

CIBERSEGURIDAD Y MENORES

CIBERSEGURIDAD Y MENORES

Efrén Varón

🔖 CFR - Centro de Formación e Recursos en Ourense



“ Formación de profesorado en activo de la Consellería de Educación, Universidad y Formación Profesional. Áreas: infantil y primaria, científico y tecnológica, artística y deportiva, lenguas extranjeras, lingüística y social, organización escolar y diversidad, formación profesional, tecnologías de la información, etc.



Avda. Universidade, 18 - A CUÑA - 32005 - Ourense (Ourense)

ver mapa

cómo llegar



De lunes a jueves de 9:00 a 14:00 y de 16:00 a 20:00. Viernes de 9:00 a 14:00.



988 241 533



www.edu.xunta.gal/portal/cfrourense



cfr.ourense@edu.xunta.gal

Enviar email

ÍNDICE DE CONTENIDOS

- ¿Qué dicen “algunas” leyes en España? Consideraciones previas.
- Noticias relevantes sobre la materia.
- ¿Qué importancia le dais a la Seguridad?
- Menores: Apuestas y Juego.
- Redes Sociales... ¿Qué datos compartes en RRSS? Perfiles... ¿Abiertos o cerrados?
- Principales delitos (Ejemplos)
- Preguntas, Dudas...

LAS LEYES EN ESPAÑA

- Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.

- MENOR de la edad DE 14 años inimputable

Según el Artículo 3 de la Ley 5/2000 reguladora de la responsabilidad penal del menor, cuando el autor de un supuesto delito sea menor de 14 años, no se le exigirá esa responsabilidad.

- **REGLAMENTO (UE) 2016/679** DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)
- **LOPDGDD - Ley Orgánica 3/2018**, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
 - Menor CON 14 años puede decidir que hacer con sus datos.

Tras la publicación de la Ley 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, en el artículo 7 se establece que el tratamiento de los datos personales de un menor de edad únicamente podrá fundarse en su consentimiento cuando sea mayor de catorce años.

LAS LEYES EN ESPAÑA

El Código Civil indica que los menores entre 14 y 18 años son libres para administrar el uso de su propio teléfono móvil; mientras que la Constitución Española reconoce que tienen derecho al respeto de su intimidad, propia imagen y secreto de las comunicaciones cuando lo utilizan. 19 mar 2019

El control paterno del teléfono móvil

El control parental se hace más complicado cuando los niños estrenan móvil a partir de los 8 años puesto que desde ese momento los menores acceden a las redes sociales.

El **Código Civil** indica que los menores entre 14 y 18 años son libres para administrar el uso de su propio teléfono móvil; mientras que la Constitución Española reconoce que tienen derecho al respeto de su intimidad, propia imagen y secreto de las comunicaciones cuando lo utilizan.



Asimismo, la Ley Orgánica 1/1996 de protección jurídica del menor indica que:

«Los menores tienen derecho al honor, a la intimidad personal y familiar y a la propia imagen. Este derecho comprende también la inviolabilidad del domicilio familiar y de la correspondencia, así como del secreto de las comunicaciones».

De contrario, **la patria potestad** que ejercen los padres, desde el nacimiento del hijo hasta los 18 años, **obliga a los padres a actuar siempre en interés de los menores**, por lo que es necesario encontrar el equilibrio entre ambas actuaciones.

¿Es correcto revisar los mensajes que nuestros hijos mandan y reciben a través de internet?

Muchos padres lo hacen y lo reconocen, otros, que también lo hacen, prefieren no confesarlo. Sin embargo, con la ley en la mano no se podría revisar los mensajes de los hijos, **SALVO** que haya sospechas de que nuestro hijo esté en peligro.

Si bien **los menores de edad** tienen derecho a que se respeten sus decisiones y a que nadie intervenga sus comunicaciones, la realidad es que **no son los únicos responsables de las consecuencias negativas que de ello puedan derivarse**. Y si sus tutores son responsables de velar por su seguridad, y quienes van a tener que hacer frente a una responsabilidad "objetiva" (art. 1902 CC) económica por los daños que causen (específicamente, si el resultado es la comisión de un delito), lo lógico es que se les reconozca capacidad suficiente para evitarlo.



El Tribunal Supremo avala que los padres revisen los dispositivos de sus hijos sin su consentimiento

No son pocos los casos en los que, en el marco de una pareja divorciada, un progenitor revisa los whatsapp que envía el menor al otro y la situación termina en los Tribunales por descubrimiento de secretos y vulneración de la intimidad de los pequeños.

Pues bien, incluso en este caso, son muchos los Juzgados y Tribunales que consideran que el desarrollo de las redes sociales como también lo es el Whatsapp *“requiere atención y vigilancia de los progenitores para preservar la indemnidad de los menores”* y, aun cuando, existe una separación de los progenitores, ambos mantienen la patria potestad de los hijos que les obliga a velar por su bienestar.

En definitiva, **el control de los teléfonos móviles de los menores por parte de sus padres es** una cuestión controvertida por la afectación de la intimidad que puede conllevar, aunque por el momento los jueces se inclinan por considerarlo **una facultad inherente al ejercicio de la patria potestad y a la obligación de velar por los hijos** y procurarles una formación integral, como establece el Código Civil.

EDAD RECOMENDADA PARA DAR EL PRIMER TELÉFONO MÓVIL A UN NIÑO

NIÑO



ESTO SON TELÉFONOS MÓVILES

Pueden ser usados por niños a partir de 7 u 8 años para comunicarse si se quedan solos, hacen algún recado, etc.



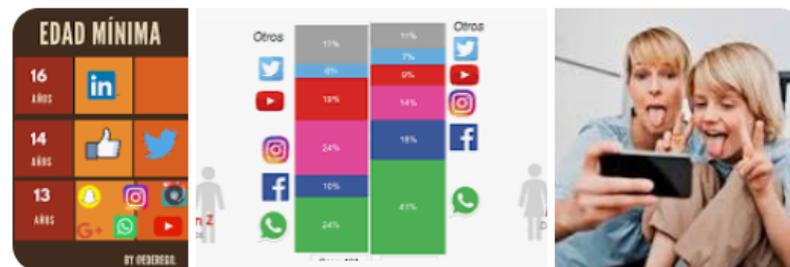
ESTO SON ORDENADORES DE BOLSILLO CON ACCESO A INTERNET

No son dispositivos recomendables en menores de 12-14 años ya que carecen de la madurez necesaria para hacer un uso racional y regular su conducta en redes

RGPD / LOPDGDD

Lo qué dice la Ley en España

Aunque el Reglamento Europeo establece que la edad mínima para tener una cuenta de Redes Sociales son los 16 años, está permitido que los Estados Miembro establezcan cualquier límite de edad a partir de los 13.



¿Cuál es la edad para que los menores puedan prestar consentimiento para tratar sus datos personales?



Tras la publicación de la Ley 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, en el artículo 7 se establece que el tratamiento de los datos personales de un menor de edad únicamente podrá fundarse en su consentimiento cuando sea mayor de catorce años.

Se exceptúan los supuestos en que la ley exija la asistencia de los titulares de la patria potestad o tutela para la celebración del acto o negocio jurídico en cuyo contexto se recaba el consentimiento para el tratamiento.

El tratamiento de los datos de los menores de catorce años, fundado en el consentimiento, solo será lícito si consta el del titular de la patria potestad o tutela.

cuando sea mayor de catorce años.

NOTICIAS DE INTERÉS

Tus dramas turcos favoritos, en un nuevo espacio.
Por 3€ al mes si eres abonado de mitele PLUS
Atrévete a vivirlo.
KANAL D DRAMA

Redacción Galicia • Ourense
31/10/2023 · 13:32h.



Los investigados ingresaron en las cuentas, tanto privadas como profesionales, del profesor EUROPA PRESS



- PUBLICIDAD
- Se trata de cuatro alumnos de un instituto de formación profesional de la localidad ourensana de Maceda
 - Todos ellos son alumnos del centro, excepto un quinto individuo, mayor de edad y amigo de uno de los menores
 - Accedieron a las cuentas de su profesor a través de ordenadores del

Cuatro alumnos de un instituto de formación profesional de Maceda (Ourense) están siendo investigados por, supuestamente y junto a otro individuo ajeno al centro, **entrar de manera ilegal en las cuentas bancarias y correo electrónico de uno de los docentes.**

Se cree que los sospechosos, entre los que hay cuatro menores de edad, **emplearon la red interna del centro para acceder de manera irregular a las cuentas**, tal y como ha informado la Guardia Civil y ha recogido *Europa Press*. Del mismo modo, usaron para lo anterior ordenadores del propio centro y equipos ajenos. Por todo esto, a los cinco investigados **se les imputa un delito contra la intimidad, derecho a la propia imagen e inviolabilidad del domicilio.**

Las diligencias instruidas fueron remitidas **al Juzgado de Instrucción de Guardia de Ourense (Ourense), así como a la Fiscalía de Menores de la Audiencia Provincial de Ourense (Ourense).**

¿Qué importancia le dais a la Seguridad?

ALJARAFE

Detenido un menor que hackeó el correo electrónico de su profesora

- El adolescente, de 17 años y alumno de un instituto de Gines, se hizo así con los exámenes
- [Accidente de tráfico en la A-49 a la altura de Almensilla](#)



La Guardia Civil de Mairena del Aljarafe ha detenido a un adolescente de 17 años por hackear la cuenta de correo electrónico de su profesora y apoderarse de documentos oficiales de ésta, como exámenes de evaluaciones continuas y recuperaciones. Según informó este sábado el instituto armado, la investigación se inició a principios de abril.

