

QUIERO FORMARME...PERO NO TENGO PERFIL TÉCNICO



Proyecto P-45 "Audaz"



Buenas a todos ciber-navegantes. En esta entrega quería daros no un consejo de seguridad como siempre, sino enseñaros **dónde podéis formaros** sobre el tema aunque no tengáis un perfil técnico. Esto es algo que puede ser muy útil de cara a vuestro día a día. ¡Y lo mejor de todo es que se trata de formación gratuita! **¿Es posible encontrar formación buena, gratuita y accesible a todos los públicos? ¡Sí!**

Muchos de estos recursos pertenecen al INCIBE. Es un instituto de carácter público que trabaja para afianzar la confianza digital y mejorar el nivel de seguridad de la ciudadanía. Depende de un ministerio, por lo que es un servicio público y por eso ofrece recursos gratuitos. No es magia, son tus impuestos 😊

¿Qué os voy a contar hoy?

Por tanto, hoy voy a afrontar la protección contra fraudes de una manera diferente. Porque sí que es verdad que saber lo que te puede pasar es una forma muy buena de prevenir que te pase, pero siempre hay alguien que me dice en alguna charla o en algún curso que doy: “*Oye Redondo, yo quiero aprender más, pero resulta que no tengo un perfil técnico, y no soy capaz de encontrar un material que me ayude y yo pueda entender sin frustrarme, porque normalmente ponen palabras y siglas que yo no entiendo*” en otras palabras: **Hay material, pero a veces es difícil encontrarlo adaptado a nuestro perfil de usuario.**

Mucho cuidado con hacer de menos a gente que no tenga perfil técnico. Cualquier persona puede ser un crack en lo suyo y no tener habilidades para la tecnología por falta de tiempo, interés, ganas o cualquier otra razón. Eso no es censurable ni criticable en absoluto. El problema es que hoy en día cualquier persona tiene muy sencillo navegar por Internet y, por tanto, tiene que ir por “la jungla” de la red forzosamente, por lo que hay que esforzarse en llegar a cualquier perfil para evitar problemas de seguridad, ya que todo el mundo necesita formación de ello, pero adaptada a su perfil de usuario.

Y la verdad es que esta gente **tiene razón**: gran cantidad de contenido que hay disponible en internet para prevenir estafas **supone que las personas tienen un determinado nivel técnico** y, en mi experiencia, eso es mucho suponer. Si un material empieza a usar siglas y nombres de cosas (IP, DNS, HTTP, certificados...) que el lector no entiende o no ha visto, y no se las explica, entonces, con razón, lo cerrará y pensará que esto es un mundo inaccesible para él o ella. **Y NO es así.**

La “experiencia senior” para gente “no técnica”

Pero fíjate que yo no soy el único que piensa esto, es más, **el estado ha pensado en eso**. Y por eso, el **Instituto Nacional de Ciberseguridad** (INCIBE) ha lanzado un programa de concienciación denominado '**Experiencia senior**'. Su objetivo es impulsar y potenciar las habilidades digitales de los usuarios mayores de 60 años con materiales que les permitirán adquirir las nociones básicas necesarias para desenvolverse con confianza y seguridad cuando naveguen por Internet. Es decir: **que pierdan el miedo**. Y lo tienes aquí: <https://www.incibe.es/ciudadania/experiencia-senior>



Guía de ciberseguridad. La ciberseguridad al alcance de todos



Ejercicios y actividades prácticas

Hombre, siendo sinceros, aunque el INCIBE diga que este material está pensado para personas de más de 60 años y ponga la palabra “sénior”, personalmente creo que el material es muy bueno y **le puede venir igualmente muy bien a personas de cualquier edad** que, por la razón que sea, no tengan ningún tipo de conocimiento técnico previo y necesiten adquirirlo. Es decir, aquí si que vale eso de que “la edad solo es un número”. Estos conocimientos son necesarios **para personas de cualquier edad** que necesiten una formación accesible.

