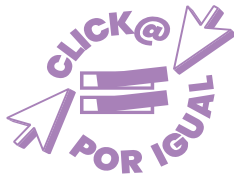




Ciberseguridad



ÍNDICE

INTRODUCCIÓN

LOS DIFERENTES TIPOS DE AMENAZAS DIGITALES:

- ▶ Phishing.
- ▶ Vishing y Smishing.
- ▶ ¿Cómo puedo protegerme de estos ataques?
- ▶ Pasos a seguir para comprobar un posible fraude.

EL ANTIVIRUS : UN ESCUDO PARA PROTEGERSE CONTRA LAS AMENAZAS DIGITALES

NAVEGAR DE FORMA SEGURA:

- ▶ WIFI: ¿Cómo usarlo?.
- ▶ Distinguir las webs fiables.
- ▶ Saber distinguir apps seguras para su descarga.
- ▶ ¿Y para mis hijas/os o nietas/os? ¿Cómo puedo velar por su seguridad digital?.

SEGURIDAD EN LAS RRSS:

- ▶ La contraseña: la base de una navegación segura.
- ▶ Pasos para configurar nuestro perfil.
- ▶ Whatsapp: una aplicación de mensajería instantánea.
- ▶ Informaciones y cuentas falsas en RRSS.
- ▶ Consideraciones para publicar en RRSS.

VÍDEOS Y WEBGRAFÍA



INTRODUCCIÓN

Hoy en día, la digitalización va impregnando, cada vez más, todas las facetas de nuestras vidas. Desde su aparición, internet y las nuevas tecnologías han revolucionado nuestra forma de interactuar. A la hora de hablar con familiares y amigos/os, de escuchar música, de hacer compras, o incluso de realizar trámites administrativos, esta manera de comunicarse y conectar se ha vuelto imprescindible. De tal modo que el número infinito de herramientas y de posibilidades ¡a veces nos da vértigo! El mundo de las nuevas tecnologías, por estimulante que parezca, puede resultar poco seguro, ¿verdad?

Además, muchas veces, los servicios que utilizamos funcionan gracias a la información que les proporcionamos. Por eso, el uso de estas tecnologías implica adoptar ciertas medidas para protegerse de posibles situaciones problemáticas. Del mismo modo que hay que tener precauciones cuando paseamos por la calle, tenemos que tener en cuenta otras para navegar por internet.

Pero, no te preocupes, al contrario de lo que se podría pensar, la ciberseguridad no requiere de un alto nivel de conocimiento técnico. Sólo hay que tener en mente algunos consejos y buenas prácticas. De hecho, a través de esta guía trataremos de facilitar conocimientos para que puedas mantener la privacidad y seguridad en la red.

Juntas aprenderemos, paso por paso, a usar y configurar nuestros dispositivos, porque ya verás que la ciberseguridad, ¡es para todas! ¿Listas? Pues, ¡descubramos cómo actuar para convertirnos en usuarias ciberseguras!

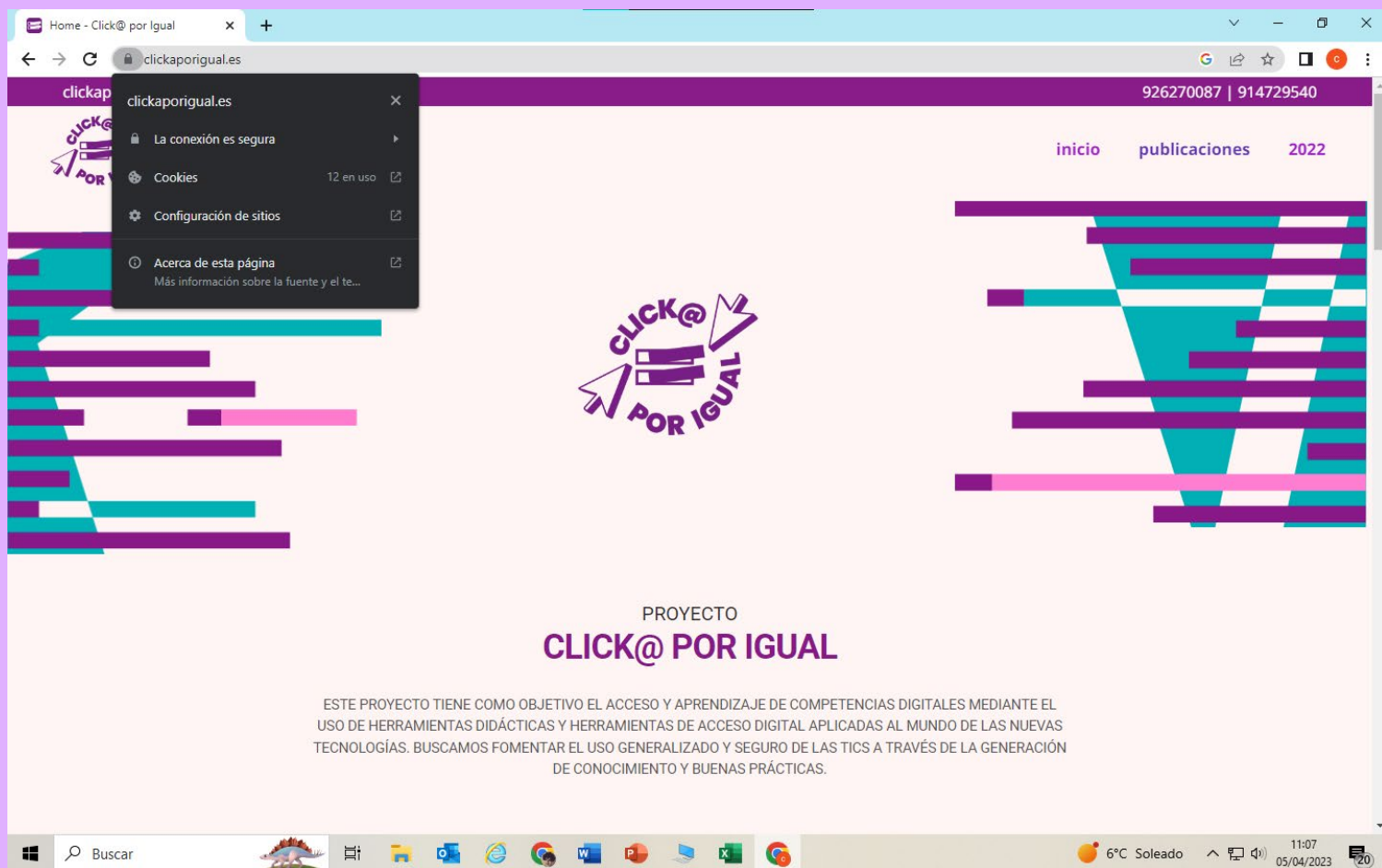
¿QUÉ ES LA CIBERSEGURIDAD?