La denuncia que motivaba el inicio de las pesquisas la puso una profesora de un instituto de educación secundaria de Gines. La docente informaba que un dispositivo no autorizado había logrado entrar en su cuenta de correo corporativo, y había estado accediendo a una gran cantidad de archivos y documentos.

¿Qué importancia le dais a la Seguridad?

21 meses de prisión para los dos estudiantes de la UPV acusados de hackear a 40 profesores y cambiar sus notas



Los **dos estudiantes de Universitat Politècnica de València** que [en abril de 2018 fueron detenidos](#) por acceder de forma ilegal al sistema informático de la institución educativa para subirse las notas **han aceptado sendas penas de 21 meses y un día de prisión por estos hechos** y sendas multas de 1.620 euros.

Ambos universitarios **se enfrentaban a una condena de 3 años de prisión** y multas a partir de 3.000 euros por un delito continuado de falsedad en concurso con otro continuado también de revelación de secretos, [hechos que han reconocido](#).

¿Qué importancia le dais a la Seguridad?

EDUCACIÓN >

Investigados dos alumnos de un instituto gallego por 'hackear' los ordenadores de los profesores

Instalaron un 'software' para acceder a las contraseñas de los correos electrónicos de los docentes

ELISA LOIS

Pontevedra - 02 MAR 2019 - 18:18 CET



Dos alumnos del instituto Manuel García Barros de la localidad de A Estrada ([Pontevedra](#)) son investigados por un juzgado tras ser denunciados por haber instalado un *software* que daba acceso a las contraseñas de los correos electrónicos de los profesores y demás servicios tecleados en los ordenadores del centro.

La investigación arrancó en marzo de 2017 por la Policía Judicial cuando fueron detectadas anomalías en las terminales. El coordinador docente de Tecnologías de la Información y la Comunicación del instituto fue uno de los primeros en percatarse de que alguien extraño había accedido a su ordenador y había modificado un documento. Luego, otros profesores observaron extrañas coincidencias en exámenes de alumnos que cursan el último año de instituto donde se copiaban al dedillo las respuestas, incluso también los fallos.

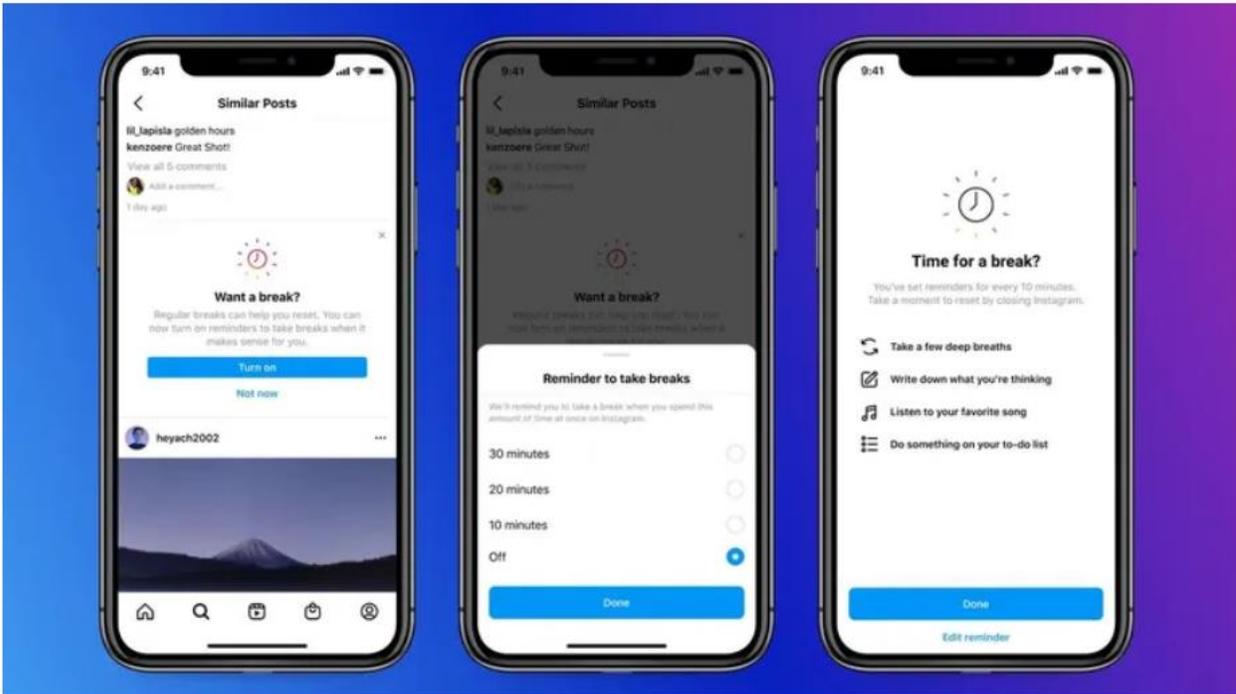
Así comenzó la dirección del instituto García Barros a descubrir el *hackeo* de las cuentas privadas del correo electrónico de los profesores y puso una denuncia ante la [Guardia Civil](#) que investigó a ocho alumnos supuestamente implicados en los hechos.



OURENSE

Investigadas dos jóvenes por acoso en Instagram

LA VOZ
OURENSE/ LA VOZ



Enviaban continuos mensajes dirigidos a una vecina de Esgos, de la que publicaron conversaciones privadas en redes sociales, según la denunciante

23 mar 2023 . Actualizado a las 05:00 h.



Comentar · 0

Dos jóvenes de 23 años de Ourense están investigadas como presuntas autoras de los delitos de **coacciones y revelación de secretos**, de los que fue víctima una vecina de **Esgos**. Esta denunció ante la **Guardia Civil** que dos perfiles de Instagram publicaban continuos mensajes hacia ella y conversaciones privadas en redes sociales. El equipo **@Ourense** descubrió a las sospechosas.

A ambas se les atribuyen supuestos delitos de coacciones (**stalking** u hostigamiento) y de revelación de secretos por particular. La investigación se inició a partir de la denuncia de la afectada en el cuartel de la Guardia Civil de Esgos. Las supuestas autoras, de iniciales A. A. C. y P.fL. F. son de Ourense y ambas tienen 23 años, tendrán que dar explicaciones en el juzgado, pues las diligencias de investigación se depositaron en la sede judicial de guardia en Ourense.

¿Cómo se puede gestionar la seguridad?

 Tododisca

Multa de 4.000 euros por añadir a un grupo de WhatsApp sin consentimiento

Hasta ahora pocas habían sido las denuncias en la aplicación de ... En tercer lugar, la AEPD ha multado al club con otros 1.00...

Hace 3 días



 Los Replicantes

WhatsApp: la multa a la que te enfrentas por añadir a alguien ...

La joven presentó su denuncia después de que su número de teléfono ... acceder al grupo de WhatsApp en el que se enco...

Hace 1 día



¿Cómo se puede gestionar la seguridad?

E Expansión

Multa de 4.000 euros por enviar un correo comercial a más de 400 personas sin autorización ni copia...

... mecánico a recibir una multa de 4.000 euros por parte de la Agencia Española de Protección de Datos (AEPD), tras tramitar...

Hace 1 mes



Cuidado con lo que hace tu hijo en redes sociales, los padres pueden ser multados con hasta 10.000 euros

Hablamos de una multa administrativa, más allá del posible delito que la Justicia pueda decidir que ocurre

11 comentarios



Sanción de hasta 10.000 euros, abonada por los padres. La Agencia Española de Protección de Datos (AEPD) es la encargada de monitorizar las denuncias que se realizan sobre determinados comentarios en internet. Fue en 2022 cuando se aplicó por primera vez en España una multa administrativa a un padre por los mensajes que había enviado su hijo.

"Fue a un joven de 16 años que extorsionaba a una chica de 13 años que le envió en un principio contenido íntimo voluntariamente, pero luego el infractor le amenazó y obligó a mandarle más bajo la amenaza de que las publicaría", [explica a 20Minutos](#) Mar España, directora de la AEPD. Por aquel caso fue multado con 5.000 euros, aunque las multas por estos casos pueden alcanzar hasta los 10.000 euros.

Los padres tienen responsabilidad subsidiaria. El [Código Civil recoge este concepto en su artículo 61](#): "Cuando el responsable de los hechos cometidos sea un menor de dieciocho años, responderán solidariamente con él de los daños y perjuicios causados sus padres, tutores, acogedores y guardadores legales o de hecho, por este orden. Cuando éstos no hubieren favorecido la conducta del menor con dolo o negligencia grave, su responsabilidad podrá ser moderada por el Juez según los casos".

Esto abre la puerta a multar a los padres del infractor que envía o graba algo sin consentimiento, pero también a los padres de los menores que ayudan a difundir esos mensajes delictivos.

"Es lo mismo que cuando les dejamos un coche. Les damos pautas (no bebas, ten cuidado que puedes matar a alguien), pues cuando damos un móvil a nuestros hijos hay que decirles que hay consecuencias", exponen desde la AEPD.

CONSEJO CONTRASEÑA SEGURA

1. Frases largas de 12 caracteres como mínimo.
2. Letras de canciones o poemas favoritos.
3. Una cita de un libro o una novela.
4. Palabras que tengan sentido para ti, pero no para alguien más.
5. Abreviaturas o juegos de palabras.

¿Cómo se puede gestionar la seguridad?

