puede tener alguna página registrada con ese pseudónimo

- Hay webs que averiguan esta información por ti

- <https://namechk.com/>
- <https://www.namecheckr.com/>

En rojo tienes las redes sociales donde hay registrado alguien con el pseudónimo que he puesto. ¿Será la misma persona en todas? 😱

Usernames

 Facebook

 YouTube

 Twitter

 Blogger

 Twitch

TikTok

 Shopify

 Reddit

 Ebay

 Wordpress

 Pinterest

 Yelp

 Slack

 Github

 Basecamp

 Tumblr

 Flickr

 Pandora

Show more



De verdad que parece una tontería, pero pasa más a menudo de lo que crees. La gente tiende a usar el mismo pseudónimo en distintos sitios, y lo hace con él en algunos...

IDENTIFICANDO CUENTAS FALSAS / BOTS POR COMPORTAMIENTO

- Es cierto que hoy en día en las redes sociales hay muchas fake news y muchas cuentas encargadas de propagarlas
- ¿Cómo las identifico?
 - **SENTIDO COMÚN**: Si dice cosas que parecen inverosímiles, es una mentira 😊
 - **Múltiples mentiras**: Si a la cuenta le han “pillado” en varias mentiras, raro será que mentir / manipular constantemente no sea uno de sus objetivos
 - Ya vimos que hay cuentas dedicadas al “fact check”, pero también pueden quedar “retratados” en los comentarios
 - **Es una cuenta con “comportamientos extraños”**: Esto solo son indicios de sospecha, no quiere decir que todas las cuentas que hagan algo así lo sean (puede haber una razón legítima para hacerlo)
 - Ha cambiado frecuentemente de nombre (*¿por qué? ¿hizo algo grave con su antiguo nombre?*)
 - Borra muchos mensajes (*¿tiene frecuentes “pilladas”?*)
 - Hace “limpias” de seguidores arbitrarias, dirigidas a un tipo de seguidor, o contrarios a su opinión (*¿es que elimina las críticas/“pilladas” que le hacen?*)
- Veamos ejemplos de ello en Twitter (nadie la llama X 😊)

CAMBIOS DE NOMBRE

- Se pueden descubrir con una búsqueda en Twitter sencilla

- El procedimiento de búsqueda es

- `to:<nombre de cuenta> until:<año>-12-31`
 - <año> es el año de creación de la cuenta
- Ejemplo, dado que el presidente de España en 2024 creó su cuenta en 2009, se haría:
 - `to:sanchezcastejon until:2009-12-31`
- Pulsamos en “Más Reciente”
- Si no sale ningún resultado, cambiamos al año siguiente y repetimos el proceso

- En los resultados vemos que las respuestas están dirigidas al mismo id. de usuario

- El presidente no ha cambiado de nombre



A screenshot of a Twitter search results page. The search bar at the top contains the query `to:sanchezcastejon until:2009-12-31`. Below the search bar, there are tabs for **Destacado**, **Más reciente** (which is selected), **Personas**, **Fotos**, and **Videos**. The results show four tweets:

- Ramón Ramón** (@ramonramon) - 29 sept. 2009: En respuesta a @sanchezcastejon @sanchezcastejon felicidades por esa nueva responsabilidad, te deseo muchos éxitos y progresos. (1 reply, 1 retweet, 1 like)
- Jorge Martínez** (@jorgermp) - 18 sept. 2009: En respuesta a @sanchezcastejon @sanchezcastejon en un zip? (1 reply, 1 retweet, 1 like)
- Jose Vicente Espino** (@JoseviEspino) - 18 sept. 2009: En respuesta a @sanchezcastejon @sanchezcastejon Ánimo amigo!!! (1 reply, 1 retweet, 1 like)
- Jose Vicente Espino** (@JoseviEspino) - 15 sept. 2009: En respuesta a @sanchezcastejon @sanchezcastejon Espero que tengas mucha suerte y éxito en tu nueva etapa. Estoy seguro que darás todo por nuestros valores. Un abrazo (1 reply, 1 retweet, 1 like)



José Manuel
Redondo López

CAMBIOS DE NOMBRE

- En cambio, este usuario sí que ha cambiado de identificador
 - Aunque esto por sí solo no quiere decir nada
 - ¡Mucha gente lo hace!
- Es un dato a tener en cuenta nada más...
 - Pero ahora sabes cómo averiguarlo con una búsqueda
- Es más sospechoso si los cambios son frecuentes cuando se va recorriendo el “historial” de la cuenta

Roberto Benito @robertobenito · 21 dic. 2011
En respuesta a @javiernegre10
@javiergnegre No sé yo si Rajoy va a confiar a Gallardón la gestión del alto el fuego de ETA.