EMPEZAREMOS POR ENTENDER QUE SIGNIFICA CIBERSEGURIDAD:

La ciberseguridad, también conocida como seguridad informática, es un conjunto de prácticas y herramientas dirigidas a proteger los dispositivos informáticos, servidores, sistemas electrónicos y redes de posibles ataques digitales maliciosos.

Se trata de medidas que se implementan para defendernos de intentos de robo de información o de control de nuestros dispositivos.

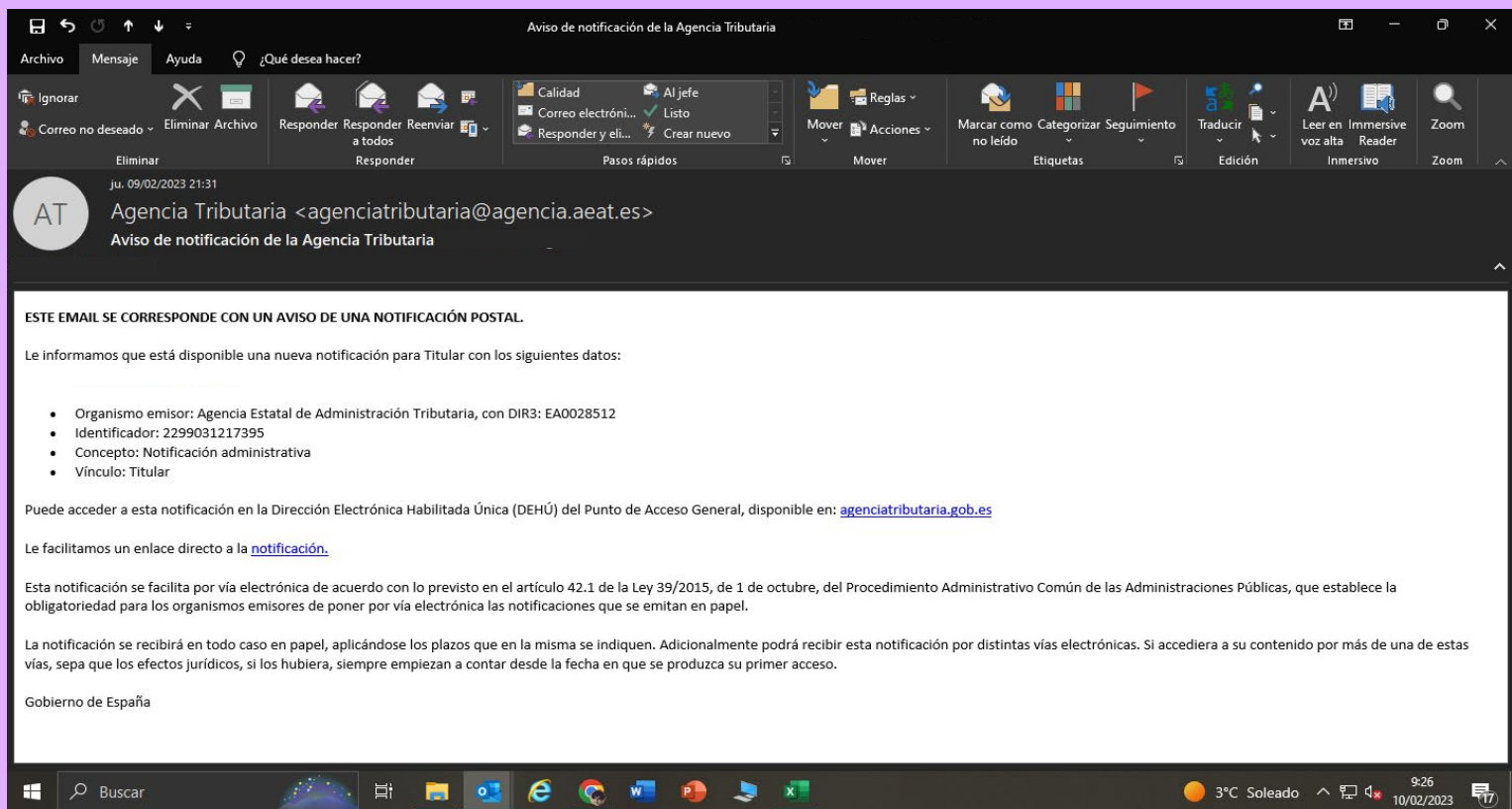
RECUERDA: ante cualquier duda, puedes llamar a la Línea de Ayuda en Ciberseguridad de INCIBE al 017 o contactar a través de los canales de chat de WhatsApp o Telegram de Tu Ayuda en Ciberseguridad, donde expertos en la materia te ayudan a resolver los problemas digitales que encuentres, de manera gratuita y confidencial.