NIVEL	ALCANCE	CONTROL	
A	PRO/TEC	Gestión de contraseñas Defines un sistema de gestión de contraseñas avanzado que contempla todos los aspectos relativos a su ciclo de vida.	<input type="checkbox"/>
A	PRO/TEC	Técnicas de autenticación externas Consideras la utilización de sistemas de autenticación externos descentralizados.	<input type="checkbox"/>
A	TEC	Herramientas para garantizar la seguridad de las contraseñas Te ayudas de técnicas y herramientas informáticas para garantizar la seguridad de las contraseñas.	<input type="checkbox"/>
B	TEC	No utilizar las contraseñas por defecto Cambias las contraseñas que vienen incluidas por defecto para el acceso a aplicaciones y sistemas.	<input type="checkbox"/>
B	TEC	Doble factor para servicios críticos Incorporas sistemas de autenticación multifactor en los accesos a servicios con información muy sensible.	<input type="checkbox"/>
B	PER	No compartir las contraseñas con nadie Mantienes en secreto tus claves y evitas compartirlas.	<input type="checkbox"/>
B	PER	Las contraseñas deben de ser robustas Generas tus contraseñas teniendo en cuenta su fortaleza.	<input type="checkbox"/>
B	PER	No utilizar la misma contraseña para servicios diferentes Te aseguras de elegir distintas contraseñas para cada uno de los servicios que utilizas.	<input type="checkbox"/>
B	PER	Cambiar las contraseñas periódicamente Haces que se modifiquen las contraseñas cada	<input type="checkbox"/>

<https://www.security.org/how-secure-is-my-password/>

<https://haveibeenpwned.com/>

MÓVILES: Siempre BIOMETRÍA y factor Doble Autenticación.



¿Cómo se puede gestionar la seguridad?

Acceso al espacioProfesores PROXECTO ABALAR

En el caso de que prefiera acceder por medio del **usuario y contraseña del correo de la Consellería** debe seguir los siguientes pasos:

1 Seleccione la opción de usuario y contraseña

2 Introduzca su usuario y contraseña

3 Pulse el botón **Entrar**



En internet “está todo”... no solo una Guía para profesores ¡también para ciberdelincuentes!

<https://www.edu.xunta.gal> > proxecto-abalar > faq > co... ▾

¿Cómo puedo acceder al servicio espacio Profesores?

El acceso al servicio espacio Profesores se realiza a través del portal espacioAbalar en la siguiente dirección: <http://www.edu.xunta.es/espazoAbalar/>.

Otras personas también buscan

edu xunta edu xunta correo
edu xunta contausuario edu xunta xade
abalar xunta edu xunta datos persoais

¿Cómo se puede gestionar la seguridad?

ADAPTACIÓN DA PROGRAMACIÓN LINGUA CASTELÁ

Sáb, 05/16/2020 - 21:38 — COORD.TIC

5 adjuntos

MATERIAIS A TRABALLAR PROFESORAS

Lun, 03/16/2020 - 16:10 — COORD.TIC

MATERIAIS A TRABALLAR

PROFESORAS

@gmail.com

e@gmail.com

O alumnado de Latín de 4º de ESO e de 4º de ESO (A) de Lingua castelá e literatura, utilizan CLASSROOM, plataforma coa que a profesora está en contacto constante cos seus alumnos para enviar/recibir tarefas, plantexar dúbidas e adxuntar enlaces a páxinas web.

28 adjuntos

Profesora de Lengua Castellana

Imparte clases de Lengua e Literatura Castellana en secundaria, é responsable da Biblioteca, do Plan Lector e do Club de Lectura no que participan alumnos e profesores do CPI

(11)

En internet “está todo”... Incluso una Guías para profesores y ¡¡¡para ciberdelincuentes!!!.

MATERIAIS A TRABALLAR - @gmail.com

Lun, 03/16/2020 - 10:12 — COORD.TIC

MATERIAIS A TRABALLAR

PROFESOR

Subiranse os contidos paulatinamente para ir traballando estas semanas.

17 adjuntos

RESUMO PROGRAMACIÓN PLÁSTICA

Mar, 11/06/2018 - 10:40 — COORD.TIC

blogue de COORD.TIC | 1 adjunto



ARTISTA

1969 en A Coruña, España

Seguir



Busca y encuentra información sobre cualquier persona en España

Nombre/s 1º Apellido 2º Apellido DNI (opcional)

Tu E-mail

Tu e-mail se mantiene privado. Lo pedimos para comunicarnos en relación a tu solicitud.



¿Qué incluye el Informe de una Persona?

Incluye la búsqueda de:

- ✓ Datos de contacto e identificación personal
- ✓ Domicilios y Teléfonos vinculados
- ✓ NIF, DNI o NIE
- ✓ Profesión u Ocupación
- ✓ Vinculaciones Comerciales y Financieras
- ✓ Cargos y Dirigentes de Empresas
- ✓ Búsqueda avanzada en todos los Boletines Oficiales
- ✓ Boletín Oficial del Registro Mercantil – BORME –
- ✓ Consulta al Registro Público Concursal
- ✓ Sanciones de Tráfico del tablón edictal
- ✓ Medios de Prensa
- ✓ Participación en Redes Sociales
- ✓ Registros de Defunciones
- ✓ Obituarios

¿Para qué te sirve?

El informe te sirve para:

- ✓ Saber con quién estás por realizar una transacción
- ✓ Conocer sus antecedentes comerciales
- ✓ Prevenirte de fraudes
- ✓ Actualizar datos de un cliente, proveedor, deudor o moroso
- ✓ Contactar a una persona por cualquier razón legítima (notificaciones, emplazamientos, etc.)

¿Cuándo te llega y cuánto cuesta?

- ✓ El costo es de sólo 9 €
- ✓ Recibirás el informe en menos de 24 horas.

```
yellow open please_secure_your_servers16 NAY3qnoXTVCUYN6y2tFXow 1 1 0 0 283b 283b
yellow open please_secure_your_servers17 e58bF5vtRAOSOU64-2G2Lw 1 1 0 0 283b 283b
yellow open please_secure_your_servers18 EqYJV8-7TtSNnY88B0zH0A 1 1 0 0 283b 283b
yellow open please_secure_your_servers19 B5grVQGARP-9efrYxc-mnw 1 1 0 0 283b 283b
yellow open please_secure_your_servers12 b-AZIkSZTfeKTCe-XXlX4A 1 1 0 0 283b 283b
yellow open please_secure_your_servers13 pB7d5fYPTSyKxJxJuullw 1 1 0 0 283b 283b
yellow open please_secure_your_servers14 d1EN9h6GRTePuaFfdQFS-g 1 1 0 0 283b 283b
yellow open please_secure_your_servers15 FRz1L-7ORNaGEnMJ6xakIA 1 1 0 0 283b 283b
yellow open please_secure_your_servers20 QWFrFbL3QPSNuCImtsma5g 1 1 0 0 283b 283b
yellow open please_secure_your_servers10 hyGgVQamQ1-ila6HoB6WeQ 1 1 0 0 283b 283b
yellow open please_secure_your_servers11 t_822Ny2S7mOWxXHj1wx1Q 1 1 0 0 283b 283b
yellow open please_secure_your_servers8 C7CKvtgTSNmdUmL6uPVMeA 1 1 0 0 283b 283b
yellow open please_secure_your_servers7 XPx1IaDCQmapbR7J4oPyTg 1 1 0 0 283b 283b
yellow open please_secure_your_servers9 GBL18pJ4SxaUXEtpryAE4Q 1 1 0 0 283b 283b
yellow open please_secure_your_servers4 fayeNoCkSs6ihGV4_-wkw 1 1 0 0 283b 283b
yellow open please_secure_your_servers3 7Gb8kNcoTjO_AIdg8itUeg 1 1 0 0 283b 283b
yellow open please_secure_your_servers6 GYYeD-H7QZCePWBFTQGFbg 1 1 0 0 283b 283b
yellow open please_secure_your_servers5 LBT-7MJLRhayVkjWdNuU-Q 1 1 0 0 283b 283b
yellow open please_secure_your_servers2 -w6i4XbaRBexLOnmBSAnsA 1 1 0 0 283b 283b
yellow open please_secure_your_servers1 f-h_QJLFRkaK87KKV7qKVw 1 1 0 0 283b 283b
```

ct Comparitech

Report: 267 Million Phone Numbers & Facebook User IDs Exposed Online

<https://www.security.org/how-secure-is-my-password/>

<https://password.kaspersky.com/es/>

¿Y ESTO QUE ES?



El Español

Roban 35 millones de dólares usando un algoritmo que clona la voz del director de la empresa

Para coordinar la operación, se contrató a un abogado llamado Martin Zelner para que, junto al gerente, pudieran compr...

Hace 1 día



¿Cómo hacer un DEEPFAKE de forma fácil? Tutorial ESPAÑOL (DeepFaceLab)

Ver

https://as.com/meristation/2020/07/29/betech/1596055393_517524.html

DEEPFAKES

¿Quién tiene la Base de Datos biométrica más grande del mundo?

SEGURIDAD Y PRIVACIDAD

EXTREMADURA >

El caso de los desnudos con IA de Almendralejo se dispara: 26 menores implicados y 21 chicas afectadas

La Fiscalía podrá investigar penalmente a 21 adolescentes, ya que son mayores de 14 años. Los otros cinco son inimputables



La app que usaron lo chicos de Badajoz para desnudar a las niñas cuesta 9 euros y se envía por redes sociales

Ver >

Fecha de subida: 19 sept 2023

La aplicación que usaron los menores de Badajoz para desnudar a las niñas con inteligencia artificial

¡QUE BIEN! HAGO ALGO MAL Y NO PASA NADA...

La ley de responsabilidad penal del menor establece que los menores de 14 son inimputables. Se entiende que las infracciones que suelen cometer los niños menores de 14 años son generalmente irrelevantes y se establece que en los casos en los que generan alarma social, la familia y la asistencia civil son suficientes. 14 abr 2023

En España los menores de 14 años, no tienen responsabilidad penal. Sin embargo, sus padres o tutores deberán hacer frente a una sanción monetaria patrimonial.