Roberto Benito @robertobenito · 21 dic. 2011
En respuesta a @javiernegre10
@javiergnegre No se me ocurre un nombre en el PP con un perfil más parecido al de Chacón.

Marcos Iriarte @MarcosIriarte · 21 dic. 2011
En respuesta a @javiernegre10
@javiergnegre Le tiene cariño porque le vio crecer...

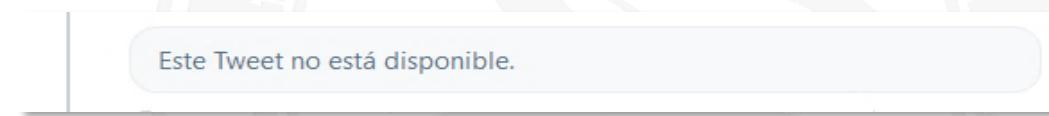
Manuel Regalado @titoregalado7 · 20 dic. 2011
En respuesta a @javiernegre10
@javiergnegre Hombre, el inefable Javi Negre! Muy bien, tío. Currando un poquillo. Mán arriba a las seis. Abrazo. Q tal tú x el norte?

@javiernegre10 antes era **@javiernegre**. Se ha cambiado de nombre por algún motivo, al menos 1 vez

BORRADO DE TWEETS

- Si un usuario ha borrado tweets o no se puede comprobar fácilmente haciendo clic en sus respuestas para verlas en detalle

- Como, por ejemplo, las obtenidas en el proceso anterior
- Si existe una respuesta a un tweet, pero al entrar a ella vemos esto:



- Implica que **el usuario ha borrado ese tweet**
- *¿Tiene muchos tweets borrados? Sospecha*
 - Implicaría que puede haber dicho cosas falsas / por las que le han denunciado / desmentidas y ha tenido que borrarlas
 - Si son muchos casos, es un potencial mentiroso habitual...

TEMÁTICAS

- Si en lugar de to: usamos from: (from:<nombre de cuenta> until:<año>-12-31 veremos los tweets hechos por la cuenta, no las respuestas que tuvieron

- Si hacemos un recorrido histórico por ellos, podemos ver si la temática de los mismos ha cambiado, o la forma de expresarse
- @norcoreano por ejemplo ha pasado de ser una cuenta de humor a una cuenta con fuerte contenido de crítica política
- ¡Ojo! **Eso no es malo**, es un hecho a considerar por si es útil para alguna investigación nada más



from:norcoreano until:2011-12-31

	Destacado	Más reciente	Personas	Fotos	Videos	
1	 Kim Jong-un @norcoreano · 30 dic. 2011	A ver si nos enteramos, aquí no prohibimos internet, lo que prohibimos es acercarse a la frontera y para pillar Wifi hay que acercarse.	...	6	2	↑
2	 Kim Jong-un @norcoreano · 30 dic. 2011	La libertad es el opio del pueblo.	...	22	4	↑
3	 Kim Jong-un @norcoreano · 30 dic. 2011	He convocado las primeras oposiciones de 2012, 10 plazas de funcionario para rascarme la espalda.	...	7		↑
4	 Kim Jong-un @norcoreano · 30 dic. 2011	Si el pueblo no come es culpa mía, si se muere gente también, a ver si va a ser culpa mía que tengan cara de chonris...	...	1	5	↑

from:norcoreano until:2019-12-31

	Destacado	Más reciente	Personas	Fotos	Videos		
1	 Kim Jong-un @norcoreano · 30 dic. 2019	Si Cristina Pedroche quiere vestirse de otro año de mamarracha para llamar la atención, está en su derecho y nosotros no somos nadie para criticarla.	...	38	246	1 mil	↑
2	 Kim Jong-un @norcoreano · 28 dic. 2019	Hoy es el Día de los Inocentes, felicidades a todos los que casi en 2020 siguen creyendo en Dios, en el horóscopo y en el marxismo-leninismo.	...	73	811	2,7 mil	↑
3	 Kim Jong-un @norcoreano · 27 dic. 2019	Si León se independiza, espero que su himno nacional sea Hakuna Matata.	...	31	423	1,6 mil	↑
4	 Kim Jong-un @norcoreano · 27 dic. 2019	Tomándome una caña en una terraza al sol en plena Navidad. Esto es lo que quiere quitarnos Greta Thunberg.	...	27	753	2,7 mil	↑

¿ES UNA CUENTA SOSPECHOSA ENTONCES?

