CIBERSEGURIDAD Y MENORES

CIBERSEGURIDAD Y MENORES

Centro Público Integrado José García García de Mende

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?
- Apuestas realizadas por menores.
- 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.

https://abogadosiurisemerita.com/2019/03/25/revisar-telefono-hijos/

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.

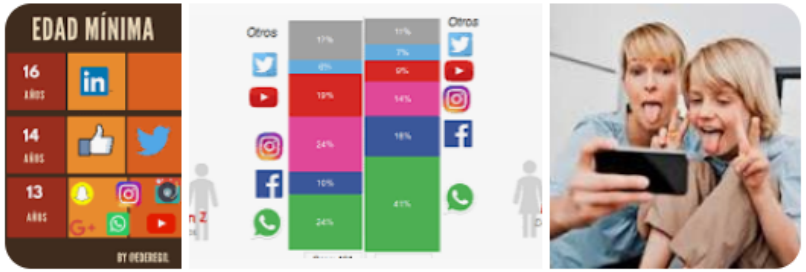
EDAD RECOMENDADA PARA DAR EL PRIMER TELÉFONO MÓVIL A UN NIÑO

https://es.aliexpress.com/item/4000458188679.html?spm=a2g0o.productlist.main.3.46e526aeUrXDfi&algo_pvid=a9dc6760-9409-400c-8021-c1261e80e625&algo_exp_id=a9dc6760-9409-400c-8021-c1261e80e625-1&pdp_ext_f=%7B%22sku_id%22%3A%2210000001861671560%22%7D&pdp_npi=3%40dis%21EUR%2152.89%2144.96%21%21%21%21%21%402145280e16792227263792674d06eb%2110000001861671560%21sea%21ES%210&curPageLogUid=NEZy1qbGmP13

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

¿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 'sotfware' para acceder a las contraseñas de los correos electrónicos de los docentes

ELISA LOIS

Pontevedra - 02 MAR 2019 - 18:18 CET

28

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.

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?

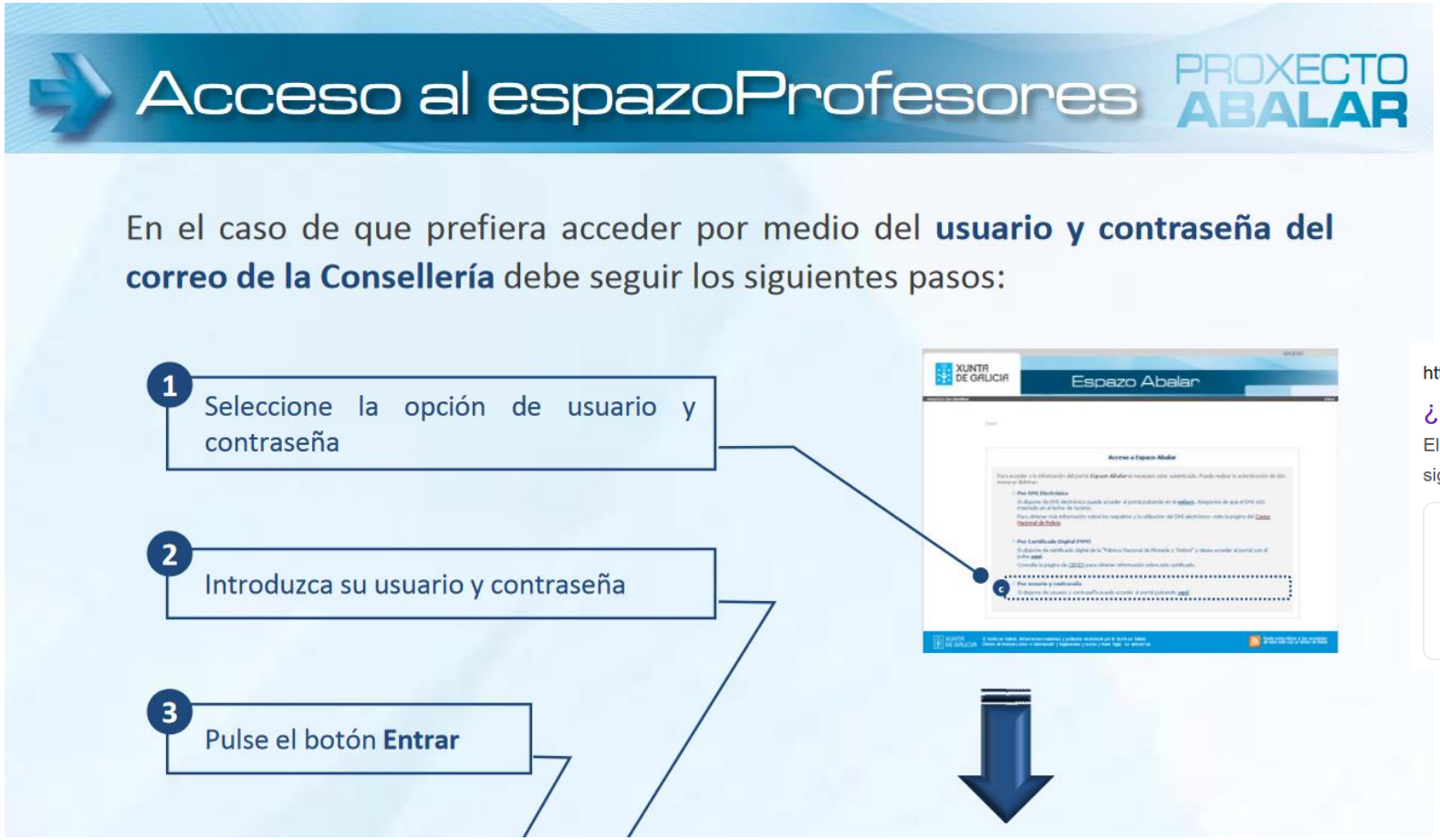
NIVEL	ALCANCE	CONTROL	
A	PRO/TEC	**Gestión de contraseñas** Defines un sistema de gestión de contraseñas avanzado que contempla todos los aspectos relativos a su ciclo de vida.	☐
A	PRO/TEC	**Técnicas de autenticación externas** Consideras la utilización de sistemas de autenticación externos descentralizados.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