EL JUEGO POR MENORES

¿Cómo se puede gestionar la seguridad?

Un menor ourensano apuesta la tarjeta de su padre en un juego online

La Guardia Civil lleva a cabo un plan director para concienciar a los escolares sobre el uso de internet

Durante una de las charlas en institutos del **Plan Director**, una iniciativa pensada para concienciar del peligro que puede causar un uso inadecuado de las redes sociales, **la Guardia Civil detectó un hecho delictivo**. Uno de los asistentes a la ponencia explicó a los agentes del grupo Arroba -un equipo de cibercriminales del **Instituto Armado**- que, cuando jugaba una partida online de "Fortnite", un jugador apostó la numeración y el pin de la tarjeta de su padre. Tras perder, se realizaron en ella gastos por valor de **2.000 euros**.

Por el momento, ya llevaron a cabo 200 charlas y se espera que este año superen las 300. Con esta actividad, además de hallar este tipo de hechos delictivos, se previene de que los menores se conviertan en víctimas de abusos o acoso.



OURENSE

APUESTAS

La adicción a apuestas online se dispara entre los jóvenes ourensanos



La proliferación de las máquinas en los bares de la ciudad y la provincia es un hecho constatable. Las casas de apuestas no ofrecen precisamente un apetitoso acuerdo económico a los bares. "Nos dan un 1% de la recaudación total, no llega ni para pagar el internet y la luz que consume", aseguran en un bar de la ciudad. Reconocen, eso sí, que "hay mucha demanda" y que tener la máquina "atrae a que vengan clientes a consumir, sobre todo los días de fútbol".

Casi uno de cada 10 menores de la provincia juega dinero en la red y el 15% de atendidos en Vigo son ourensanos

El auge de las casas de apuestas online y la proliferación de máquinas de estas empresas en los establecimientos hosteleros de la provincia sin ningún tipo de control amenaza la convivencia en las familias. La publicidad sin control de las apuestas deportivas, así como la facilidad de acceso a las distintas plataformas que se ofrecen en internet preocupa a la sociedad, que ha exigido en las últimas semanas la remodelación de la Lei do Xogo de Galicia.

Sportium, Bwin, Luckia, Codere....son algunas de las casas de apuestas online que también tienen presencia en distintos puntos de la provincia en tiendas físicas. Y el bum parece imparable si no se somete a un rígido control.

"Afecta a más adolescentes de los que pensamos", asegura Antonio Rial Boubeta, profesor de la Universidad de Santiago de Compostela experto en adicciones. De hecho, el análisis de la unidad de psicología del consumidor de la USC apunta a que el 8,4% de los menores de edad reconocer haber apostado online a juegos de azar o eventos deportivos. Una cifra claramente en aumento, ya que en 2010 apenas suponía el 1,5% del total de los menores consultados.

Perfil del menor adicto a las apuestas deportivas en España

Aunque en España las apuestas online de menores están prohibidas, el estudio '**Perfil de los adolescentes jugadores de azar a través de internet**', realizado por los profesores de la Universitat Oberta de Catalunya (UOC) Irene Montiel y José Ramón Ubieta, refleja que casi un 20% de los adolescentes han apostado en línea antes de la mayoría de edad y una parte importante lo hace habitualmente con el riesgo de adquirir una adicción.

Cuanto antes empieza el adolescente a jugar, mayor es el riesgo de que desarrolle un trastorno. A nivel estatal, las cifras de menores con algún problema de juego u otras adicciones (como a internet o a los videojuegos) es de entre el 5% y el 10%.

El perfil más habitual del **menor ludópata** es el de un adolescente que pasa de media en Internet entre 2,2 y 3,5 horas al día, muy impulsivo, entre los 15 y los 17 años, con una necesidad de búsqueda de sensaciones, y con dificultades para gestionar emociones.

Además, existen otros **factores que contribuyen a la adicción**:

- La presión de grupo
- La baja o nula supervisión parental
- El escaso control de uso del móvil por parte de padres y madres
- Falta de filtros en internet para este tipo de contenido

¿Cuándo alarmarse?

Una vez que detectas que un menor ha realizado apuestas online, existen varios indicadores que pueden ayudarte a diferenciar si un adolescente ha hecho una apuesta ocasional o es adicto al juego online:

- Está irritado si no juega.
- Pide dinero a otras personas.
- Apuesta cuando se siente ansioso o deprimido.
- Cuando pierde dinero, vuelve para "recuperar".
- Apuesta cada vez más dinero.
- Miente negando que juegue con frecuencia.
- Arriesga aspectos importante de su vida como amistades, estudios... por el juego.
- Intenta dejarlo pero es incapaz.

LUDOPATÍA EN ADOLESCENTES

https://www.alimente.elconfidencial.com/bienestar/2022-01-29/ludopatia-en-adolescentes-lejos-de-la-diversion_3364456/

ADICCIONES DEL SIGLO XXI

Ludopatía en adolescentes, más allá de la diversión

El 82,2% de los estudiantes españoles declara haber jugado a videojuegos en el último año, una cifra que alarma y alerta de lo que está por venir



¿Cuándo se convierte en algo patológico?

Según este análisis del Ministerio de Sanidad, **de los encuestados de entre 14 a 18 años, el 6,1% presentaría un potencial trastorno por uso de videojuegos** según la escala basada en criterios **DSM-V** (el manual clínico de los trastornos mentales). Este porcentaje se duplica (12,1%) cuando la población de referencia es la de estudiantes que han jugado a videojuegos en los últimos 12 meses.

Por sexo, se aprecian grandes diferencias. Este porcentaje supera el 10% entre los chicos mientras que entre las chicas el dato es inferior al 2%. Por edad, **las mayores prevalencias de posible trastorno se registran entre los alumnos de 14 y 15 años**. El 26,1% de los estudiantes de 14 a 18 años con un posible trastorno por videojuegos dedica, de media, más de 5 horas en un día.

Los datos hablan por sí solos

En España, **el 82,2% de los estudiantes declara haber jugado a videojuegos en el último año**. En cuanto a la actividad con los eSports (deportes electrónicos) en los últimos 12 meses, el 47,9% de los alumnos ha jugado y el 34,7% ha sido espectador mientras otros eran participantes, según los últimos datos del **'Informe'** sobre adicciones comportamentales 2020', elaborado por el Ministerio de Sanidad.

"El 26,1% de los estudiantes de 14 a 18 años con un trastorno por videojuegos dedica -de media- más de 5 horas en un día", según un informe

Más datos del informe de Sanidad:

- Las actividades son mucho **más frecuentes entre los chicos que entre las chicas**. En el caso de los videojuegos, el 96% de los chicos ha jugado en el último año, porcentaje que desciende al 69% en el caso de las chicas.
- Se registran las **mayores prevalencias entre los estudiantes de 14 años**, reduciéndose las mismas según avanza la edad de los alumnos.
- **Cerca del 50% ha jugado al menos semanalmente** y un 14,2% lo ha hecho como máximo 3 días al año.
- La mayoría ha jugado en los últimos 12 meses y dedican menos de 2 horas al día a realizar dicha actividad, **siendo un 5,6% de entre todos los estudiantes aquellos que han jugado más de 5 horas al día**. Los chicos son los que dedican más horas a jugar, aunque por **edad** no hay diferencias reseñables.

LUDOPATÍA EN ADOLESCENTES

https://www.alimente.elconfidencial.com/bienestar/2021-09-17/asi-es-la-adiccion-a-los-videojuegos_3290507/

EN AUGE

Hospitalizado por exceso de 'Fortnite': los síntomas de la adicción a los videojuegos

El psiquiatra que atendió al adolescente que estuvo ingresado en Castellón dos meses explicó que el paciente llegó a estar conectado a las pantallas 20 horas diarias



El peligro de las 'loot boxes' para la ludopatía de los menores: "Mi hijo gastó 1.000 euros para abrir unos cromos de un videojuego"

IGNACIO BLANCO | NOTICIA | 01.04.2024 - 10:27H



- Las cajas de recompensa generan una "adicción similar" a la que producen los salones de juegos.
- El Ministerio de Consumo persigue una "ley específica" que prohíba su acceso a los menores de edad.



Un aficionado a jugar videojuegos. / iStock



Clash Royale, uno de los diversos juegos que ofrece cofres de desbloqueo mediante pago. / RTVE

REDES SOCIALES

Investigado por delito de acoso un joven de A Valenzá (Ourense) que enviaba vídeos sexuales a dos mujeres por Instagram

20M EP/ NOTICIA / 20.11.2020 - 10:07H



La Guardia Civil de Ourense ha tomado declaración, en calidad de investigado, a un vecino de A Valenzá de 19 años como presunto autor de delito de acoso por enviar vídeos de contenido sexual a dos mujeres por la red social Instagram.

Según informa la Benemérita, el joven (J.R.R.) realizaba estos hechos desde cuatro perfiles diferentes y lo hacía desde el mes de julio. Las dos víctimas se corresponden con dos mujeres de 43 y 25 años, también vecinas de A Valenzá.

Las declaraciones tomadas, así como el resto de actuaciones realizadas, fueron remitidas al Juzgado de Instrucción número uno de Ourense.