💡 **También vale para chavales/as jóvenes que sí que pueden saber mucho más que esto, pero a lo mejor son los encargados de explicar determinadas cosas a personas de su casa que no tienen ese nivel y no saben cómo hacerlo. Bueno, pues si te ves en esa coyuntura aquí tienes una guía para enseñar a los tuyos 😊.**

¿Y sabes qué es **lo mejor**? Que vale tanto para **Windows**, como para **Android** como para **MacOS**, ¡Tiene ejemplos para cualquier sistema operativo! Fíjate en esta imagen para ver como es el material que tiene esta guía:

1.2. Cómo comprobar que tus dispositivos están protegidos (antivirus)

En Windows (Versión 10)

Nuestro sistema trae varias herramientas de protección ya preinstaladas.

- Haremos clic en el **ícono de Windows**, abajo a la izquierda, y seleccionaremos el ícono de la rueda dentada **'Configuración'**.
- A continuación, seleccionaremos el apartado de **'Actualización y seguridad'**.
- Nos aparecerá una nueva ventana donde seleccionaremos la opción **'Seguridad de Windows'** en el menú que aparece a la izquierda.
- Dentro de la opción **'Protección contra virus y amenazas'** veremos las diferentes protecciones que nos ofrece el antivirus que viene instalado por defecto, Windows Defender, y si están activadas o configuradas.

También podremos, por ejemplo, realizar un examen rápido del ordenador para confirmar que está limpio (libre de virus).

1.2. Cómo comprobar que tus dispositivos están protegidos (antivirus)

En Android

La herramienta **Google Play Protect** sirve para protegernos de las amenazas a las que nos exponemos. Para comprobar que está activada.

- Lo primero será acceder a la aplicación **'Play Store'** y pulsar sobre el ícono de menú de la esquina superior derecha: ícono con nuestra inicial.
- Luego, pulsaremos sobre la opción de **'Play Protect'**. Una vez dentro, veremos el estado en el que se encuentra nuestro dispositivo y las aplicaciones instaladas. Si todo está bien, deberíamos ver **'No se ha encontrado ningún problema'**.
- Además, veremos cuándo se realizó el último análisis y sobre qué aplicaciones.
- Si queremos, también podemos forzar un nuevo análisis pulsando sobre **'Analizar'**.
- Finalmente, debemos asegurarnos de que están activadas las opciones de **'Analizar aplicaciones con Play Protect'** y **'Mejorar la detección de aplicaciones dañinas'**, haciendo clic en el ícono de la rueda dentada de la esquina superior derecha.

Al activarlas, aparecerá en color verde, y esto significará que Google estará monitorizando las aplicaciones que instalamos en busca de posibles amenazas.

En MacOS

Los ordenadores de Apple también disponen de herramientas de protección preinstaladas.

- Iremos al **'menú de Apple > Preferencias del Sistema'** y haremos clic en **'Seguridad y privacidad > General'**.

En definitiva, este material es gratis y tan bueno que puede servir a **cualquier persona** que no tenga conocimientos técnicos para “ponerse las pilas” y perder el miedo a navegar por internet y usar en general el ordenador. Y además ataca al principal punto débil que ya os he dicho en semanas pasadas que existe a nivel social: **la formación y la concienciación en estos temas**.

💡 ¿Sabéis cuál es el único problema que yo creo que tiene? ¡Que mucha gente no sabe que existe! así que por eso estoy haciendo esta sección 😊.

¿Y que cubre más o menos esta guía? pues cosas muy necesarias y básicas:

- Cómo **actualizar** tus dispositivos
- Cómo comprobar que están protegidos por un **antivirus**
- Cómo impedir que cuando no estás en el ordenador otro vaya y a cotillear lo que estás haciendo, es decir, **cómo bloquearlo**
- Cómo **cifrar tu información** para que solo tú la puedas leer
- Cómo **descargar aplicaciones** sin riesgo
- Cómo **acceder a Internet** y navegar de forma segura
- Y también un apartado de **prevención contra fraudes**

Todo esto lo puedes ver en esta imagen del índice de este documento:

Índice

	Pag.
La ciberseguridad al alcance de todos	4
1. Tus dispositivos y su seguridad (Windows, Android, MacOS e iOS)	5
1.1. Cómo actualizar tus dispositivos <ul style="list-style-type: none">• En windows• En Android• En MacOS• En iOS	6
1.2. Cómo comprobar que tus dispositivos están protegidos (antivirus) <ul style="list-style-type: none">• En windows• En Android• En MacOS• En iOS	10
1.3. Cómo comprobar que dispone de un bloqueo de acceso. <ul style="list-style-type: none">• En windows• En Android• En MacOS• En iOS	14
1.4. Cómo comprobar que tus dispositivos están cifrados <ul style="list-style-type: none">• En windows• En Android• En MacOS• En iOS	19
1.5. Cómo descargar aplicaciones y programas sin riesgo	22
2. Protege tus cuentas y tu información (buenas prácticas)	24
2.1. Cómo crear contraseñas robustas.	25
2.2. Cómo funciona la verificación en dos pasos.	27
3. Acceder a Internet y navegar de forma segura	29
3.1. Cómo conectarnos a Internet de forma segura (conexiones wifi)	30
3.2. Cómo blindar nuestra conexión a Internet (router)	32
3.3. Cómo comprobar que nuestro navegador está actualizado <ul style="list-style-type: none">• En Google Chrome• En Mozilla Firefox• En Safari• En Microsoft Edge	35
3.4. Cómo eliminar cookies y el historial de navegación <ul style="list-style-type: none">• En Google Chrome• En Mozilla Firefox• En Safari• En Microsoft Edge	38

Índice

	Pag.
3.5. Cómo activar el modo incógnito <ul style="list-style-type: none">• En Google Chrome• En Mozilla Firefox• En Safari• En Microsoft Edge	41
3.6. Cómo instalar extensiones <ul style="list-style-type: none">• En Google Chrome• En Mozilla Firefox• En Safari• En Microsoft Edge	42
3.7. Cómo identificar webs fiables y no fiables	45
4. Descubre y evita los principales tipos de fraude	47
4.1. Cómo identificar ataques de ingeniería social (phishing, vishing, smishing)	48
4.2. Cómo evitar fraudes en compras online (Chollos falsos, Tiendas online falsas, Métodos de pago).	50
4.3. Cómo detectar noticias falsas o Fake News (Noticias falsas, Cadenas de mensajes).	53
4.4. Cómo identificar otros fraudes (Anuncios, Alquileres, Préstamos, Webs falsas)	55
5. Disfrutando de las redes sociales y las comunicaciones por Internet sin riesgos	57
5.1. Cómo configurar de forma segura nuestro perfil	58
5.2. Cómo detectar una cuenta falsa y cómo denunciar	60
5.3. Cómo configurar nuestro WhatsApp de forma segura	62
6. Checklist de seguridad	66
7. Recursos para ampliar	69
8. Denuncia	70

Y, como decíamos, todo eso para Windows, Android o iOS, así como para los 3 navegadores más usados del mercado. También te explica **cómo denunciar delitos** y tiene una guía complementaria de **actividades prácticas**, para que practiques un poco sobre lo que has aprendido y veas si lo has entendido bien.

También quiero deciros que el INCIBE, entre los servicios que da, **tiene una línea de ayuda temas de ciberseguridad a la que puedes llamar si te ocurre cualquier incidente**. Esto puedes hacerlo por teléfono (al 017) o por mensajería instantánea a la dirección que te indican en la siguiente imagen, o bien a través de un formulario web donde tú rellenas y cuentas tu caso, y ellos te responden donde tú le digas, lo cual os puede venir muy bien si os metéis en un lío o tenéis cualquier incidencia. Puedes encontrar más información aquí: <https://www.incibe.es/linea-de-ayuda-en-ciberseguridad/faq>

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



TU AYUDA EN CIBERSEGURIDAD



Teléfono
017



WhatsApp
900 116 117



Telegram
@INCIBE017



Formulario
web



Atención
presencial

La “experiencia junior” para los más jóvenes (y sus tutores legales)

El INCIBE ofrece servicios de ciberseguridad orientados a fomentar el uso seguro de las tecnologías por parte de niños/as y adolescentes. Esto lo hace a través de la iniciativa **Internet Segura for Kids** (IS4K), que es a su vez el Centro de Seguridad en Internet para menores de edad en España. Puedes acceder a todos los materiales aquí: <https://www.incibe.es/menores>.