LOS DIFERENTES TIPOS DE AMENAZAS DIGITALES

Los ciberataques son cada vez más diversos e ingeniosos, y se aprovechan de nuestras vulnerabilidades para llegar a sus fines. De forma general, los fraudes en internet suelen presentar un carácter urgente o atractivo, para evitar que te tomes tiempo y te lo pienses dos veces. Por eso, descubramos juntas los diferentes tipos de amenazas que podemos encontrar en la web y cómo evitar que nos roben nuestros datos personales.





Phishing

El phishing es una ciberestafa que consiste en el envío de correos o mensajes, incluso por vía de redes sociales. En este caso el ciberdelincuente se hace pasar por una entidad bancaria o organismo público para robar datos bancarios o personales y nos dirige a una web fraudulenta a través de un enlace. Estos mensajes suelen ser muy parecidos a los de las empresas o instituciones que suplantán.



Vishing y Smishing

Estas son dos variantes del phishing y son muy parecidas en su ejecución. ¿Cómo funcionan? El vishing se lleva a cabo mediante llamadas telefónicas mientras que el canal utilizado para el smishing son los sms del móvil. La Oficina de Seguridad del Internauta (OSI) explica que el mecanismo de estas estafas consiste en alertar a las víctimas de un cargo extraño en su cuenta, de un cargo extra por parte de su compañía de servicios, o de problemas de seguridad en sus cuentas de usuario para invitarlas a ceder datos personales.



¿Cómo puedo protegerme de estos ataques?

Pasos a seguir para comprobar un posible fraude

1



Confirma si la dirección de email en la que has recibido el mail ha sido facilitada por ti para que la empresa o entidad pública que supuestamente te escribe pueda comunicarse contigo. Por ejemplo, si se ponen en contacto desde una empresa de suministros cuando no has dado tu contacto de email estamos ante un contacto ilegítimo.

2



Pregúntate **si la institución tendría que comunicarse contigo**. Por ejemplo, nos contacta la DGT (dirección general de tráfico) con la notificación de una multa realizada con un automóvil y no tenemos carné de conducir.

3



Desconfía cuando se usa un lenguaje con errores de ortografía, concordancia o redacción.

Se suelen usar traductores automáticos para realizar emails malintencionados que producen este tipo de errores.

Comprueba que el nombre del remitente es conocido y que la dirección de correo electrónico es legítima.

Verifica que el dominio (texto que se encuentra a la derecha de la arroba "@") se corresponde con la empresa o entidad de la que dice provenir. Busca distintivos o logos de la empresa o entidad pública y ante la duda contrasta con una búsqueda en internet.

4



5



Si el **contenido del email o mensaje te parece sospechoso, confía en tu sentido común** y no sigas las indicaciones. Por ejemplo, cuando te llega la notificación de un premio de un sorteo en el que no has participado, una oferta de empleo a la que no has aplicado, etc.

Ten cuidado con los **correos o sms amenazantes** o los que te dejan poco tiempo para actuar. Por ejemplo, bloqueo de cuentas, chantajes, etc.

6



7



Si tienes la sospecha de que sea un **virus**, haz un **análisis con el antivirus** y permite que actúe. Si tienes alguna sesión abierta, red social o banco, **ciérrala** para que no robe tus datos.



RECUERDA



Una empresa o entidad pública **nunca** solicitará datos personales: usuario/a, contraseñas o claves. Si necesita verificar tu identidad probablemente sea en persona o te pedirá que confirmes los datos que ya tienen pero nunca te solicitará tus claves.



Es importante que no pinches enlaces recibidos a través de mensajes o correos, y que compruebes siempre quién es el remitente de cada comunicación y cómo ha sido redactado el mensaje.



Si al hablar con una persona por teléfono o al leer un mensaje, dudas de su autenticidad, corta la comunicación y contacta a través de los canales oficiales con la entidad interesada para comprobar si es cierta la comunicación y/o para informarles de lo sucedido.



Si recibes un email, sms, whatsapp o mensaje en Redes Sociales de un/a familiar o amigo/a con un contenido no habitual o que te hace sospechar, no pinches en enlaces y avisa a esa persona porque puede tener un virus en su dispositivo.

RECOMENDACIÓN



Si quieres ampliar tus conocimientos en ciberataques, te recomendamos la **Guía de Ciberataques** del Instituto Nacional de Ciberseguridad (INCIBE) y al servicio de la Oficina de Seguridad del Internauta (OSI): <https://www.incibe.es/sites/default/files/docs/guia-ciberataques/osi-guia-ciberataques.pdf>

Si quieres saber qué es la ingeniería social:
[Experiencia senior - Cómo intentan engañarte: la ingeniería social](#)

Notas



EL ANTIVIRUS : UN ESCUDO PARA PROTEGERSE CONTRA LAS AMENAZAS DIGITALES

Una de las herramientas útiles para mantener tu seguridad y privacidad digital es el antivirus.

Un antivirus es un programa informático cuyo objetivo es detectar y eliminar virus o aplicaciones maliciosas de tus dispositivos para que puedas usarlos con total seguridad.

Muchas veces nuestros dispositivos electrónicos traen una herramienta antivirus ya instalada, pero hay que comprobar en los parámetros, en la pestaña relacionada con la seguridad, que está activada y actualizada para detectar las últimas amenazas en la red.

También es posible descargar otro antivirus a través del playstore o el apple store. Existen varias opciones que puedes comparar revisando la valoración y los comentarios de los usuarios.