BLOGS DE 20MINUTOS



EL BLOG DEL BECARIO

Es real el 'gato serpiente' cuya imagen se ha viralizado en las redes sociales

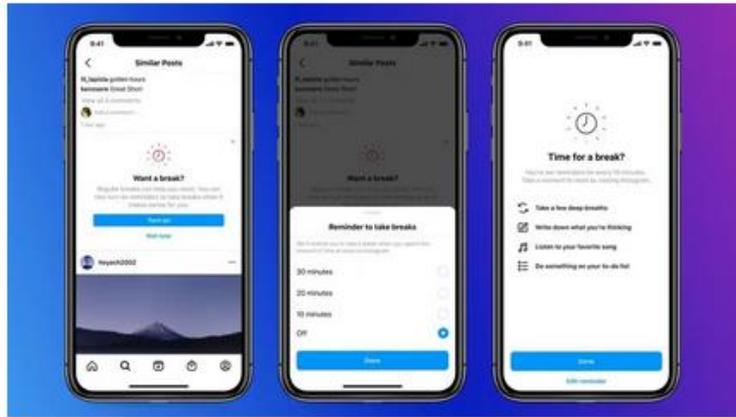


EL BLOG DE LILIH BLUE

La mirada masculina 3.0: el nuevo sexismo viene de una inteligencia artificial

OURENSE

Investigadas dos jóvenes por acoso en Instagram

LA VOZ
OURENSE | LA VOZ

Instagram

Enviaban continuos mensajes dirigidos a una vecina de Esgos, de la que publicaron conversaciones privadas en redes sociales, según la denunciante

23 mar 2023 · Actualizado a las 05:00 h.



Comentar ·

Dos jóvenes de 23 años de Ourense están investigadas como presuntas autoras de los delitos de **coacciones y revelación de secretos**, de los que fue víctima una vecina de Esgos. Esta denunció ante la **Guardia Civil** que dos perfiles de Instagram publicaban continuos mensajes hacia ella y conversaciones privadas en redes sociales. El equipo **@Ourense** descubrió a las sospechosas.

A ambas se les atribuyen supuestos delitos de coacciones (**stalking** u hostigamiento) y de revelación de secretos por particular. La investigación se inició a partir de la denuncia de la afectada en el cuartel de la Guardia Civil de Esgos. Las supuestas autoras, de iniciales A. A. C. y P.f.L. F. son de Ourense y ambas tienen 23 años, tendrán que dar explicaciones en el juzgado, pues las diligencias de investigación se depositaron en la sede judicial de guardia en Ourense.

Investigados dos vecinos de Ourense por coacciones a través de Instagram

La Guardia Civil de Ourense ha investigado a dos personas, naturales de Ourense, por un presunto delito de coacciones y otro de revelación de secretos a través de la red social Instagram.



La Guardia Civil de Ourense ha investigado a dos personas, naturales de Ourense, por un presunto delito de coacciones y otro de revelación de secretos a través de la red social Instagram.

Según informó el Instituto Armado, la investigación arrancó a raíz de una denuncia interpuesta por una persona, vecina de Esgos, en el cuartel de la Guardia Civil de esta localidad.

Esta persona denunció que en dos perfiles de Instagram estaban publicando "de forma reiterada y constante" mensajes relacionados con la víctima, así como publicaciones de conversaciones de índole privado en otras redes sociales.

Los investigados son A.A.C., de 23 años, vecina de Ourense, y P.F.L., de la misma edad, por sendos delitos de coacciones y de revelación de secretos.

Estas mismas fuentes han explicado que las diligencias han sido remitidas al Juzgado de instrucción de guardia de Ourense.

PUBLICIDAD

DISTORSIÓN, PRESIÓN Y FILTROS

Repunta la anorexia por culpa de Instagram: "Las redes sociales son veneno"

En los últimos años han aumentado los trastornos de conducta alimentaria (TCA) por la sobreexposición de los más jóvenes a través de las plataformas. Las principales causas son la presión social y la distorsión de la realidad

Vidas distorsionadas y presión social

Los motivos por los que las plataformas han aumentado **los TCA** son varios, aunque dos de ellos están especialmente relacionados: la presión social y la distorsión de la realidad en **un periodo de formación de la identidad**.

"En redes sociales, como Instagram, se tiende a pensar que se tiene que dar una imagen perfecta, tanto de nuestra cara como de nuestro cuerpo. De hecho, cuando llega el calor te metes en Instagram y todo lo que te aparece son 'influencers' en bikini que te hablan de **cómo tener un culo perfecto o el vientre más plano del mundo**. Algo que genera unas expectativas poco realistas", ejemplifica la psicóloga sobre los contenidos a los que están expuestos los más jóvenes. "Estas redes señalan que el cuerpo perfecto es el delgado y asocian este tipo de imagen al éxito, la belleza y la habilidad social", añade.



La mayoría de estas redes sociales cuenta con filtros que, sin necesidad de saber de Photoshop, te permiten **tener una cara y un cuerpo de modelo** (llegando incluso a existir un filtro llamado 'belleza').

"Ahora todas las chicas se dedican a hacerse fotos con filtros que les ponen los **labios más gordos, pecas, piel más morena, ojos más grandes, pestañas más largas...** De alguna manera por culpa de estos filtros se está transmitiendo que eso es lo bonito, lo que **te hace recibir 'likes'**, estar guapa y caerle bien a la gente". "Ya no solo se reduce a gustar, sino a caer bien y tener unas relaciones sociales adecuadas. Si relaciono tener la cara y el cuerpo como quedan con estos filtros con relacionarme bien y en la vida real no lo tengo, genera una insatisfacción tremenda con la imagen", manifiesta la experta.

¿Cómo se puede gestionar la seguridad?

CERBERUS

**DISPOSITIVOS SECURIZADOS
(BIOMETRÍA, NO PIN O PATRÓN)**

WHATSAPP WEB – TELEGRAM WEB ---OJO

(Instalación en otros dispositivos)

¿Cómo se puede gestionar la seguridad?

Con este nuevo truco pueden robar tu WhatsApp

Javier Jiménez | Publicado el 01 de junio, 2022 · 09:23



Usan el desvío de llamadas para robar WhatsApp

Se trata de un truco que han detectado unos investigadores de seguridad de **CloudSEK** y que consiste en utilizar el servicio automatizado de las operadoras móviles para el desvío de llamadas a un número de teléfono distinto y además usar la opción de WhatsApp para enviar un código de verificación de un solo uso a través de una llamada.

Básicamente se basa en **ingeniería social**. El atacante necesita conocer el número de teléfono de la víctima y convencerla de que haga una llamada a un número que comience a través de un código MMI (que comienzan con "*" o "#", que es lo que va a desviar las llamadas, según la operadora, a otro número si está ocupado o no lo cogen).

A partir de ahí, una vez ha engañado a la víctima para que **desvíe las llamadas**, el atacante va a iniciar el proceso de registro de WhatsApp en su dispositivo y va a elegir la opción de recibir un código de verificación de contraseña único (OTP) mediante llamada de voz. A partir de ese momento, el atacante va a poder registrar la cuenta de WhatsApp, habilitar 2FA y evitar así que el usuario legítimo pueda recuperar su cuenta.

Como ves, este truco puede **robar tu cuenta de WhatsApp**. Ahora bien, es un método complejo, que requiere de ingeniería social y por supuesto va a necesitar la interacción de la víctima. Los piratas informáticos van a encontrarse con múltiples obstáculos que van a hacer que esto sea difícil de llevar a cabo.

¿Cómo se puede gestionar la seguridad?

¿Es seguro guardar las contraseñas en el navegador?

El *'hijacker'*, o secuestro de navegador, es uno de los muchos tipos de *'malware'* que pueden comprometer nuestra seguridad cuando navegamos por internet.

Una de las funciones que nos ofrecen los navegadores es la de poder **guardar las contraseñas de acceso** para no tener que recordarlas ni teclearlas, y así entrar en un clic. Esto puede ser muy útil en algunos casos ya que nos permite trabajar más rápido pero no debemos olvidar que conlleva algunos riesgos que se deben tener en cuenta.

Esta práctica, más que facilitarnos la gestión de nuestra información, **supone un riesgo elevado en caso de que accedan a nuestro dispositivo**. Los navegadores web suelen almacenar las credenciales en un formato cifrado dentro de un almacén de credenciales; sin embargo los ciberdelincuentes pueden usar técnicas para hacerse con ellas.

¿Cómo acceden los ciberdelincuentes a las credenciales almacenadas en el navegador?

Algunas páginas, normalmente de juegos o contenido para adultos, solicitan la instalación de algún tipo de software adicional. Este software puede ser malicioso y tiene como objetivo hacerse con el control del navegador con la intención de espiar nuestra actividad, **robar nuestra información** o mostrar publicidad engañosa. Esta publicidad puede contener enlaces a otras páginas creadas por los ciberdelincuentes que suplantan a las originales, donde pueden aprovechar, a su vez, para solicitar y hacerse con nuestras credenciales.

Se debe sospechar de este ataque cuando se observe un cambio en el comportamiento de nuestro navegador, por ejemplo si cambia la página de inicio, si empezamos a tener muchas más publicidad de lo habitual o si se observan nuevas herramientas o iconos en el navegador que antes no estaban.



Ana Gómez Blanco

Casi todo lo que utilizamos en Internet tiene usuario y contraseña. Son necesarias para iniciar sesión en cualquiera de los servicios más usados, como redes sociales, lugares de compra 'online', o televisión en 'streaming'. Cuando ingresamos esas credenciales por primera vez en un dispositivo, inmediatamente el navegador nos ofrece guardar esas claves para no tener que escribirlas ni recordarlas en las próximas ocasiones. ¿Es usted de los que responde que sí? Entonces siga leyendo porque esta información le resultará útil.



¿Cómo se puede gestionar la seguridad?