Como ves en la siguiente imagen, hay cosas pensadas para varios perfiles: educadores, familias y los jóvenes en general, para así abordar los problemas desde distintos puntos de vista, que es la mejor manera de hacerlo.

Servicios para educadores, familias y jóvenes



Educadores

Material didáctico para trabajar la ciberseguridad y el uso seguro y responsable con el alumnado, la ciberconvivencia, acciones formativas y pautas de ciberseguridad para el trabajo docente.



Familias

Mediación parental, preguntas que surgen en las familias, herramientas de control parental, pactos y vales de tiempo para el día a día, Información sobre apps y redes sociales y acciones formativas.



Jóvenes

Niñas, niños y adolescentes pueden ayudar en la creación de una Internet más segura a través de la ciberseguridad y el uso responsable de la Red, con espacios de reflexión y panel de jóvenes.

Virus y otras amenazas

Otra de las *peticiones* más frecuentes que se hacen habitualmente es informarse sobre los virus (o, en general, malware) y otras **amenazas que circulan en la red**. El INCIBE también proporciona materiales para que aprendas a identificarlas y a hacerles frente. Puedes ver los recursos disponibles en esta dirección: <https://www.incibe.es/ciudadania/tematicas/virus-amenazas>.

Como puedes ver también en la imagen, te explica, entre otras cosas, qué perfil tienen los ciberdelincuentes y **qué buscan** con sus acciones, para que tengas más claro porqué ocurren los ciberfraudes (algo de lo que hablaremos en la siguiente sección).

Los ciberdelincuentes, ¿quiénes son?

Los ciberdelincuentes son personas que usan sus habilidades informáticas con fines maliciosos. Sus motivaciones son muy dispares, como la obtención de ganancias económicas a través del robo de datos, el espionaje laboral para obtener ventajas competitivas, el activismo político o social mediante ataques y la propagación de desinformación. En algunos casos, simplemente tienen como objetivo superar barreras de seguridad como un “reto personal” o demostrar en la red ante otros usuarios su superioridad en dicho campo.



La figura del ciberdelincuente (Vídeo)

Vídeo que explica cuáles son las principales características de un ciberdelincuente y cómo actúan.



¿Quiénes son los ciberdelincuentes y qué buscan? (Infografía)

Infografía que detalla claves interesantes sobre quién son las víctimas de los ciberdelincuentes y cuáles son sus motivaciones.

Estafas y *phishing*

El INCIBE también proporciona información para tratar de luchar contra lo que será el delito del futuro. En un informe publicado en 2023 por la empresa de ciberseguridad *Trend Micro* se afirma que el 91% de las empresas es **susceptible de sufrir un ataque de *phishing***. Por tanto, se deduce que la suplantación de identidad se encuentra a la orden del día en el mundo digital.

El *phishing* es un engaño, con el cual se consigue robar información sensible y/o credenciales a través de la falsificación de identidad. Es un ataque que, además, tiene múltiples formas y variantes, de las cuales te puedes informar en este enlace: <https://www.incibe.es/empresas/blog/principales-formas-de-estafa-traves-del-email-phishing-mas-comunes>. En el podrás ver ejemplos de phishing comunes que puedes usar de ejemplo para formarte.

Phishing más comunes. Presta atención para no ser “pescado”

A continuación, veremos una serie de modalidades de estos ataques de *phishing*, las cuales se encuentran muy presentes en la actualidad del cibercrimen:

Phishing fraude de la Agencia Estatal de Administración Tributaria (AEAT)

Durante el período de la declaración de la renta entre abril y junio, durante los meses previos y la temporada habilitada se puede apreciar un auge de esta modalidad de phishing. Se trata de una **campaña de correos maliciosos que tratan de suplantar a la Agencia Tributaria**, con el objetivo de obtener las credenciales de acceso del usuario a través de una página fraudulenta que suplanta a la legítima, o trata de infectar su dispositivo.