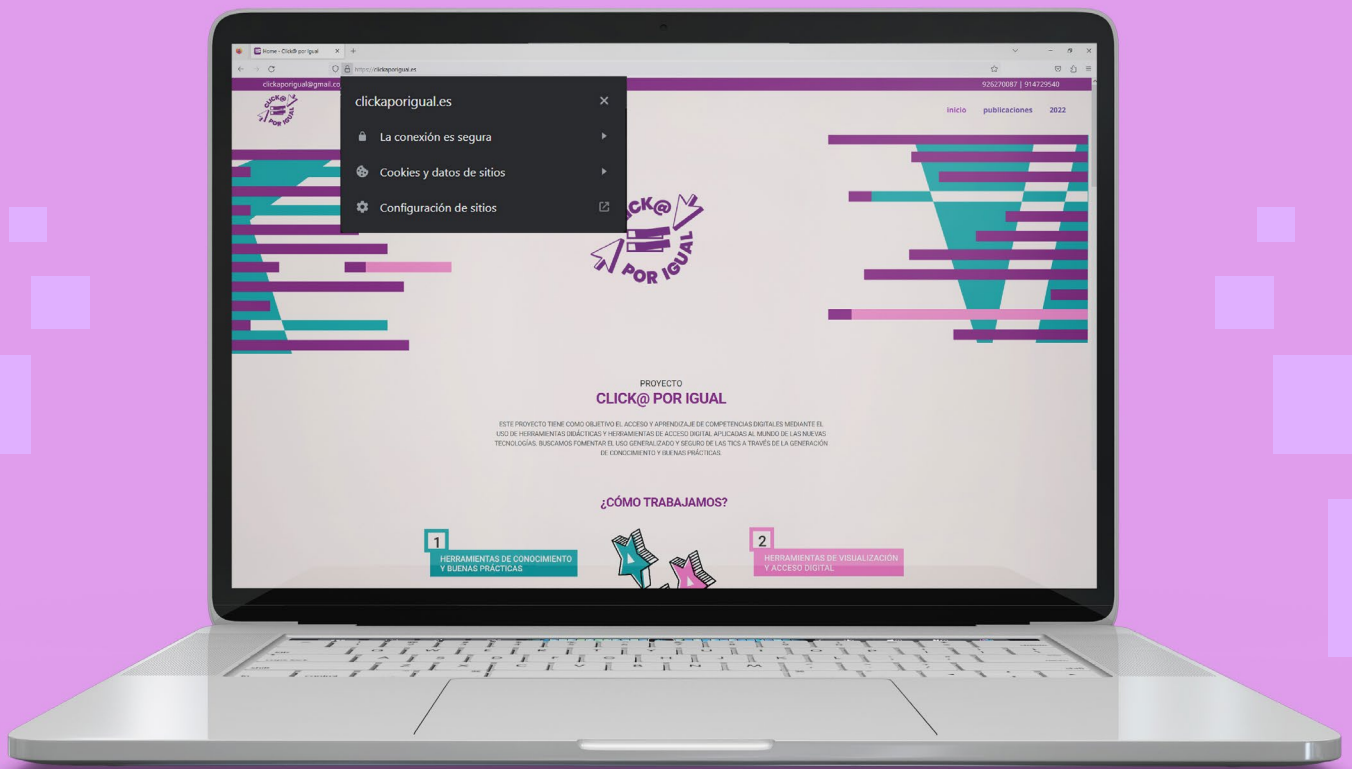


RECOMENDACIÓN:

Para entender mejor la función del antivirus, te recomendamos: [Antivirus. ¿Cómo nos protegen?](#)



Notas



NAVEGAR DE FORMA SEGURA EN INTERNET

Pasos a seguir para comprobar un posible fraude

Realizar un trámite administrativo, comprar una prenda de ropa, o comunicarse con familiares o amistades: ¿Cuál es el punto común entre estas tres situaciones? ¡Todas ellas son actividades que se pueden llevar a cabo a través de Internet!

Sin embargo, para disfrutar de todas las funcionalidades que ofrece la web con total seguridad, hay que tener en cuenta algunas recomendaciones.

WIFI: ¿Cómo usarlo?

Es importante priorizar la conexión a redes wifi privadas porque son más seguras. Si estás fuera de casa y es posible, conéctate a Internet a través de tu propia conexión móvil 4G/5G. En el caso que solo tengas acceso a redes wifi públicas y gratuitas (en bibliotecas, centros cívicos, cafeterías...):

- Comprueba siempre que la red es oficial.
- Evita ingresar con tu usuario y

contraseña en alguna web, porque los ciberdelincuentes pueden acceder más fácilmente a tus datos.

- Verifica que tu antivirus esté actualizado y activado.

Distinguir las web fiables

Cuando estés navegando por internet, asegúrate siempre de que la página en la que estás es segura, especialmente a la hora de facilitar datos sensibles.

¿Cómo lo puedes comprobar? La URL de una web segura empieza por "https" y muestra un candado en la barra de direcciones. Cuando hagas clic sobre dicho candado, la URL también deberá estar bien escrita. *(Ver imagen)

Ocurre lo mismo a la hora de hacer compras online. Para evitar las web fraudulentas y los chollos recuerda que puedes mirar la información de la empresa, porque una tienda online legítima dispondrá siempre de un apartado con NIF y otros datos. Estate también atenta al precio de los productos, si están muy bajos o tienen grandes descuentos es probable que se trate de un fraude.

Además, antes de hacer una compra en cualquier página que sea, puedes buscar información sobre las condiciones de envío, la devolución de productos y averiguar las formas de pago permitidas. Muchas veces, las tiendas falsas sólo permiten pago por transferencia internacional.

RECOMENDACIÓN:

También es recomendable que consultes la valoración de otros usuarios sobre la página web o el vendedor mediante búsquedas en la red.



Saber distinguir apps seguras para su descarga.

Cuando quieres instalar nuevas aplicaciones, descárgalas siempre a través de las tiendas de app oficiales (Playstore, Applestore...) y acuérdate de revisar las opiniones y las valoraciones de los usuarios, ya que muchas veces si una app no es segura, se ve reflejado en los comentarios.