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

https://haveibeenpwned.com/

MÓVILES: Siempre BIOMETRÍA y factor Doble Autentificación.

¿Cómo se puede gestionar la seguridad?



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 espazoAbalar 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 adxuntos

MATERIAIS A TRABALLAR PROFESORAS [redacted]

Lun, 03/16/2020 - 16:10 — COORD.TIC

MATERIAIS A TRABALLAR

PROFESORAS [redacted]

[redacted]@gmail.con

[redacted]e@gmail.com

O alumnado de Latín de 4º de ESO e de 4º de ESO (A) de Lingua castelá e literatura, utilizan CLASSROON, 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 adxuntos

[redacted]: 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 [redacted]

En internet "está todo"… Incluso una Guías para profesores y ¡¡¡para ciberdelincuentes!!!.

MATERIAIS A TRABALLAR - [redacted]@gmail.com

Lun, 03/16/2020 - 10:12 — COORD.TIC

MATERIAIS A TRABALLAR

PROFESOR [redacted]

Subiranse os contidos paulatinamente para ir traballando estas semanas.

17 adxuntos

RESUMO PROGRAMACIÓN PLÁSTICA

Mar, 11/06/2018 - 10:40 — COORD.TIC

blogue de COORD.TIC | 1 adxunto

(11) [redacted]

ARTISTA [redacted]

Seguir

Busca y encuentra información sobre cualquier persona en España

Nombre/s

Nombre/s

1º Apellido

1º Apellido

2º Apellido

2º Apellido

DNI (opcional)

DNI (Opcional)

Tu E-mail

Tu E-mail

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

Buscar

¿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.

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 ciberdelitos 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 Ubieto, 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.

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.

¿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?

CERBERUS

DISPOSITIVOS SECURIZADOS
(BIOMETRÍA, NO PIN O PATRÓN)

WHATSAPP WEB – TELEGRAM WEB ---OJO

¿Cómo se puede gestionar la seguridad?

BBVA ¿Es seguro guardar las contraseñas en el navegador? English

¿Es seguro guardar las contraseñas en el navegador?

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.

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 una 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.

¿Cómo se puede gestionar la seguridad?

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

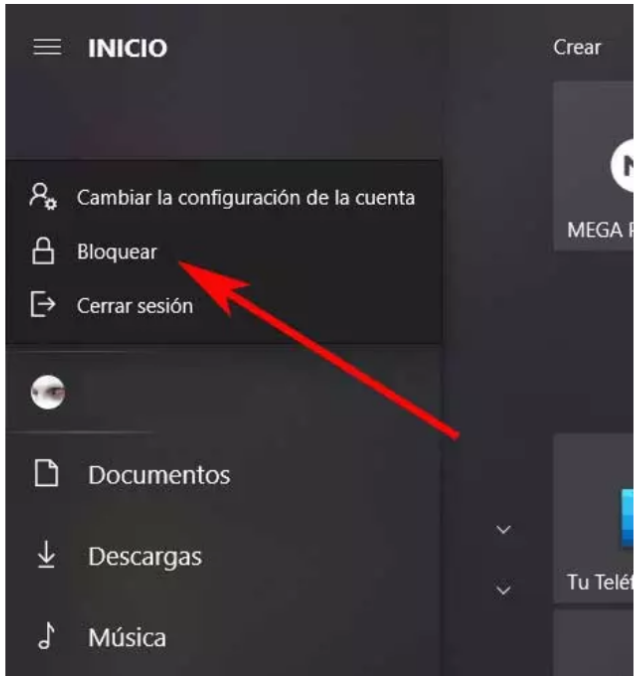
David Onieva | Actualizado el 10 de enero, 2022 • 10:38

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 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.