Así bloqueas Windows en un segundo para que nadie más use tu PC

David Onieva | Actualizado el 10 de enero, 2022 • 10:38

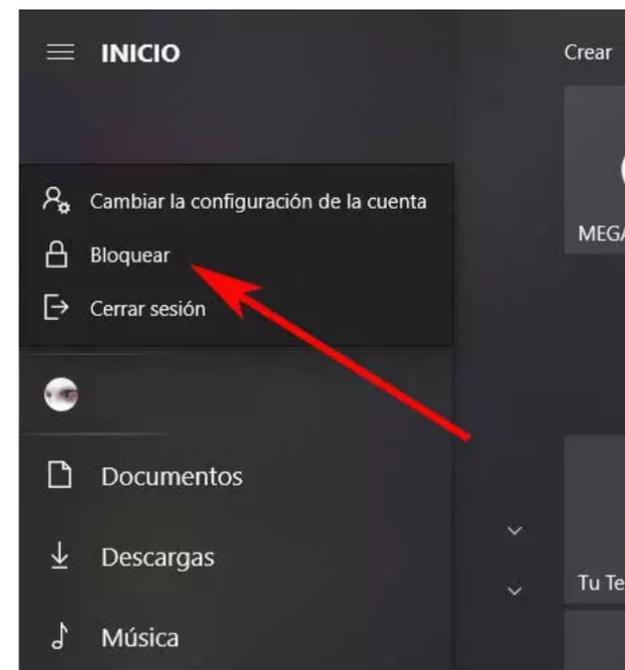


WIN + L

Bloquear el equipo desde el menú Inicio

Aunque no está en el mismo lugar de **versiones anteriores de Windows**, desde el menú Inicio podemos llevar a cabo esta tarea que os comentamos. Por tanto, para ello lo primero que hacemos es abrir el menú de Inicio, ya sea presionando la tecla del logo de Windows, o haciendo clic con el ratón en el botón de Inicio.

Tras ello, cuando aparezca este, en el panel izquierdo pinchamos sobre la imagen de la cuenta de usuario, donde aparecerá la opción de **Bloquear**, entre otras. Po tanto lo único que tenemos que hacer es situarnos sobre la misma y seleccionarla para así bloquear la sesión abierta.



¿Cómo se puede gestionar la seguridad?

- Sentido Común. Piensa y “no te agobies a las primeras de cambio”.
- Si no sabes... no hagas.
- Pregunta... el que pregunta es burro una vez y el que no pregunta, es burro toda la vida.
- No compartas datos personales... y menos si son de otro.
- Cuidado con las contraseñas del móvil (patrón, pin...) mejor biometría.
- Se cuidadoso con tus datos. Perfiles mejor cerrados.
-

LOS CIFRADOS – EL CORREO EMAIL

- Correo Electrónico XUNTA.GAL o GMAIL.COM, YAHOO.COM...
 - ¿Creéis que sois los únicos que veis vuestro correo?
 - ¿Qué guardamos en nuestro correo?
- LEGALMENTE:
 - En caso de baja por larga duración.
 - En caso de fallecimiento.
 - En caso de comisión de un ilícito penal.
- ILEGALMENTE:
 - Servidores dudosos.
 - Usuarios y contraseñas expuestos: “Have I Pwned”

LOS CIFRADOS

- Vale... me han hackeado el mail ¿Y que? No tengo nada que ocultar. ¿Qué me puede pasar?
 - CASO: Usurpación de Estado Civil.
 - NOMBRE: Abogada.
 - NEXO: Email

LOS CIFRADOS EN RRSS MENSAJERÍA

Parte 1: ¿Qué es el cifrado de extremo a extremo de WhatsApp?

Entonces, ¿qué es el cifrado de extremo a extremo en WhatsApp?



Las funciones de Signal

Las funciones disponibles a todos los usuarios de Signal incluyen el cifrado de extremo a extremo, el almacenamiento seguro de datos y la capacidad para ver el código de Signal.

El cifrado de extremo a extremo, un pilar de la privacidad

Una de las ventajas indiscutibles de Signal es su función **predeterminada de cifrado de extremo a extremo**. Esto significa que solo las partes que comparten mensajes entre ellos pueden leerlos, y que nadie (ni siquiera los desarrolladores de la aplicación) pueden escuchar las llamadas individuales o grupales. Con el **cifrado de extremo a extremo** se consigue mejorar la seguridad durante el intercambio de los mensajes.

En muchos sentidos, ha sido gracias a Signal que el cifrado de extremo a extremo ha conseguido hacerse tan popular entre las aplicaciones de mensajería. Incluso la competencia, WhatsApp, Facebook Messenger y Skype, **utilizan el protocolo de Signal para una comunicación segura**. Pero, en comparación, Signal cifra mucho más datos.

Telegram no es tan seguro como WhatsApp si no activas esta función

Sin esta configuración, Telegram podría acceder a tus conversaciones si así lo quisiera.

Por: **Leonardo Ancajima** 26 de enero del 2021 11:28 AM | Actualizado el 26 de enero del 2021 11:28 AM

Síguenos en Google News



EL NEGOCIO DE LA PRIVACIDAD

LOS CIFRADOS

- Mejor DOS VIDAS una privada y otra profesional.
- ¿Os imagináis mantener una conversación con vuestro urólogo en público?
- Si os llama el del banco, para deciros que debéis dos mensualidades del coche, o del piso... ¿Pondrías el altavoz del móvil?
- Si uno de vuestros familiares, critica a uno de vuestro amigos... Mejor en privado ¿no? Que no en un grupo de WhatsApp.
- Qué es mejor en seguridad ¿WhatsApp, Telegram, Signal...?



Datos que se vinculan a tu cuenta

WHATSAPP	TELEGRAM	SIGNAL
Número de teléfono	Número de teléfono	Número de teléfono
ID de usuario	ID de usuario	
Contactos	Contactos	
ID de dispositivo	Nombre de tu cuenta	
Datos de publicidad		
Historial de compras		
Ubicación aproximada		
Número de teléfono		
Correo electrónico		
Interacción del producto		
Informes de fallos		
Informes de rendimiento		
Información de pagos		
Atención al cliente		
Otro contenido de usuario		

NUESTROS DATOS ¿SOMOS IMPORTANTES?

- Facebook compra WhatsApp ¿Motivo?
 - Tú eres donde Tú estas.
- Las Redes Sociales y sus permisos.
 - Get Account – GPS Localitation (Waze, Tinder, Find My Mobile...)
 - Battery Cookies + Big Data + Machine Learning
- Datos:
 - Lo que pueden saber de ti.....

NUESTROS DATOS ¿SOMOS IMPORTANTES?

- Donde Vives
- Donde vas de vacaciones
- Donde Trabajas
- Donde Compras
- Si vas andando o en coche
- Donde Duermes
- Si vas al Gimnasio
- Donde comes o cenas
- Si vas al médico por enfermedad leve o crónica
- Qué tiendas visitas
- A quien visitas en la cárcel... con quién te juntas.
- Si vas al Cine o al Teatro... conciertos.
- Si vas a la Iglesia
- Si vas a manifestaciones con tintes políticos
- Si tienes amante (apagas el teléfono en determinada ubicación)
- Cual es tú círculo social (Nos juntamos con otros dispositivos, si utilizamos la misma APP (Big Data))

SÍ... REALMENTE SOMOS IMPORTANTES.

- Si una aplicación es gratis... el producto somos nosotros.

- Fintonic

¿Que ganan los de Fintonic?

Fintonic gana dinero cobrando a las compañías cuando el usuario elige contratar un producto.
Nunca cobramos al usuario.



¿Cómo obtiene beneficios Fintonic?

← [Bienvenido a Fintonic](#)

Fintonic es una aplicación gratuita. Nuestro modelo de negocio consiste en ayudar a los usuarios a que encuentren los productos que más les convienen entre más de 50 compañías líderes.

Nos comprometemos a ofrecer siempre lo mejor para el usuario, porque no tenemos conflicto de intereses. Fintonic gana dinero cobrando a las compañías cuando el usuario elige contratar un producto. Nunca cobramos al usuario.

Fintonic en ninguno de los casos comparte información de carácter personal con terceros, los datos personales son estrictamente confidenciales y están amparados por la Ley Orgánica de Protección de Datos (LOPD).

SÍ... REALMENTE SOMOS IMPORTANTES

- DOS CASOS: DOS PERSONAS MALAS.

TÍTULO: COMO “RETORCER” EL USO DE LA TECNOLOGÍA
PARA BENEFICIO PROPIO.

NEXO: EL NIÑO 6 AÑOS, COMO HERRAMIENTA DELICTIVA

- CASO1 – VARELA – PADRE “BUENO”, MADRE “MALA”
- CASO2 – CASA CHOCOLATE – PADRE “MALO”, MADRE “BUENA”

SÍ... REALMENTE SOMOS IMPORTANTES.



Descubrir cómo cambia tu salud con el tiempo

1. Abre la app Salud y toca la pestaña Resumen.
2. Desplázate hacia abajo hasta Lo destacado. En Lo destacado, se muestra tu salud a lo largo del tiempo para que puedas ver tu desempeño en general.
3. Toca un dato destacado para obtener más información sobre esa categoría o toca Mostrar todo lo destacado en la parte inferior de la lista.