No des permisos a las apps cuando notes que no son coherentes o imprescindibles para el correcto funcionamiento de la app.

¿Y para mis hijas/os o nietas/os? ¿Cómo puedo velar por su seguridad digital?



Hoy día los jóvenes y niñas/os desarrollan competencias digitales muy temprano ya que se ven expuestos a muchos contenidos virtuales y pueden relacionarse con los demás por medio de dispositivos móviles. Sin embargo, a pesar de que ellos adquieran conocimientos y desarrollen hábitos muy fácilmente, es necesario acompañarlos en este proceso de descubrimiento y de aprendizaje, porque no siempre poseen todas las claves para entender y responder adecuadamente a lo que viven en la red.

Por eso, ¡aquí estamos nosotras, para ayudarles a aprovechar al máximo los beneficios que les puede aportar Internet en total seguridad! Así, aunque incluso a nosotras el mundo virtual se nos puede aturullar, nuestra experiencia de adultas junto con nuestro sentido común hace de nosotras unas aliadas imprescindibles para nuestras/os hijas/os o nietas/os ante los peligros en Internet. De hecho, al dialogar y acompañarlos, podremos sensibilizarlos sobre la importancia de tener mucho cuidado con sus datos personales y a la hora de interactuar con otras personas en la red.



Una herramienta útil para prevenir situaciones peligrosas como el ciberbullying (acoso entre iguales a través de medios digitales), o la exposición a contenidos inapropiados es el control parental. Hoy día todos los dispositivos móviles, que sean Iphone o Android, incluyen opciones para adaptar tu móvil para que lo usen niñas/os.

Aquí siguen algunos ejemplos para configurar tu móvil si quieres que tus peques lo utilicen con total seguridad :

El modo Kids (Modo Niños) en los teléfonos Android (teléfonos que no sean Iphones):

Desliza el dedo hacia abajo en la pantalla para que aparezca el panel de notificaciones y, a continuación, deslízalo hacia la izquierda. Selecciona Modo Niños en el panel de notificaciones para configurarlo.

Pulsa "Siguiete" y, a continuación, establece un código de acceso o una plantilla que tu peque desconozca. El código predeterminado es 0000. Luego aparecerá la pantalla principal del Modo Niños.

Esto te permite iniciar el control parental, controlar el uso del dispositivo, ya que las/os niñas/os no pueden salir del modo infantil sin que se les pida el PIN o la plantilla. Todas las aplicaciones que se encuentran allí han sido seleccionadas para tus peques.

Si tu móvil no tiene este servicio, otra opción es configurar desde Google Play Store:

Ve a Google Play Store.

Dale al círculo del perfil de tu cuenta (está arriba a la derecha) y accede a "Ajustes".

Selecciona "Control parental" (dentro de Familia) y actívalo. Te pedirá que crees un PIN de protección, así que ponle uno y, por supuesto, no lo compartas con la niña/o porque podrá acceder para desactivarlo.

Hay tres secciones: aplicaciones y juegos, películas y música. Dentro de cada una de ellas encontrarás la clasificación PEGI, simplemente tienes que seleccionar el nivel que quieras (de PEGI 3 a todo el contenido)

Filtrar contenido y restringir acceso en Iphones:

Ve a Ajustes.

Selecciona Accesibilidad > Acceso Guiado.

Desliza el botón hacia la derecha para activar el Acceso Guiado y establece un código que tu peque desconozca.

Ahora que está configurado, cada vez que quieres utilizar el Acceso Guiado, abre la única aplicación que quieres que tu peque utilice y repite los dos primeros pasos para activar el Acceso Guiado.

Tendrás que entrar el código que has elegido cada vez que quieras activar el Acceso Guiado. Para salir de este modo, pulsa tres veces el botón lateral o el botón principal (según el modelo de iPhone) e introduce el código de acceso guiado.



RECOMENDACIÓN:

Otra aplicación útil para mantener la seguridad de tus peques es Youtube Kids : esta app les permite ver videos y contenidos adaptados a su edad.



Notas



SEGURIDAD EN LAS RRSS

Las redes sociales (RRSS) revolucionaron nuestras vidas al hacer posible que entremos en contacto con cualquier persona en el mundo, y desde cualquier sitio. Se han convertido año tras año en espacios atractivos porque permiten comunicarse con los demás de varias maneras y de forma instantánea. Hoy día las redes sociales también pueden ser un canal de información y/o de entretenimiento.

Sin embargo, para poder aprovechar al máximo las ventajas de las redes sociales, no se puede descuidar el proceso de configuración de nuestros perfiles. Por ejemplo, es importante crear una contraseña robusta, que no sea la misma que utilices en otras páginas para proteger tus cuentas de ciberataques.

Crea tu contraseña segura

PASO A PASO

PASO 1

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

Mi cuenta segura

PASO 2

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

MiCuentaSegura

PASO 3

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

MiCu3nt4S3gur4

PASO 4

Añadir caracteres especiales
Solo queda incluir algún símbolo (-!@#\$%^&*+=~|'"/{}[];:, ""<>.,?/).
MiCu3nt4S3gur4!

PASO 5

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

MM1Cu3nt4S3gur4!A

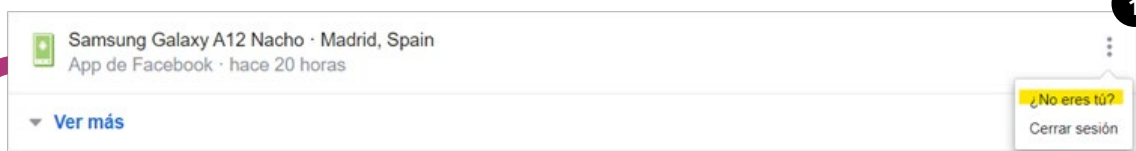
¡Y listo! Así de sencillo hemos creado nuestra contraseña robusta, segura y fácil de recordar.