Existen **variaciones** en las cuales puede cambiar el cuerpo del correo o el asunto del mismo.

"Agencia Tributaria - Aviso n. [REDACTED]
De AgenciaTributaria <Ager[REDACTED]@[REDACTED].com
Fecha lun 22:45
Cuerpo del mensaje
ESTE EMAIL SE CORRESPONDE CON UN AVISO DE UNA NOTIFICACIÓN ELECTRÓNICA.
Le informamos que está disponible una nueva notificación. Titular con
los siguientes datos:

Titular: gestor[REDACTED].com
Organismo emisor: Agencia Estatal de Administración Tributaria, con
DIR3: [REDACTED]
Identificador: [REDACTED]
Concepto: Notificación administrativa
Vinculo: Titular

Puede acceder a esta notificación en la Dirección Electrónica Habilitada
Única (DEHU), disponible en: <https://agenciatributaria.gob.es/> (el
enlace real es:
[http://prcapedia.com/gvdlbbv/atonelement?em=gestor@\[REDACTED\].com](http://prcapedia.com/gvdlbbv/atonelement?em=gestor@[REDACTED].com))
Para que conste como leída, por favor acceda a
<https://notificaciones.agenciatributaria.gob.es> (el enlace real es:
[http://proexit.com/vunrpklj/prometheus?em=gestor@\[REDACTED\].com](http://proexit.com/vunrpklj/prometheus?em=gestor@[REDACTED].com))
De acuerdo con lo previsto en los artículos 41 y 43 de la Ley 39/2015,
de 1 de octubre, del Procedimiento Administrativo Común de las
Administraciones Públicas, la aceptación de la notificación, el rechazo
expreso de la notificación o bien la presunción de rechazo por no haber
accedido a la notificación durante el período de puesta a disposición,
dará por efectuado el trámite de notificación y se continuará el
procedimiento.
Puede recibir esta notificación por distintas vías electrónicas o
incluso en papel por vía postal. Si accediera al contenido de esta

Estrategias de protección contra fraudes y ataques vía email de la Universidad de Oviedo

Además de todo el material visto, **la Universidad de Oviedo ofrece un curso gratuito** (previo registro gratuito con cualquier email) con el nombre del título de la sección, disponible en este enlace: <https://uniovix.uniovi.es/course/view.php?id=62>. Es un curso con algo más de nivel técnico, pero pensado para ser asequible para cualquiera que esté familiarizado con el uso de un PC para labores de oficina. Ofrece tres apartados:

- Conocer distintas técnicas que puedan **proteger nuestras cuentas de correo electrónico** y de mensajería en general.
- Conocer las **técnicas de falsificación y fraudes modernas** para evitar caer en una estafa electrónica de los numerosos tipos que existen hoy en día.
- Conocer los detalles de una base amplia de **ejemplos de estafas reales** para lograr una concienciación contra la acción de los ciber delincuentes y de esta manera estar más protegido ante las estafas de hoy y las que puedan venir en un futuro.

TÉCNICAS DE SEGURIDAD Y PREVENCIÓN DEL FRAUDE EN MENSAJERÍA ELECTRÓNICA

Página Principal / Cursos / Técnicas De Seguridad Y Prevención Del Fraude En Mensajería Electrónica