Agregar más datos sobre tu salud

- [Haz un seguimiento de tu sueño](#) con Hora de dormir en la app Reloj.
- [Configura Ficha médica](#) en la app Salud para acceder a información médica importante.
- En un dispositivo con iOS 11.3, puedes ver tus expedientes clínicos de varias instituciones desde el iPhone. [Agrega tus expedientes clínicos y conoce las instituciones compatibles.](#)

EXCHANGE - NUESTROS DATOS

https://www.google.com/search?client=firefox-b-d&sca_esv=27178ea4ecd47877&sxsrf=ACQVn08qzqsKt9N_0wSkf6ayaGdqFwa-PA:1706650809887&q=persona+con+dni&tbm=isch&source=lnms&sa=X&ved=2ahUKEwivm53aiYaEAXuf8AIHHdywDa8Q0pQJegQIDBAB&biw=1440&bih=799&dpr=1.5





VENTA DNI EN TELEGRAM

Un pasaporte del Reino Unido, por ejemplo, cuesta 2.499 dólares; un visado de residencia para Australia, 999 dólares; un 'pack' de pasaporte, documento de identidad, permiso de conducir y tarjeta SIM de Nueva Zelanda, 2.599 dólares. Así lo publicita abiertamente el canal de Telegram, que cuenta con casi 3.800 suscriptores, algunos más que **ID passport original**, que tiene cerca de 1.200 seguidores. Este último se centra más en los documentos de identidad. En concreto, cuelga cientos de DNI de Francia, Suecia, España, Holanda, Alemania, República Checa, Bulgaria, Bélgica, Italia o Finlandia cada día.

<https://www.youtube.com/watch?v=-KIUq1TH9k>

<https://web.telegram.org/k/>

<https://web.telegram.org/k/#@PasaporteespanolyDNI>

SEGURIDAD - USB

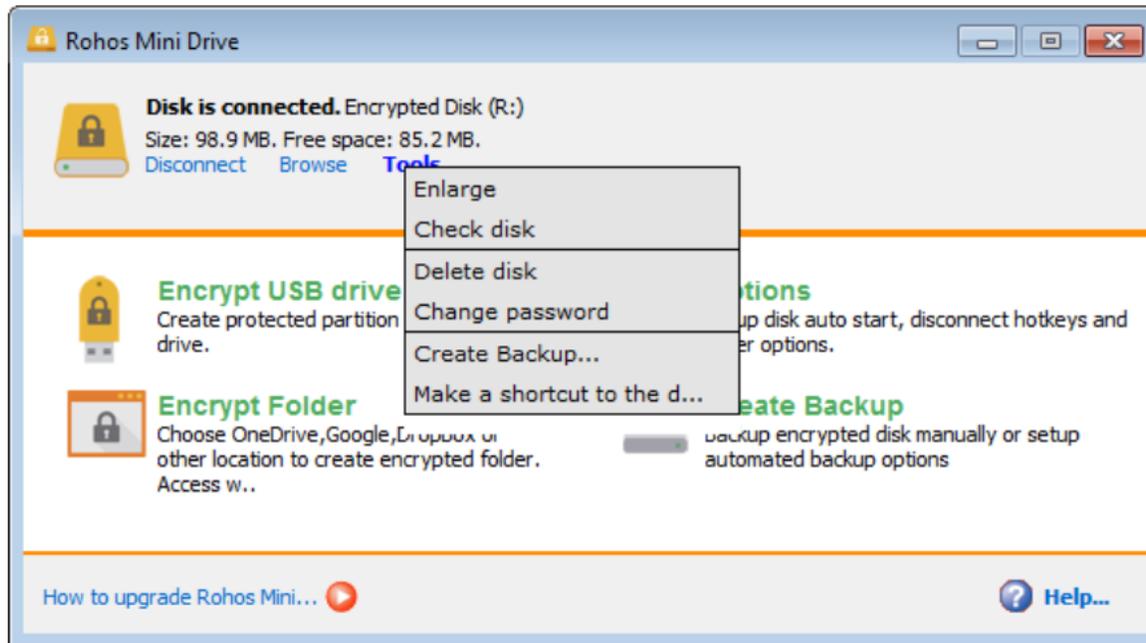
Riesgos de utilizar memorias USB con vistas a compartir información

Para empezar, uno de los datos más preocupantes habla de hasta **un 62 % de empresas que adolecen de la pérdida de datos confidenciales por el extravío de memorias de tipo USB**. ¿Cómo es posible? No hay que olvidar que una memoria USB es un dispositivo de gran capacidad y muy sencillo de guardar y transportar, pero su pequeño tamaño y ligero peso lo hacen más susceptible de perderse sin que nos demos cuenta. Tan sencillo e inadvertido como perder una moneda.

El 30 % de las infecciones por *malware* suceden a través de tarjetas SD y memorias USB infectadas. Y es que la principal medida de seguridad ante virus informáticos y *malware* es el correcto uso del ordenador y de los navegadores de red. Prácticamente no hay persona que, incluso en su ámbito laboral, no navegue por Internet sin la correcta protección, más aún cuando sus empresas son objetivos atacados de manera activa por determinados tipos de *malware*. Esto explica el elevado porcentaje de amenazas a través de los dispositivos portátiles, tan inofensivos que parecen cuando los miramos.

SEGURIDAD - USB

Rohos Mini Drive



Descarga

Rohos Mini Drive es una aplicación gratuita que permite crear particiones con cifrado, ocultarlas y protegerlas con contraseña en cualquier unidad USB flash. Con los datos cifrados puede trabajar en cualquier ordenador aún sin derechos administrativos. El programa crea una partición protegida con el estándar AES 256 bits accesible sólo con la clave secreta que elijas. Rohos Mini Drive muestra en el Explorador de Windows una unidad nueva donde podrás colocar todos tus archivos. Rohos Mini Drive permite analizar el disco en busca de errores, cambiar el tamaño de la partición cifrada o formatearlo, y tendrá espacio libre para colocar ficheros que no quiere cifrar.

SEGURIDAD - USB

Muchos somos los que, mientras vamos caminando por la calle, nos hemos encontrado algo por el camino, como una cartera, algunas llaves o un **dispositivo de memoria USB o pendrive**. Pues bien, estos últimos son uno de los cebos utilizados por los ciberdelincuentes para **engañar e infectar con *malware* los equipos de los usuarios**. A este tipo de ataque se conoce como ***baiting*** y es más común de lo que creemos. Veámoslo en el siguiente ejemplo:

La madre de la familia acababa de terminar su jornada laboral en la universidad donde trabajaba. Cuando se disponía a entrar en su coche, se percató de que, a los pies de este, junto a la puerta del conductor, había una memoria USB tirada en el suelo. Parecía estar en buen estado y decidió llevársela a su casa puesto que podría ser de algún alumno.

Por la tarde, decidió conectar el dispositivo a su equipo para comprobar su contenido y tratar de averiguar quién podría ser su dueño/a. Nada más conectarlo, el antivirus alertó a nuestra protagonista por medio de una notificación: **¡Alerta! El dispositivo que está tratando de conectar podría ser una amenaza.**

Rápidamente, llamó a su hijo para que le ayudase. Le explicó que los dispositivos que encontramos por la calle pueden estar infectados y que conviene no utilizarlos. Por suerte, el antivirus estaba debidamente actualizado y pudo contener la amenaza.

Además, le comentó que podría tratarse de un alumno queriendo infectar el equipo de su profesora intencionadamente para tratar de conseguir las preguntas de un examen o cambiar su nota, por poner algunos ejemplos, mediante la instalación de algún *malware*. ¡Qué casualidad que estuviese justo caído a la altura de la puerta del piloto del coche!

Por suerte para nuestra protagonista el incidente no fue a más. Pero, **¿qué habría pasado si no tuviese su antivirus actualizado?**



NUESTROS DATOS RRSS ¿SOMOS IMPORTANTES?

- ¿Qué hacen con todo eso?
 - De TODO MALO
 - PREDECIR COMPORTAMIENTOS.
 - ELABORACIÓN DE PERFILES (MUY PELIGROSO – RGPD)
 - PUBLICIDAD DIRIGIDA (Kellogs mujeres embarazadas 3 a 6 meses – 1,6 mil).
- ¿Qué hacen con todo eso?
 - De TODO BUENO.
 - Bancos pueden aceptar o no transferencias.
 - Procesar datos tráfico para ir más rápido a algún lugar.
 - Predecir enfermedad para se expanda menos...

PERFILES / IDENTIDADES EN RRSS

- PERFIL ABIERTO (NEGOCIO).
 - BENEFICIO: MAYOR ALCANCE
 - “MALEFICIO”: MAYOR RIESGO DE SUPLANTACIÓN DE IDENTIDAD

CASO: Falsedad Documental.

NOMBRE: Ataque al CISO.

NEXO: EMAIL.

CASO: Usurpación de Estado Civil.

NOMBRE: Ej. Laura y Laura_.

NEXO: Instagram / OnlyFans

MODALIDADES DELICTIVAS



BIZUM INVERSO

https://www.antena3.com/noticias/sociedad/timo-bizum-inverso-nueva-estafa-que-alerta-guardia-civil_2022061062a31303837e3c0001296d67.html

La Guardia Civil viene advirtiendo en los últimos días de un tipo de estafa con la que es muy fácil caer. La han denominado el **timo del 'Bizum inverso'**.

¿En qué consiste? Normalmente suelen coger datos de personas que han puesto su contacto en páginas de anuncios. Se hacen pasar por alguien interesado en ellos y ahí es dónde empieza el engaño.

Les **envían una solicitud de 'bizum'**. Pero lo que realmente les solicitan dinero pero en el concepto, normalmente, suelen referirse como "pago". Las víctimas, al leerlo, piensan que es cierto y al clicar, lo que realmente están haciendo **es pagar a sus estafadores**.

La Guardia Civil recalca que fijarse bien en este tipo de operaciones porque los ladrones juegan a despistar al usuario ya que este al clicar en el mensaje está dando su consentimiento para que se realice el pago de dinero.





Cadena Dial

<https://www.cadenadial.com> › cuidado-timo-bizum-in... ⋮

Cuidado con el timo del 'Bizum inverso': un usuario perdió ...