● Por tanto

- Si nos encontramos con una cuenta de usuario que ha tenido **varios cambios de nombre**
- Cada vez que cambia de nombre “**muta**”
 - Habla de noticias de distintas ideologías, apoya posturas contrapuestas, se le descubren diferentes bulos...
 - Hay personas que son una especie de “ciber-mercenarios” de opiniones: ja cambio de dinero hablan bien de lo que les digan!
- Y además **borra muchos tweets** (probablemente por cada cambio de nombre borre un buen puñado de ellos)
- Entonces...



Y AHORA DAROS CUENTA DE UN DETALLE...

● **CUIDADO con las redes sociales**

- **Se clonian perfiles** con fotos con fines ilegales / destrucción de reputación
- Si publicas tu foto en sitios, aunque no estén geolocalizadas **se podrían identificar esos sitios**: dónde vives, por donde paras, con quien andas...
- Si ya los geolocalizas tú mismo/a, entonces revelas tus rutinas (qué días publicas en qué sitios)
- Facilitas la vida a posibles ciber-acosadores... ☹

● **Si mientes, también pueden pillarte (¡acabamos de verlo!)**

● **Y, si cometes un delito, VAN A PILLARTE**

- La policía puede, bajo denuncia, acceder a muchos más datos que tú pidiéndolos a redes sociales / proveedores de Internet: tu IP, horas de conexión...
- Solución: **¡NO COMETAS DELITOS!**



PRECIOS EN LA DARK WEB DE LOS DATOS QUE NOS ROBAN

¿A cuánto el kilo de dato privado?



¿QUÉ TE VAS A ENCONTRAR EN ESTE BLOQUE?



- *¿Nunca te has planteado por qué hay tanto robo de datos privados y de cuentas en internet?*
- Pues en esta sección vas a ver que hay un mercado para ello y que hay gente que compra, aunque sea ilegal
- Así que como fin a esta presentación te voy a enseñar un estudio
 - Dónde vas a ver los precios que tienen determinada información robada en la web oscura (dark net)
 - Que es donde se venden estas cosas...
- Así que ten cuidado porque tu actividad en redes sociales
 - Tu información y otros datos es una mercancía que alguien puede estar interesado en comprar para hacer diferentes delitos

PRECIOS EN LA DARK WEB DE LO QUE MÁS DEBEMOS DEFENDER

- La presencia de tiendas de servicios ilegales en la dark web se ha incrementado en los últimos años, y va en ascenso
 - Aunque se han cerrado varios de ellos, en general ha habido **un aumento de su presencia**
 - Debes saber que tus datos valen dinero en ellos, y por eso se roban
- Entiende que el mercado de contenidos fraudulentos de la dark web es una realidad y que no es algo que vaya a desaparecer
 - Los delincuentes roban datos **porque su venta les es rentable**
 - Existen investigaciones recientes acerca del tipo de cosas que se venden en él y sus precios
 - Vamos a usar como base para este apartado una de ellas: <https://www.privacyaffairs.com/dark-web-price-index-2023/>
 - El comercio ilegal de datos es un negocio floreciente y que pone en peligro a cualquiera

PRECIOS EN LA DARK WEB DE LO QUE MÁS DEBEMOS DEFENDER

● El informe referenciado detectó también cambios significativos en las operaciones de la Dark Web

- **No hay un líder claro del mercado:** El cierre de muchos sitios “grandes” dio lugar a muchos más “pequeños”, pero que duran poco tiempo
 - La oferta de bienes no ha disminuido, pero se reparte más
 - Es una respuesta de los criminales a las operaciones policiales
 - El objetivo es **evadir mejor la acción de las fuerzas del orden** al borrar cualquier evidencia en solo unos pocos meses
 - También evitan ser lo suficientemente grandes como para **llamar demasiado la atención**
 - Es una especie de “guerra de guerrillas”
- **Telegram en lugar de sitios web:** Telegram se ha convertido en un canal importante para facilitar la venta de datos personales pirateados
 - Existen muchos canales con gran cantidad de usuarios para vender estos bienes obtenidos ilegalmente
 - También se usa para anunciar la creación de nuevos sitios de venta de artículos delictivos