Técnicas de Seguridad y Prevención del Fraude en Mensajería Electrónica



Compartir

Matricúlate

Inicio Matrícula: 18/10/2023

Inicio MOOC: 18/10/2023

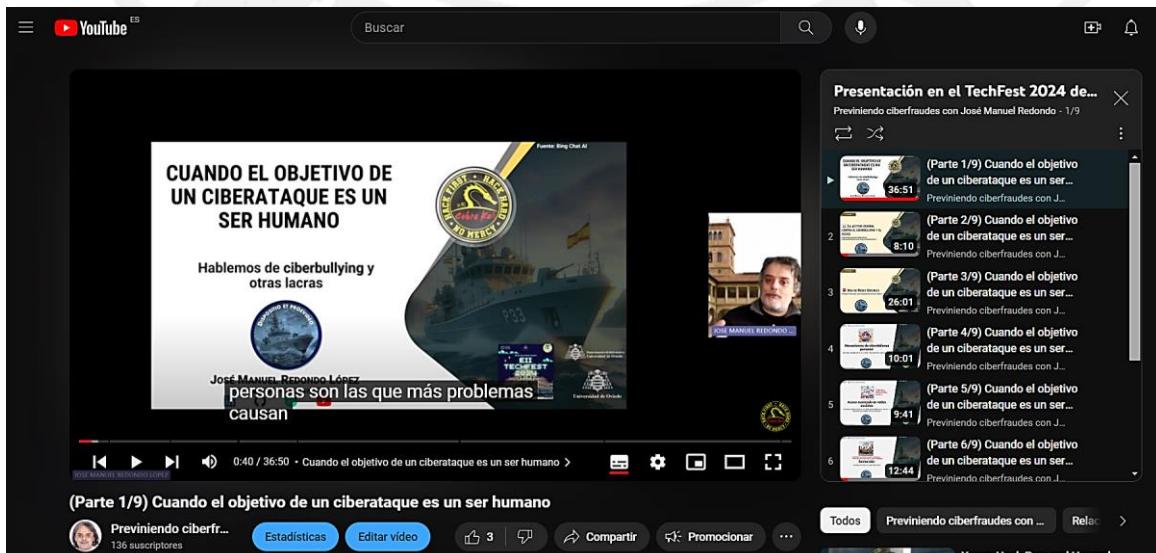
Fin del MOOC: 31/07/2024

Más sitios donde formarse

Nunca debemos descartar **YouTube como lugar de aprendizaje**, especialmente si somos más de que nos expliquen cosas de forma visual que de leerlas. Yo tengo un canal donde cada semana explico en menos de cinco minutos un fraude diferente (o algo relacionado con los mismos), fruto de mi trabajo en *Onda Cero*, al que podéis acceder aquí: <https://www.youtube.com/@j.m.redondo8618/featured>.

💡 Semanalmente también preparo un dossier formativo asociado a cada video (como lo que estás leyendo 😊), y lo enlazo en la descripción de cada video cuando está disponible. No obstante, puedes acceder a todos los dossiers clasificados desde aquí: <https://github.com/jose-r-lopez/Fraudes-y-Timos/wiki>. ¡YouTube puede ser una herramienta educativa muy buena también! 😊

Dentro de los materiales que ofrezco, es de especial relevancia el apartado contra el **acoso y el ciberbullying**, para estar prevenidos si uno de nuestros familiares o allegados lo sufriese. Puedes acceder al video de la charla (dividido en secciones para que sea más fácil verlo) aquí: https://www.youtube.com/watch?v=HGs4c32jyFg&list=PL8v8CMTNtRtiTEHtQNzUid5dLb_Gz8k_pR



The screenshot shows a YouTube video player. The main content is a presentation slide with the following text:
CUANDO EL OBJETIVO DE UN CIBERATAQUE ES UN SER HUMANO
Hablemos de ciberbullying y otras lacras
José Manuel Redondo López personas son las que más problemas causan

The sidebar displays a list of video thumbnails for a presentation titled "Presentación en el TechFest 2024 de...". The thumbnails are numbered 1 to 6 and have titles like "Cuando el objetivo de un ciberataque es un ser humano" and "Cuando el objetivo de un ciberataque es un ser humano".

Si te interesa la investigación de fraudes actuales desde un estilo más periodístico y con una realización técnica cuidada, puedes consultar el canal del streamer **Lord Draugr** aquí: <https://www.youtube.com/@LordDraugr>.