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

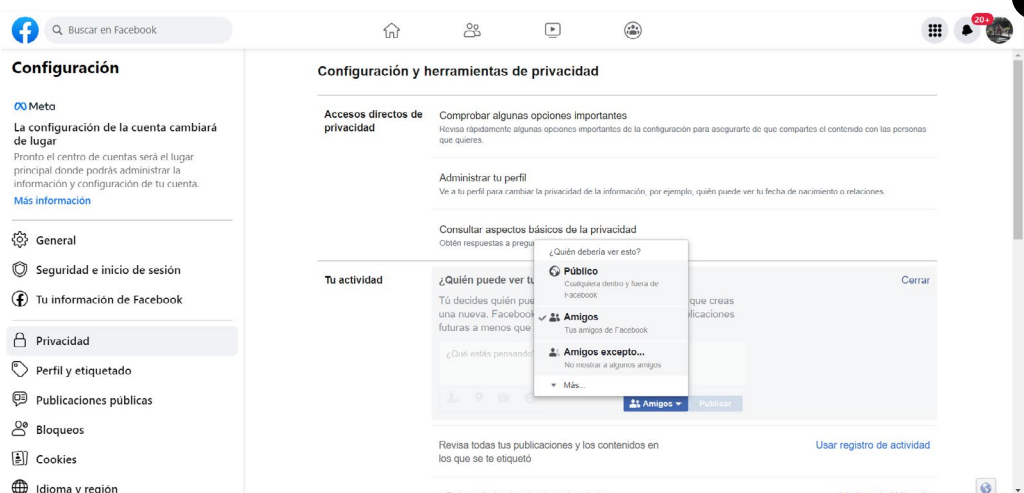
- Utiliza gestores de contraseñas para guardar todas las claves.
- No repitas las mismas contraseñas en distintas cuentas.
- Cámbialas cada cierto tiempo (3 meses).
- No las compartas con nadie, ni siquiera con familiares.
- Utiliza la verificación en dos pasos siempre que sea posible.
- Configura tu móvil para que si lo pierdes o lo roban, no se muestren los caracteres que pulas.

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

www.incibe.es | www.osi.es



La contraseña: la base de una navegación segura



El primer paso a seguir para asegurar la seguridad de tus cuentas en cualquier tipo de redes sociales es de crear una contraseña robusta para que no la pueda adivinar nadie.

PARA MANTENER EL CONTROL DE NUESTRA INFORMACIÓN, Y CONVERTIR LAS RRSS EN UN ESPACIO SEGURO Y PRIVADO, VEAMOS AHORA CÓMO CONFIGURAR NUESTROS PERFILES EN LAS REDES SOCIALES MÁS COMUNES :

Pasos para configurar nuestro perfil

En todas las redes sociales, existe una página de ajustes que te permite acceder a la configuración de tu cuenta. Estas páginas suelen ser accesibles a partir de nuestro perfil, y se identifican gracias a iconos que se parecen a un engranaje o a tres rayas.



Inténtalo ahora con Facebook: por ejemplo: Haz clic en tu foto del perfil en la parte superior derecha de Facebook. Selecciona Configuración y privacidad y, luego pulsa Configuración.

En esta página, encontrarás un listado de pestañas importantes en la parte izquierda de tu pantalla:

En el apartado “**Seguridad e inicio de sesión**” puedes cambiar tu contraseña y activar las alertas y aprobaciones para proteger tu cuenta. Desde esta pestaña podrás ver la ubicación de las diversas sesiones iniciadas. Así pues, podrás controlar si alguien se ha conectado a tu cuenta sin que lo sepas. Así que si ves que un dispositivo que no conoces se ha conectado a tu cuenta puedes hacer clic en los tres puntos que se sitúan a la derecha del nombre del dispositivo sospechoso y seleccionar “no eres tú?” para retomar el control sobre tu dispositivo con total seguridad. (imagen 01)

En el apartado de “**Privacidad**” puedes decidir quién puede ver tu actividad, así como quién puede encontrarte y ponerse en contacto contigo. Si quieres hacer una modificación, solo tienes que:

1. Pinchar la palabra “editar”.
2. Seleccionar el pequeño triángulo que se encuentra a la derecha de la opción que está actualmente elegida, para poder ver todas las posibilidades que existen.
3. Hacer clic en la opción que te gusta más y luego pulsar la palabra “cerrar” (imagen 02)

Y cómo hacerlo con Instagram? Pues, el proceso es muy parecido, pero si te interesa ir un poco más lejos, puedes mirar este vídeo de la [Configura tu privacidad en Instagram](#) Agencia Española de Protección de Datos que te lo explica todo:

RECUERDA:

Si necesitas tomarte tu tiempo para asimilar la información que estás viendo en un vídeo, siempre puedes hacer clic en el icono de pausa, para pararlo. También puedes cambiar la velocidad al tocar el icono de ajustes en la parte inferior derecha, y luego hacer clic en la flecha a la derecha de “velocidad de reproducción”. Si quieres reducir la velocidad, puedes pinchar en el valor x0.75

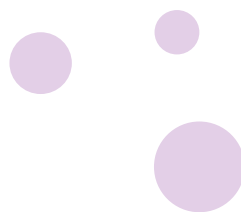
Whatsapp: una aplicación de mensajería instantánea

Whatsapp es una herramienta de comunicación que nos permite comunicarnos fácilmente con los demás, y que ofrece una alternativa interesante al teléfono sobre todo cuando se trata de llamar a familiares o amigos/os que viven lejos y, de hecho, ¡son cada vez más personas las que usan esta app tan completa! Pero en Whatsapp, como en cualquier otro sitio de internet, hay que tener cuidado con algunos puntos, porque aunque parezca ser un espacio más privado que otras redes sociales, sigue siendo una aplicación a través de la cual nuestros contactos pueden acceder a mucha información sobre nosotras.