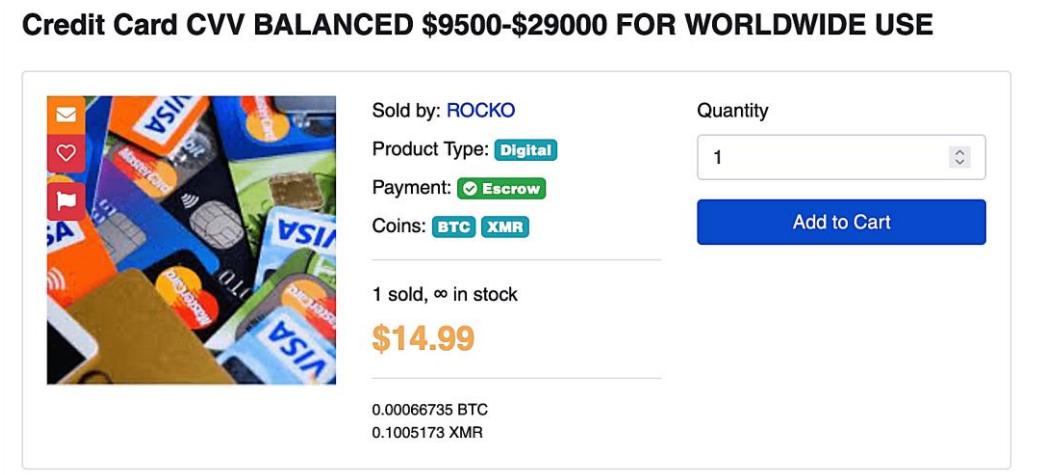
PRECIOS EN LA DARK WEB DE LO QUE MÁS DEBEMOS DEFENDER

- El estudio referenciado es un índice de precios de productos de dark web en 2023

- Ha analizado varios mercados, foros y sitios web de la dark web
- Procesando la información para calcular el promedio de precios para una gama de productos ilegales muy amplia

- Tarjetas de crédito clonadas y datos del titular de la tarjeta

- En diciembre de 2022, se estima que **7,5 millones de tarjetas de crédito** estaban disponibles en la dark web



Los pagos en criptomonedas por estos productos permiten el anonimato. Esto es un requisito, teniendo en cuenta que se trata de un mercado del crimen...

PRECIOS DE DATOS DE TARJETAS DE CRÉDITO

- Estos son los precios de tarjetas de crédito, incluso con cierto saldo en cuenta
- Todas con el código CVV para poder usarlas en compras online
- Como puedes ver, el precio permite hacer una compra grande por mucho menos de lo que vale
- Hay tarjetas robadas de todos los países

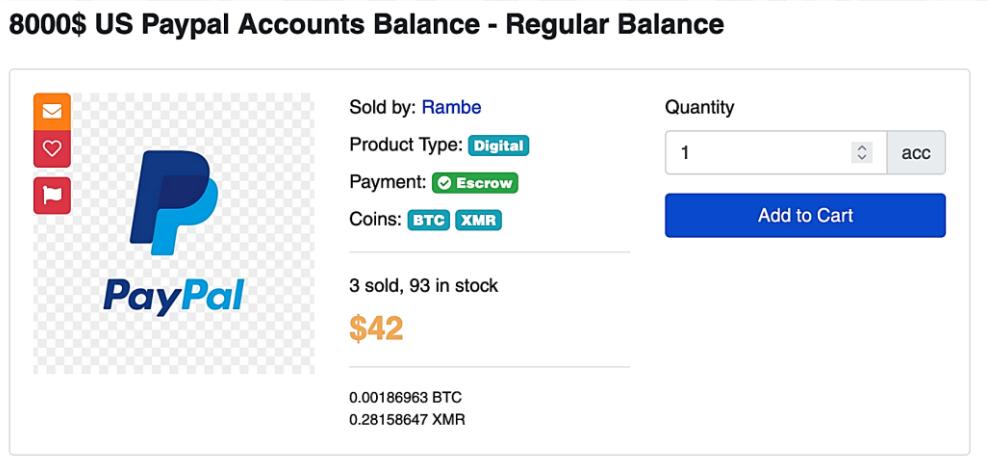
Credit card details, account balance up to 5,000	\$110
Card.com hacked account	\$75
Credit card details, account balance up to 1,000	\$70
Stolen online banking logins, minimum 2,000 on account	\$60
United Arab Emirates credit card with CVV	\$35
Stolen online banking logins, minimum 100 on account	\$40
TDBank hacked account	\$30
Canada hacked credit card details with CVV	\$30
Australia hacked credit card details w/ CVV	\$23
Israel hacked credit card details with CVV	\$20
Spain hacked credit card details with CVV	\$20
UK hacked credit card details with CVV	\$20
Cloned American Express with PIN	\$20
Cloned Mastercard with PIN	\$20
Cloned VISA with PIN	\$20
USA hacked credit card details with CVV	\$15
Hacked (Global) credit card details with CVV	\$10
Walmart account with credit card attached	\$5

Fuente: Investigación de precios en la dark web de Privacy Affairs
(<https://www.privacyaffairs.com/dark-web-price-index-2023/>)

PRECIOS EN LA DARK WEB DE LO QUE MÁS DEBEMOS DEFENDER

• Servicios de procesamiento de pagos online

- Cuentas en servicios de pagos desde móvil, procesadores de pago, etc. son cada vez más populares en estos mercados
 - Da más oportunidades de robar los datos personales y la información financiera de las personas
- El tipo de cuenta más común **es la de PayPal**
- Debido a que hay tantos servicios de este tipo disponibles, su precio es bajo
 - Es más caro transferir dinero desde una cuenta pirateada



Prácticamente hacemos casi todas las compras online, por lo que como mínimo deberíamos tener un 2FA activo en cada cuenta que tengamos en este tipo de servicios. Ya vemos que es una mercancía a la venta muy común...