The screenshot shows the YouTube channel page for 'Lord Draugr'. The channel has 932K subscribers and 116 videos. The bio reads 'Historias con ánimo de lucro.' and includes a link 'foroclickbait.com/index.php'. A 'Suscripto' button is visible. Below the channel info, there's a navigation bar with 'Inicio', 'Vídeos', 'Shorts', 'Listas', 'Comunidad', and a search icon. The main section is titled 'Para ti' (For you) and features three video thumbnails:

- BlackRock.** TE HAN MENTIDO [15:47] En realidad, BlackRock no controla el mundo 382 K visualizaciones • hace 13 días
- EL GÁNGSTER MÁS QUERIDO** Historia de ASCENSO Y CAÍDA de AL CAPONE [24:53] 384 K visualizaciones • hace 4 semanas
- Cómo superar la DEPRESIÓN según los anuncios de INSTAGRAM [9:49] 633 K visualizaciones • hace 1 año

Otro streamer que trata los mismos temas, pero suele hacer reportajes de investigación largos y complejos, para tratar cada tema con profundidad y de manera muy completa es **Carles Tamayo**. Puedes ver su canal aquí: <https://www.youtube.com/@TamayoStuff>

The screenshot shows the YouTube channel page for 'TAMAYO'. The channel has 692K subscribers and 145 videos. The bio reads 'Reportajes de investigación.' and includes a link 'instagram.com/tamayostuff y 7 enlaces más'. A 'Suscripto' button is visible. Below the channel info, there's a navigation bar with 'Inicio', 'Vídeos', 'Shorts', 'En directo', 'Listas', 'Comunidad', and a search icon. The main section is titled 'Para ti' (For you) and features three video thumbnails:

- ¿VENDEHÚMOS?** [23:13] ¿VENDEHÚMOS?: el ANÁLISIS en profundidad que estás deseando. 489 K visualizaciones • hace 2 años
- PILLO al HACKER que me BANEÓ de INSTAGRAM y le LLAMO. [19:12] 484 K visualizaciones • hace 1 año
- SOBREDOSIS EN DIRECTO [33:46] La HOMEOPATÍA es una ESTAFA... demostrado. | DOCUMENTAL 1,3 M de visualizaciones • hace 2 años

🔍 Hay más canales de esta clase, pero estos son muy conocidos y buenos. Si te gustan las series de "True Crime", estos probablemente también 😊

Y por hoy eso es todo. De verdad que os recomiendo mucho que, si queréis aprender un poco más, busquéis esa guía gratuita, os la descargueís, y le deis una lectura con calma y practiquéis lo que pone. Y lo mismo con el resto de los recursos que os he dado sobre distintas temáticas relacionadas 😊. Y como siempre os digo: si no es para ti, seguro que conoces a alguien que la necesita, **así que ¡Que corra la voz!**. Dile que están ahí, que son gratis, y que le puede venir muy bien.

¡Y esto es todo! Muchas gracias y... ¡nos vemos en la próxima entrega!

Y recuerda amigo/a, si te interesa aprender y no te lo puedes permitir, ¡no estás solo! Tienes muchos recursos buenos y gratuitos de los que ir tirando para estar más seguro



¿Quieres escuchar como hablo de esta estafa en menos de 5 minutos?



- [Escúchalo en IVOOX](#)
- [Escúchalo en Amazon Podcast](#)
- [Escúchalo en YouTube](#)
- [¿Tienes otro cliente de Podcast? Este es el feed RSS](#)

¿Quieres saber enlaces relacionados?



- Enlace a la 'línea de ayuda en ciberseguridad' del INCIBE: Contactar por mensajería instantánea, teléfono o formulario para preguntar tus dudas de ciberseguridad: <https://www.incibe.es/linea-de-ayuda-en-ciberseguridad>
- Enlace a la información disponible en el programa de formación gratuita 'experiencia senior' del INCIBE: <https://www.osi.es/es/experiencia-senior>
- Acceso directo a la guía de aprendizaje: https://www.osi.es/sites/default/files/docs/senior/guia_ciberseguridad_para_todos.pdf
- Acceso directo a las actividades prácticas (¡pero léete antes la guía!): <https://www.osi.es/sites/default/files/docs/senior/osi-experiencia-senior-ejercicios-y-actividades-practicas.pdf>

Este documento usa material generado con IA²

¹ Audio emitido en "Más de Uno". 95.2 Onda Cero Oviedo (<https://www.ondacero.es/emisoras/asturias/oviedo/directo/>) el 28/12/2022

² Algunas imágenes del documento han sido generadas con la IA Bing Chat