13 jun 2022 — Un usuario llegó a perder hasta 9.000 euros con la estafa del '**Bizum inverso**'. Te contamos cómo funciona este timo, cada vez más habitual.



La Voz de Galicia

<https://www.lavozdeg Galicia.es> › vigo › 2023/11/06 › d... ⋮

Estafan 5.500 euros a un cliente que hizo 19 veces un ...

7 nov 2023 — La Guardia Civil ha detenido a dos jóvenes, vecinos de Vigo de 20 y 23 años, pc supuestamente timar 5.500 euros a través de la app de **Bizum** ...



El País

<https://elpais.com> › España ⋮

La estafa del “bizum inverso”, o cómo perder el dinero ...

8 jun 2022 — La Guardia Civil recupera más de 6.000 euros sustraídos mediante engaño a un hombre que vendía un artículo en un portal de segunda mano.

Falta: OURENSE | Buscar con: OURENSE



La Voz de Asturias

<https://www.lavozdeasturias.es> › temas › estafas ⋮

Últimas noticias sobre Estafas. La Voz de Asturias

Un momento del juicio en **Ourense**. Puso a la venta en internet un ... La amenaza de las ciberestafas: del **Bizum inverso** a contestar «sí» a una llamada de teléfono.



La Región

<https://www.laregion.es> › Sociedad ⋮

Ojo, así son las 10 estafas del siglo XXI

23 dic 2023 — El **bizum**, un arma de doble filo: de la falsa compra al “**inverso**”. Es una gran innovación, no cabe duda, pero su facilidad de uso también lo ...

BLANQUEO DE CAPITALES... ¿?

El blanqueo de capitales consiste en ocultar o encubrir el origen de beneficios obtenidos ilícitamente, de forma que parezcan provenir de fuentes legítimas. Normalmente es un componente de otros delitos graves como el tráfico de drogas, el robo con violencia o la extorsión.

“

1. El que adquiera, posea, utilice, convierta, o transmita bienes, sabiendo que éstos tienen su origen en una actividad delictiva, cometida por él o por cualquiera tercera persona, o realice cualquier otro acto para ocultar o encubrir su origen ilícito, o para ayudar a la persona que haya participado en la infracción o infracciones a eludir las consecuencias legales de sus actos, será castigado con la pena de prisión de seis meses a seis años y multa del tanto al triplo del valor de los bienes. En estos casos, los jueces o tribunales, atendiendo a la gravedad del hecho y a las circunstancias personales del delincuente, podrán imponer también a éste la pena de inhabilitación especial para el ejercicio de su profesión o industria por tiempo de uno a tres años, y acordar la medida de clausura temporal o definitiva del establecimiento o local. Si la clausura fuese temporal, su duración no podrá exceder de cinco años.

Artículo 301.1 del Código Penal

BIZUM DIRIGIDO Y TRANSFERENCIA CTA. BANCARIA CASA RURAL

DIFICULTAR LA INVESTIGACIÓN

ESTAFA que se comete, utilizando un número de teléfono.

El ciberdelincuente tras publicar un anuncio de un bien inexistente, atractivo para la víctima, pone un número telefónico elegido al azar.

Ese número telefónico será el receptor del dinero objeto de la estafa.

Una vez tienen constancia de la transferencia económica efectuada por la víctima, se pondrán en contacto con el beneficiario y alegando cualquier excusa, le solicitarán la devolución del dinero, a otro número telefónico o incluso a través de pasarelas como Western Union, WorldRemit y similares, dificultando con todo ello la investigación del ilícito.

BLANQUEO DE CAPITAL



ABOGADA EN EXTRANJERO

LA IMPORTANCIA DEL CORREO ELECTRÓNICO

SMS informa de problemas en cuenta correo "yahoo". (22.45 horas)

Introduce sus datos en el link facilitado. (22.45 horas)

No observa nada raro y continúa con su "vida normal"

Día siguiente NO ACCEDE a su correo electrónico (09.00 horas).

Recibe en su terminal telefónico multitud de llamadas de clientes preguntándole si necesitaba algo (09.00 hasta 21.00 horas).

Se confirma que ciberdelincuente envía texto a todos sus contactos:

"Hola soy xxxxxx. Estoy en el extranjero. He dejado olvidada mi cartera y mi móvil en un taxi. Necesito 2000 euros que te los devolveré en cuanto llegue a Ourense. Mándamelos por Western Union. No me llames, porque el teléfono no se quien lo tendrá. Gracias."



¿CÓMO LO HACEN?

- Fake Name Generator
- This Person Does Not Exist
- Fake WhatsApp (Capturas)

Your Randomly Generated Identity

Gender

Name set

Country

[Generate](#) [Advanced Options](#)

These name sets apply to this country:
Hispanic

<https://www.fakenamegenerator.com/>



Logged in users can view full social security numbers and can save their fake names to use later.



Otilde Corrales Correa

Avda. Los llanos, 43
26311 Cordovín

Geo coordinates **42.356002, -2.72798**

PHONE

Phone 610 252 028

Country code 34

BIRTHDAY

Birthday October 21, 1952

Age 71 years old

Tropical zodiac Libra

ONLINE

Email Address OtildeCorralesCorrea@teleworm.us
This is a real email address. [Click here to activate it!](#)

Username Suffell

Password Uong5ohquee

Website MortgageDo.es

Browser user agent Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/73.0.3683.103 Safari/537.36

FINANCE

MasterCard 5158 9757 8615 6424

Expires 3/2025

CVC2 695

EMPLOYMENT

Company One-Up Realtors

Occupation Chemical equipment tender

PHYSICAL CHARACTERISTICS

Height 5' 4" (163 centimeters)

Weight 214.5 pounds (97.5 kilograms)

Blood type A+

TRACKING NUMBERS

UPS tracking number 1Z 65A 718 63 9433 951 0

Western Union MTCN 5362334873

MoneyGram MTCN 78616871

OTHER

Favorite color Green

Vehicle 2010 Toyota Hilux

GUID ee39318a-05dd-42fb-ac15-f71248945184

QR Code [Click to view the QR code for this identity](#)

Generador De Caras Aleatorias (Esta Persona No Existe)

Generar cara humana al azar en 1 clic y descargarlo! Al generó fotos falsas de personas: hombre, mujer o niño.

Género:

Femenino

Edad:

50 + años de ec

Etnia:

Latino Hispano

Actualizar Imagen



CAPTURAS NO APORTAN EVIDENCIA SUFICIENTE

<https://www.fakewhats.com/generator>

The screenshot displays the 'WhatsApp FAKE CHAT' generator website. The navigation menu includes: SECOND NUMBER, WHATS SIM, FAKE, RECEIVE, FREE, HOW-TO, GENERATOR, SPOOFBOX. The main interface is divided into four sections: PHONE SETTINGS, BATTERY OPTIONS, CONNECTION, and MESSAGES. The 'PHONE SETTINGS' section contains the following fields:

Name	Profile Picture <input checked="" type="checkbox"/> Show?	Phone Clock	"Contact"
Johnny Doe	Click to upload	9:41 AM	Contact
Online	Operator	"Chats"	"Message"
online	vodafone	Chats	Message

At the bottom, a smartphone mockup shows a WhatsApp chat with 'Johnny Doe' (online) containing a message: 'Lorem Ipsum is simply dummy text of the printing and typesetting industry.' The status bar shows 'vodafone', '9:41 AM', and '50%' battery. A cookie notice is visible in the bottom right corner with a 'Got it!' button.

CAPTURAS NO APORTAN EVIDENCIA SUFICIENTE

The screenshot displays the 'Fake Details' website, which is an 'Online Generator'. The navigation menu includes 'Mail', 'IMEI', 'Personal Detail', 'Social Media', 'Text Messenger', 'Name Generator', 'Blog', and 'More', along with a 'Press Release' button. The main content area is titled 'Fake Telegram Chat Generator' and features a 'Live preview' window. On the left, there are configuration options: 'Parts' (Hide Header, Hide Footer, Offline), 'Clock' (10:04 am), 'Battery percent' (50), 'Direct message with' (John Doe), 'Status' (online), and 'Profile photo' (Select Image). The 'Live preview' window shows a simulated Telegram chat interface with a contact named 'John Doe' (online). The chat history includes three messages: a white bubble from John Doe saying 'Hello there. Thanks for the follow. Did you notice, that I am an egg? A talking egg? Damn!' (2:40 PM), a green bubble from the user replying 'Yeah that is crazy, but people can change their own picture and build their own Twitter conversation with this generator, so it does not matter that you are an egg' (2:40 PM), and a white bubble from John Doe replying 'Thanks mate! Feel way better now. Oh, and guys, these messages will be removed once your add your own :-)' (2:40 PM).

<https://fakedetail.com/fake-telegram-chat-generator>

Fake Facebook Messenger Chat Generator

 Desktop View

 Tablet View

 Mobile View

Parts :

- Active now
- Hide Header
- Hide Footer

Layout :

- android
- iphone

Clock

10:04 am

Battery percent

50

Direct message with

John Doe

Person 1 | Person 2

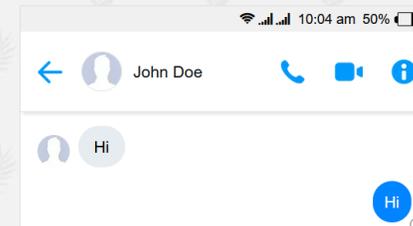


Profile photo

Select Image

Message

Live preview



CONTROL PARENTAL

ANDROID:

<https://www.youtube.com/watch?v=4cES-8KtxQM>

IOS:

<https://www.youtube.com/watch?v=4ZwnJsW--tQ>