PRECIOS DE SERVICIOS DE PROCESAMIENTO DE PAGOS

- Las cuentas robadas en servicios de banca y de pagos tienen unos precios dispares
- En bancos suelen ser más caras, en función del tamaño de este
- Los servicios de pago suelen ser más baratos, probablemente al ser cuentas más efímeras
- Llama la atención la compra de transferencias desde cuentas de PayPal robadas
 - Se usan para timos en ventas

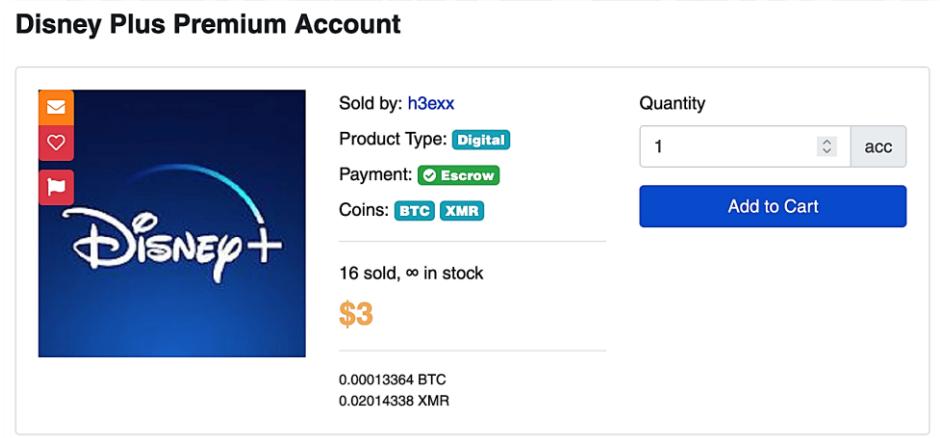
ING bank account logins (verified account)	\$4,255
HSBC UK Business account	\$4,200
Switzerland online banking login	\$2,200
Barclays online banking login	\$2,100
Santander personal bank account	\$1,800
Revolut verified account (UK, USA)	\$1,600
Verified Stripe account with payment gateway	\$1,200
Cashapp verified account	\$860
Stolen UK fully verified Skrill account details	\$610
Chase Bank login	\$500
Hacked Weststein Card account	\$500
Hacked TransferGo account	\$500
Payoneer verified account	\$200
CitiBank verified account	\$200
Wells Fargo banking login	\$150
Chime Bank account login	\$125
50 Hacked PayPal account logins	\$120
Hacked PerfectMoney account	\$100
Luno Account together with a balance of \$5,000	\$80
Bluebird Bank account login	\$75
Go2Bank hacked account	\$60
Huntington bank account login	\$60
PayPal transfer from stolen account, \$8,000+ balances	\$54
Hacked Western Union Account	\$39
Western Union transfer from stolen account, \$1,000+ balances	\$32
Bank of America account login	\$30
PayPal transfer from stolen account, \$1,000 – \$3,000 balances	\$30
Suntrust Bank account	\$30
PayPal transfers from stolen account, \$100-\$1,000 balance	\$25
CBA Random Bank login	\$25
PayPal transfer from stolen account, \$5,000+ balances	\$22
Stolen PayPal account details, no balance	\$15
Movo.Cash Login	\$11
Stolen PayPal account details, minimum \$1,000 balances	\$10
Stolen PayPal account details, minimum \$100 balances	\$10

Fuente: Investigación de precios en la dark web de Privacy Affairs (<https://www.privacyaffair.s.com/dark-web-price-index-2023/>)

PRECIOS EN LA DARK WEB DE LO QUE MÁS DEBEMOS DEFENDER

• Servicios en línea y cuentas de entretenimiento robadas

- Las cuentas de redes sociales robadas se pueden usar para **propagar estafas o desinformación** con una cuenta que sea menos sospechosa que una creada para ello
- También se ofrece **acceso a servicios de suscripción** a precios más baratos
 - Pero a riesgo de que el robo sea descubierto y se cancele sin previo aviso
 - Se suelen adquirir para ver contenido gratis en regiones diferentes a las del comprador
 - Si bien esto normalmente se puede hacer legalmente vía VPN (Ej.: ProtonVPN, [Nivel A2](#))