Repasemos juntas los pasos importantes de la configuración de la privacidad y de la seguridad en Whatsapp:

Abre la aplicación y haz clic en los tres puntos verticales que se sitúan en la parte superior derecha de la pantalla.



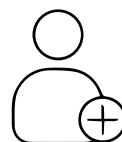


Pincha en **Ajustes** y luego en **Privacidad**.

Desde la pestaña que se abre, podrás configurar cada una de las opciones de privacidad que aparecen al hacer clic en ellas, y luego tocando en el botón de la opción que quieres elegir. Por ejemplo podrás modificar:

- a. Quién puede ver tu última conexión, “la hora de última vez”.
- b. Quién verá tu **foto de perfil y tus informaciones** de contacto.
- c. Quién te puede agregar a grupos,
- d. Si quieres activar tu ubicación en tiempo real.

4. Si ya no quieres que un contacto molesto pueda comunicarse contigo, puedes bloquearlo pinchando en la pestaña “Contactos bloqueados”.



Pulsa sobre el ícono en el lado superior derecho de la pantalla y luego selecciona en la lista el contacto que quieres bloquear. Si quieres bloquear un número que no está en tus contactos, abre la conversación con este contacto, pulsa en los tres puntos, desliza la página hacía arriba hasta que veas la palabra bloquear en rojo, en la cual puedes hacer clic.



Informaciones y cuentas falsas en las RRSS

1. ¿Cómo identificarlas y denunciarlas?

Las cuentas falsas son creadas por personas que se ocultan tras una identidad diferente de la propia, que son inventadas o robadas a otra persona. Esta estafa es una manera de ganarse nuestra confianza para proponernos servicios fraudulentos o extorsionarnos con datos personales.

Pero se puede identificar este tipo de perfiles falsos al mirar algunos elementos específicos de la cuenta como:

La foto de perfil y las publicaciones: Muchas veces las cuentas falsas tienen imágenes de poca calidad que parecen haber sido sacadas de Internet y/o que representan situaciones demasiado perfectas. También pueden parecerse a las personas cuyas identidades quieren suplantar: personas famosas, familiares o amistades tuyas, etc. En cuanto a las publicaciones, algunos elementos pueden alertarnos: a menudo se publican todas a la vez sin descripciones, para hacer que parezca auténtico, se refieren al mismo tema y/o son pocas y antiguas.

Información del perfil: Estas cuentas comparten muy poca información y tienen pocos seguidores o contactos.

El nombre de usuario: Suele ser muy parecido al nombre del usuario o de la entidad que quiere suplantar pero no es del todo igual, puede incluir un símbolo especial o letras y cifras intercaladas.

¿Qué puedo hacer cuando me encuentro ante una cuenta falsa?

Hay que tener mucho cuidado con los enlaces o los mensajes enviados por cuentas sospechosas. Nunca pinches en enlaces y tómate tu tiempo para analizar los mensajes que te escriben y los anuncios que puedas ver.

Si te das cuenta que es una cuenta falsa, puedes denunciarla al hacer clic en el símbolo de los tres puntos que está en su perfil. Este símbolo suele ser el mismo en la mayoría de las redes sociales y se encuentra cerca del nombre de usuario o de la foto del perfil.



2. ¿Qué son las fake news?

Del mismo modo que existen cuentas falsas en la red, circulan también muchas noticias falsas, o “fake news” que imitan el contenido periodístico y que difunden artículos, imágenes o vídeos que se hacen pasar por reales para crear polémica o sustraer datos personales.

¿Cómo puedo detectar el truco?

Confía en tu instinto. Si una noticia te parece sospechosa, léela por completo para tener una idea de su contenido y de la calidad de la redacción. Luego puedes comprobar algunos elementos porque los bulos no resisten un análisis prudente:

El título: una noticia verdadera siempre tendrá eco en varios medios de comunicación fiables.

La fecha de publicación: En Internet, es una práctica habitual descontextualizar noticias, muchas veces más antiguas, y hacerlas pasar por actuales.

La fuente: siempre que tengas una duda o que leas algo escrito por un medio que no conoces puedes investigar un poco escribiendo su nombre en el buscador.

Por internet también se propagan concursos promocionados, donde te informan de que has resultado ser la ganadora de un concurso al que no recuerdas haberte apuntado. Seguro que te suena, ¿verdad?. En este caso, recuerda los consejos que te damos al principio de esta guía sobre cómo hacer frente a las amenazas digitales.

Una herramienta que también te puede ayudar a identificar estos bulos es la página <https://maldita.es/malditobulo/>, en la que puedes mantenerte al tanto de las últimas noticias falsas que circulan por Internet.



Consideraciones para publicar en RRSS

Son tantas las opciones de divulgación en las RRSS, que a veces ni siquiera nos damos cuenta de la cantidad de informaciones que compartimos en las redes y que pueden ser vistas por otras personas. Así, aunque a la hora de registrarnos las redes sociales suelen pedir bastante información, recuerda que no te ves obligada a compartir datos personales. Evita publicar en tus perfiles todo tipo de datos personales cómo :

- Fecha de nacimiento completa.
- Ubicación actual.
- Correo electrónico o número de teléfono.
- Domicilio.
- Planes y vacaciones.
- Información sobre menores.

Además, todo lo que publiques en tus redes constituye tu “reputación digital”, que va de la mano con tu reputación personal, ya que ambas tienen efecto en la percepción que pueden tener de ti amigas/os, familiares o incluso empleadora/es etc. Por eso, ten cuidado porque como en nuestro día a día, las publicaciones inapropiadas y los comportamientos ofensivos con otros usuarios pueden comprometer tu responsabilidad personal.