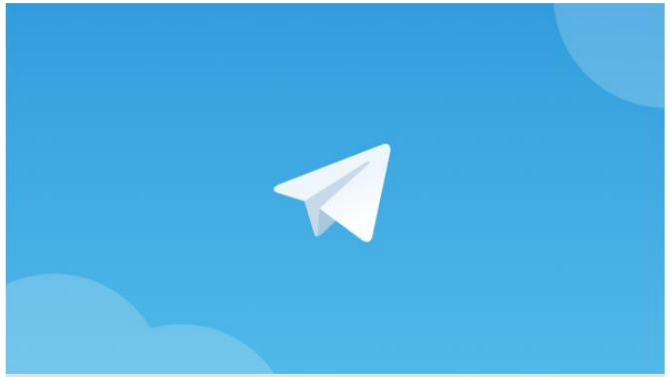
En muchos sentidos, ha sido gracias a Signal que el cifrado de extremo a extremo ha conseguido hacerse tan popular entre las aplicaciones de mensajería. Incluso la competencia, WhatsApp, Facebook Messenger y Skype, utilizan el protocolo de Signal para una comunicación segura. Pero, en comparación, Signal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



La app es una de las más seguras del mercado, pero también tiene configuraciones que ajustan su nivel de privacidad. | ***Fuente:*** *Telegram*

EL NEGOCIO DE LA PRIVACIDAD

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		

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

- 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… ¿Pondríais 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…?

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…)
  - Batterry 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 tíntes 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.

fintonic

¿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.

Samsung Health

Traducción del inglés - Samsung Health es una aplicación gratuita desarrollada por Samsung que sirve para rastrear varios aspectos de la vida diaria que contribuyen al bienestar, como la actividad física, la dieta y el sueño. Wikipedia (Inglés)

Ver descripción original

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.

SEGURIDAD - USB

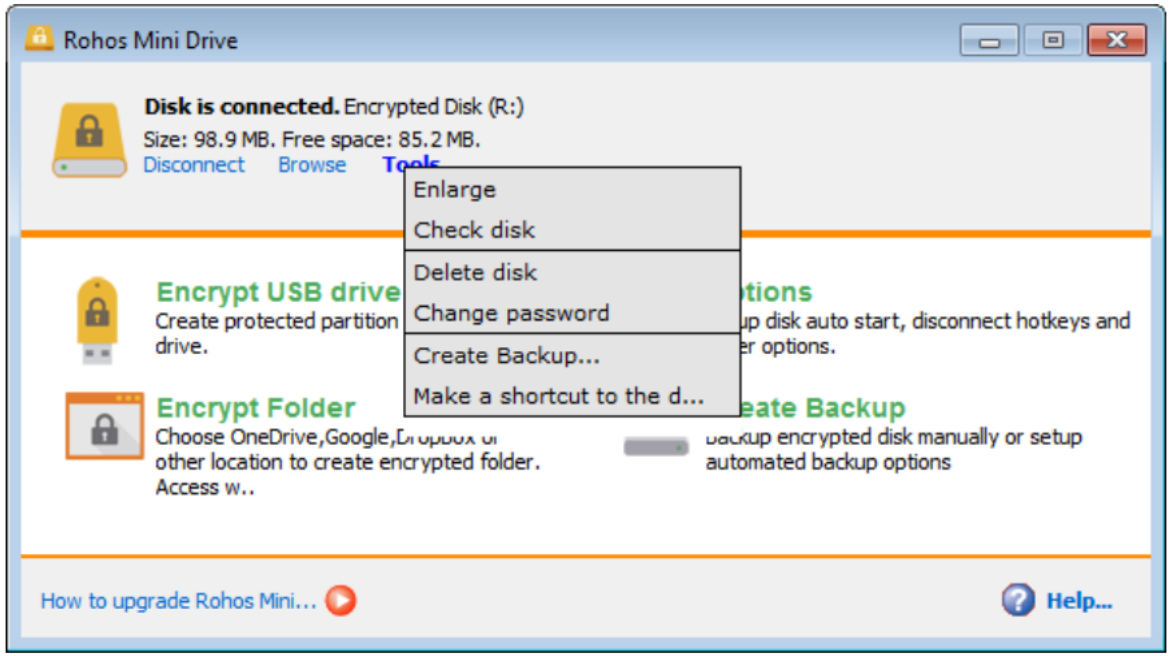
Riesgos de utilizar memorias USB con vistas a compartir información

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