Venta de una cuenta premium al servicio de streaming Disney+

CUENTAS DE REDES SOCIALES Y CORREOS ROBADAS

- A nivel de redes sociales se venden tanto cuentas como seguidores
- El precio es muy bajo (especialmente el de seguidores)
- Este servicio permite hacer creer que cuentas son más importantes de lo que lo son realmente
 - Es compra de cuentas bot
- Por ello todo lo que veamos en redes sociales hay que asumir que es falso

<i>Hacked Gmail account</i>	\$60
<i>Hacked Facebook account</i>	\$25
<i>Hacked Instagram account</i>	\$25
<i>Hacked Twitter account</i>	\$20
<i>Twitter retweets x 1000</i>	\$10
<i>LinkedIn company page followers x 1000</i>	\$5
<i>Instagram followers x 1000</i>	\$2
<i>Pinterest followers x 1000</i>	\$2
<i>Twitch followers x 1000</i>	\$2
<i>Instagram likes x 1000</i>	\$2
<i>Spotify followers x 1000</i>	\$1
<i>Soundcloud plays x 1000</i>	\$1

Fuente: Investigación de precios en la dark web de Privacy Affairs (<https://www.privacyaffairs.com/dark-web-price-index-2023/>)

CUENTAS DE SERVICIOS ROBADAS

- Prácticamente se venden cuentas de cualquier clase de servicio
 - Streaming, casinos, deportes...
- Los precios no suelen ser muy altos
- Mientras el dueño original siga pagando, el ladrón puede disfrutar del servicio por un precio ridículo
 - No obstante, la prohibición de compartir cuentas de algunos servicios de streaming puede detectar estos robos

<i>AirBNB.com verified account</i>	\$300
<i>Bet365 account</i>	\$35
<i>Uber driver hacked account</i>	\$30
<i>US eBay account</i>	\$20
<i>Netflix account, 1-year subscription</i>	\$20
<i>Uber hacked account</i>	\$12
<i>Spotify hacked account</i>	\$10
<i>Hacked Alaskaair account</i>	\$10
<i>NBA League Pass</i>	\$8
<i>Kaspersky account</i>	\$7
<i>Various adult site accounts</i>	\$6
<i>Canva Pro yearly</i>	\$5
<i>Disney Plus hacked account</i>	\$3
<i>CNBC Pro</i>	\$3
<i>Hulu</i>	\$3
<i>HBO</i>	\$2
<i>Orange TV</i>	\$2
<i>Netflix 4K 1 year</i>	\$1

Fuente: Investigación de precios en la dark web de Privacy Affairs
(<https://www.privacyaffairs.com/dark-web-price-index-2023/>)

PRECIOS EN LA DARK WEB DE LO QUE MÁS DEBEMOS DEFENDER

● Documentos falsificados (escaneos)

- Una categoría de bienes y servicios ilícitos que se venden con éxito en estos mercados son los escaneos de documentos personales
- Los delincuentes pueden usar estos datos para **hacerse pasar por alguien real** en Internet
 - E incluso abrir cuentas a su nombre
 - Por ejemplo, sitios webs de citas, pornográficos, de criptomonedas, casinos...
 - Ya no solo es una pérdida económica, sino también **reputacional**

● Otra categoría popular es la de las plantillas de identificación y facturas de servicios públicos

- Los compradores pueden modificar estas plantillas con cualquier detalle que necesiten
- Con información real y algo de experiencia, se puede crear fácilmente una colección de documentos falsos de aspecto auténtico
- Se pueden usar en **cualquier clase de estafa** (especialmente spear phishing), suplantación o contratación de bienes (por ejemplo, alquileres)

DOCUMENTOS FALSIFICADOS

- Por todo ello, la fabricación de documentos falsos en formato digital también es un negocio floreciente
- Muchos servicios piden copia o escaneo del documento original
- Con estas copias es posible suplantar a personas en muchos casos
- Los hay de todos los países
 - Para usar a la hora de hacer gestiones, contratar servicios...

<i>Alberta CA driver's License (scan)</i>	\$140
<i>USA selfie with holding ID</i>	\$110
<i>Forged WalMart prescription Rx labels</i>	\$100
<i>Russian passport scan</i>	\$80
<i>New York driver's license</i>	\$60
<i>USA passport scans</i>	\$50
<i>NSW (Australia) driver's license</i>	\$40
<i>Custom drivers' license</i>	\$35
<i>Minnesota driver's license</i>	\$22
<i>UK passport template</i>	\$22
<i>Germany passport template</i>	\$22
<i>New Hampshire drivers license template</i>	\$20
<i>Utility bill templates</i>	\$15
<i>Belgian passport template</i>	\$10
<i>UK utility bill templates</i>	\$10
<i>US business cheque templates</i>	\$8