Notas

VÍDEOS Y WEBGRAFÍA

VIDEOS

Agencia Española de Protección de Datos (AEPD). (2021, 2 de Marzo). *Configura tu privacidad en Instagram*. YouTube. <https://www.youtube.com/watch?v=hg460iqPG94>

KZguneaTIC. (s.f.). YouTube. <https://www.youtube.com/@KZguneaTIC>

Oficina de Seguridad del Internauta (OSI). (2020, 6 de Noviembre). *Antivirus. ¿Cómo nos protegen?* YouTube. <https://www.youtube.com/watch?v=f8FWKR7YUq0>

Vélez Martínez, C., & Instituto de Ingeniería de la Universidad Nacional Autónoma de México (IIUNAM). (2017, 18 de Mayo). *Ingeniería Social*. YouTube. <https://www.youtube.com/watch?v=pYdCJWa02j0>

WEBGRAFÍA

Agencia Española de Protección de Datos (AEPD), & Instituto Nacional de Ciberseguridad (INCIBE). (2018). *Guía de privacidad y seguridad en Internet*. Oficina de Seguridad del Internauta (OSI). <https://www.aepd.es/es/>

Aguilar, R. (2021, 6 de Marzo). *Cómo adaptar un teléfono para que lo usen los niños: configuraciones y apps recomendadas*. Xataka Móvil. <https://www.xatakamovil.com/tutoriales/como-adaptar-telefono-usen-ninos-configuraciones-apps-recomendadas>

Alcántara, B. (2021, 12 de Enero). *WhatsApp para mayores: guía de uso fácil y en imágenes*. Andro4all. <https://andro4all.com/whatsapp/guia-facil-uso-whatsapp-personas-mayores>

Asociación de Mujeres Opañel. (2022). *Publicaciones*. Click@ por Igual. <https://clickaporigual.es/publicaciones/>

Confederación Española de la Pequeña y Mediana Empresa (CEPYME). (2022, 4 de Abril). *Cómo identificar un perfil falso en redes sociales*. <https://cepymenews.es/como-identificar-perfil-falso-redes-sociales>

Fundación Cibervoluntarios. (2022, 21 de Enero). *Fake News: 7 pasos para detectar bulos en Internet*. <https://www.cibervoluntarios.org/es/news/post/fake-news-7-pasos-para-detectar-bulos-en-internet>

García, J. (2019, 7 de Diciembre). *Cómo adaptar un teléfono para que lo usen los niños: aplicaciones y configuraciones recomendadas*. Xataka. <https://www.xataka.com/moviles/como-adaptar-telefono-usen-ninos-aplicaciones-configuraciones-recomendadas>

Linares, I. (2022, 20 de Junio). *WhatsApp para el abuelo: cómo configurar WhatsApp para personas mayores*. Xataka Móvil. <https://www.xatakamovil.com/tutoriales/whatsapp-para-abuelo-como-configurar-whatsapp-para-personas-mayores>

VÍDEOS Y WEBGRAFÍA

Maldita. (s.f.). Maldito Buló - *Periodismo para que no te la cuelen*. <https://maldita.es/malditobulo/>

Meta Platforms Inc. (s.f.). *Controlar quiénes pueden ver lo que compartes en Facebook*. Facebook - Servicio de Ayuda. <https://www.facebook.com/help/393920637330807/>

Meta Platforms Inc. (s.f.). *Consejos de Seguridad*. Instagram - Servicio de Ayuda. https://es-la.facebook.com/help/instagram/377830165708421/?helpref=hc_fnav

Nieto, A. (2018, 9 de Febrero). *Siete trucos para que tu móvil sea apto para niños*. Xataka Android. <https://www.xatakandroid.com/tutoriales/siete-trucos-para-que-tu-movil-sea-pto-para-ninos>

Oficina de Seguridad del Internauta (OSI). (2019, 20 de Marzo). *Consideraciones a tener en cuenta al publicar en redes sociales*. <https://www.osi.es/es/actualidad/blog/2019/03/20/consideraciones-tener-en-cuenta-al-publicar-en-redes-sociales>

Oficina de Seguridad del Internauta (OSI). (2022, 2 de Marzo). *Cómo configurar y usar WhatsApp de forma segura*. <https://www.osi.es/es/actualidad/blog/2022/03/02/como-configurar-y-usar-whatsapp-de-forma-segura>

Oficina de Seguridad del Internauta (OSI), & Instituto Nacional de Ciberseguridad (INCIBE). (2019). *Guía para aprender a identificar fraudes online*. <https://www.incibe.es/ciudadania/formacion/guias/guia-para-aprender-identificar-fraudes-online>

Oficina de Seguridad del Internauta (OSI), & Instituto Nacional de Ciberseguridad (INCIBE). (2020). *Guía de ciberataques*. <https://www.incibe.es/sites/default/files/docs/guia-ciberataques/osi-guia-ciberataques.pdf>

Oficina de Seguridad del Internauta (OSI), & Instituto Nacional de Ciberseguridad (INCIBE). (2020). *Guía para configurar dispositivos móviles*. <https://www.incibe.es/ciudadania/formacion/guias/guia-para-configurar-dispositivos-moviles>

Oficina de Seguridad del Internauta (OSI), & Instituto Nacional de Ciberseguridad (INCIBE). (2022). *Guía de ciberseguridad. La ciberseguridad al alcance de todos* | Oficina de Seguridad del Internauta. <https://www.osi.es/es/guia-de-ciberseguridad-la-ciberseguridad-al-alcance-de-todos>

Organización de Consumidores y Usuarios (OCU). (2023, 13 de Enero). *Phishing: cómo evitarlo y prevenirlo*. <https://www.ocu.org/tecnologia/antivirus/consejos/evitar-ataque-phishing>