Fuente: Investigación de precios en la dark web de Privacy Affairs
(<https://www.privacyaffairs.com/dark-web-price-index-2023/>)

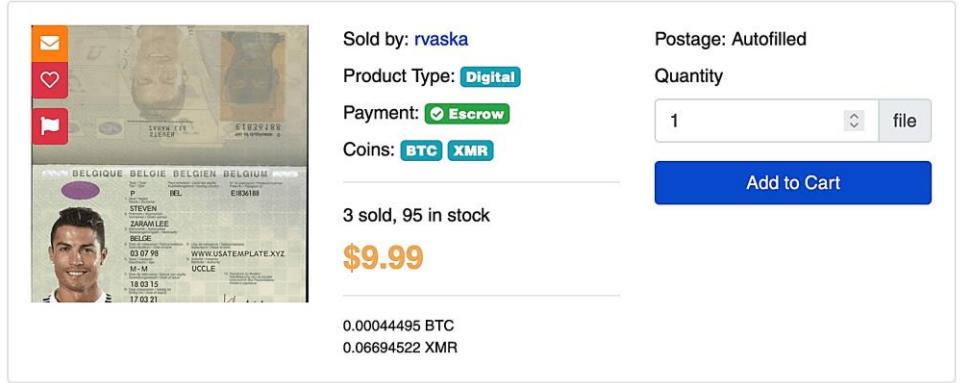
PRECIOS EN LA DARK WEB DE LO QUE MÁS DEBEMOS DEFENDER

● El dinero falso es un artículo muy común y fácil de encontrar

- Las monedas más demandadas son el euro, la libra esterlina y los dólares de Canadá, Australia y EEUU
- Algunos ofrecen la garantía de que pueden pasar una prueba de verificación por rayos UV
- Los billetes falsos de alta calidad suelen costar **un 30% ciento de su valor nominal**

● Los escaneos de documentos que incluyen un selfie con su propietario también están a la venta

- Son como las plantillas vistas, pero con ese dato adicional
- Lo suelen pedir en varios servicios para **verificación de identidad**



BELGIUM (BELGIAN) PASSPORT Template -HQ - INSTANT DELIVERY

Sold by: rvaska

Product Type: Digital

Payment: Escrow

Coins: BTC XMR

Postage: Autofilled

Quantity: 1

3 sold, 95 in stock

\$9.99

0.00044495 BTC
0.06694522 XMR

Add to Cart

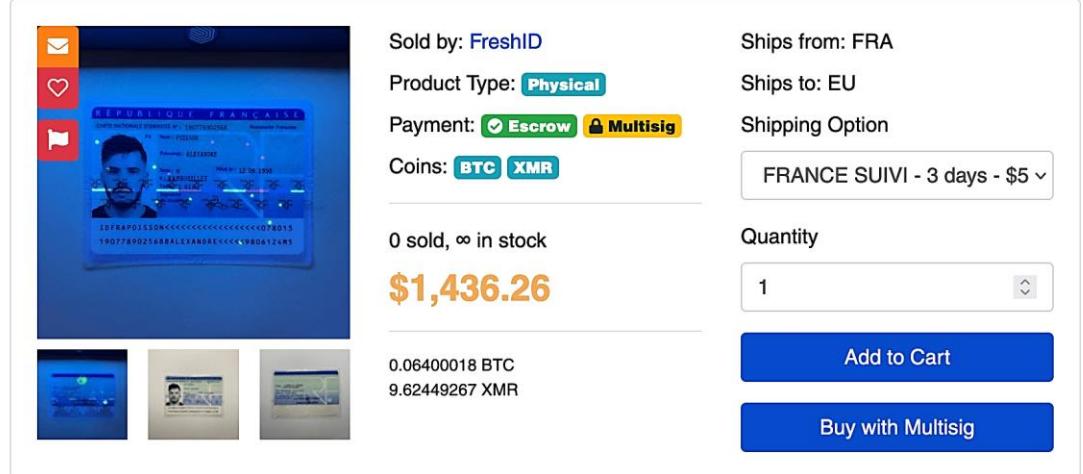
Plantilla para crearse un escaneo de un pasaporte belga. Con un poco de Photoshop, se puede crear uno que parezca auténtico a nombre de quien sea

PRECIOS EN LA DARK WEB DE LO QUE MÁS DEBEMOS DEFENDER

● Documentos falsificados (físicos)

- Los compradores también pueden obtener **documentos físicos falsos** en la dark web
- Debido a la dificultad de falsificarlos por todas las medidas de seguridad que tienen, **son los artículos más caros** normalmente
- Otra opción es que sean **robados**
- Pero entonces si el propietario ha denunciado el robo el comprador podría ser “cazado” fácilmente

Carte d identite francaise cni FULL SECU



Sold by: FreshID
 Product Type: Physical
 Payment: Escrow Multisig
 Coins: BTC XMR
 Ships from: FRA
 Ships to: EU
 Shipping Option: FRANCE SUIVI - 3 days - \$5
 0 sold, ∞ in stock
\$1,436.26
 0.06400018 BTC
 9.62449267 XMR
 Quantity: 1
 Add to Cart
 Buy with Multisig

Un DNI francés falsificado, supuestamente que pasa todas las medidas de seguridad (si te fías del delincuente)



José Manuel
Redondo López

DOCUMENTOS FÍSICOS FALSIFICADOS

- Obviamente, si existe un mercado para documentos digitales, también lo hay para físicos
 - Falsificados...o robados
- Con esto cualquier delincuente puede suplantar a quien desee en cualquier parte del mundo
 - ¿Entiendes por qué no debes enviarle tu DNI a nadie?
- Los precios son más elevados que las copias digitales
 - En función de lo que cueste hacer la falsificación (o el robo)

<i>Maltese Passport</i>	\$4,000
<i>French Passport</i>	\$3,000
<i>Netherlands Passport</i>	\$3,000
<i>Various European Union passports</i>	\$3,000
<i>Poland Passport</i>	\$2,500
<i>EU drivers' license</i>	\$2,000
<i>Lithuanian passport</i>	\$1,800
<i>European Union National ID (avg.)</i>	\$1,700
<i>Poland ID card</i>	\$1,700
<i>France drivers' license</i>	\$1,500
<i>Romania drivers' license</i>	\$1,450
<i>Latvian National ID</i>	\$1,300
<i>Fake US Green Card</i>	\$450
<i>Delaware ID</i>	\$200
<i>Indiana ID</i>	\$200
<i>Montana ID</i>	\$200
<i>Nevada ID</i>	\$200
<i>Texas ID</i>	\$200
<i>New Jersey drivers license</i>	\$200
<i>Louisiana ID</i>	\$200
<i>Utah ID</i>	\$200
<i>US driver's license (avg.)</i>	\$150

¿CREEES QUE LO HAS ENTENDIDO TODO? ¡AUTOEVALÚATE!

?

- *¿Entiendes ahora que muchas de las cosas que se puedan subir a internet tienen valor para alguien especialmente vinculado con el crimen?*
- *¿Eras consciente de que existe todo un mercado de cuentas identificación etcétera robado, que incluso fluctúa en función de la oferta y la demanda?*
- *¿Para qué crees que se usa este tipo de información?*
- *¿Qué ventaja para un delincuente crees que tiene hacerse pasar por ti con las cosas que te ha robado otra persona y que las ha puesto a la venta?*
- *¿Te das cuenta de que algunos de estos elementos casi se venden en packs por un precio realmente bajo?*
- *Debido a lo anterior ¿Cómo te crees entonces qué se hacen los review bombing o los ataques de bots en redes sociales?*



MÁS INFORMACIÓN...

Para saber más...



REFERENCIAS

- Como has visto, esta presentación forma parte de un proyecto de formación pensado para gente joven
 - Y/o sin conocimientos previos
- Si te gusta “el cacharreo”, tengo más cosas para ti
 - Si quieres saber más cosas “de hacker” sin instalar nada y requiriendo conocimientos técnicos mínimos, puedes echarle un ojo a **S-64 “Isaac Peral”**
 - Si quieres tener tus propios “mini-ordenadores” emulados para tus cosas, la **R-11 “Príncipe de Asturias”** te gustará
 - *¿Tienes un colega en problemas?* Creo que puedes ayudarle con la **P-74 “Atalaya”**
 - *¿Te flipa que haya gente así de mala por la red?* Te cuento como engañan a los demás en la **M-31 “Segura”**
 - *¿Te vienes arriba porque esto te mola?* Prueba alguna del **Rango 3 ;)**
- Quien sabe...a lo mejor esto te gusta y ¡en el futuro tú des charlas como esta! ☺



REFERENCIAS

● Otros enlaces interesantes

- **Redes sociales:** <https://www.incibe.es/node/53247>
- **Estar a la última en fraudes:**
<https://www.incibe.es/ciudadania/tags/Redes%20sociales>
- **Más consejos para ti:** <https://www.incibe.es/ciudadania/redes-sociales>
- **Y también para tus padres**
 - <https://www.incibe.es/menores/recursos/redes-sociales-en-la-adolescencia>
 - <https://www.incibe.es/menores/tematicas>



SOBREVIVIENDO EN LAS REDES SOCIALES

