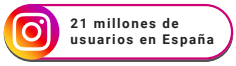
# SEGURIDAD EN LAS REDES SOCIALES

ADICAE CV
Asociación de Usuarios de Bancos, Cajas y Seguros

GENERALITAT VALENCIANA
Conselleria d'Economia Sostenible, Sectors Productius, Comerç i Treball







# INTRODUCCIÓN

Las redes sociales vinieron para quedarse. En la actualidad más de 37 millones de españolas y españoles tienen cuentas activas en las redes sociales y se conectan a ellas, al menos, una vez al mes. Cualquier internauta usa al menos una red social y la gran mayoría más de una. Además la pandemia y las medidas de confinamiento han motivado el crecimiento de un 27% de usuarios en redes sociales a lo largo de un año. Se les da muchos usos tanto en el ámbito personal como en el laboral, no hay duda de que las redes sociales aportan muchas ventajas, pero también implican riesgos e inconvenientes que desde ADICAE CV queremos visibilizar y combatir a través de esta guía.

Estas plataformas permiten a sus usuarias y usuarios estar en contacto con mucha facilidad, pero el precio es la publicación de información personal. A partir de su uso constante, los usuarios se exponen a múltiples amenazas informáticas que pueden robarles su identidad en la red, acceder a sus datos bancarios o estropear el dispositivo desde el cual están navegando.

**CONSEJOS GENERALES**

Es recomendable crear una cuenta de correo específica para registrar tus redes sociales, de esta forma tendrás otro correo diferente para asuntos personales, laborales y bancarios. Así mismo deberías tener precaución con los datos personales que aportas en el momento de registro como tu DNI, dirección, fecha de nacimiento o nombre completo.

## ÍNDICE

## EL MALWARE O "SOFTWARE MALICIOSO"

Se trata de un archivo que al infectar tu ordenador, tablet o teléfono tiene la capacidad de robar o secuestrar toda la información que guardas en el dispositivo, controlar el sistema, capturar tus contraseñas y las sesiones de plataformas que tienes activas y por supuesto puede deteriorar el rendimiento de tu dispositivo.

**EJEMPLOS**

Los malware se pueden encontrar camuflados en herramientas falsas, pero la forma más habitual es mediante el **envío de vídeos o mensajes masivos a través de perfiles falsos.** Estos mensajes pueden ser solo molestos spam, pero también pueden pretender que instales un complemento en tu navegador, que puede dañar o controlar tu dispositivo, o que inicies sesión en una página adjunta, exponiendo así tus datos personales.

Podemos recibir archivos adjuntos como un documento de texto que contenga malware y que al descargarlo infecte tu sistema. El mismo procedimiento podemos verlo mediante enlaces maliciosos o cupones de ofertas o descuentos que, aparte de ser cebos para llevarte a una página de publicidad engañosa, también pueden infectar tu dispositivo.

**¡CUIDADO!**
El Malware se propaga con mucha facilidad y a una velocidad de vértigo

Cuando la cuenta de tu red social es infectada los códigos maliciosos la aprovechan para continuar esparciéndose entre tus contactos. De esta manera cualquiera de tus contactos puede ver como le mandas un vídeo o un enlace. Siendo tu la persona que se lo envías ¿No va a abrirlo?

## ¿CÓMO PUEDO PREVENIR EL MALWARE?

**TEN AL DÍA LAS ACTUALIZACIONES DE TU SISTEMA OPERATIVO.**

**INSTALA UN PROGRAMA ANTIVIRUS Y UN CORTAFUEGOS ACTUAL Y EFICAZ.**

**¡SE PRUDENTE CUANDO UTILIZAS INTERNET!**

- Ten cuidado con los anuncios, banners o ventanas emergentes a los que accedes.
- No abras ningún archivo o enlace que provenga de una personas o empresa desconocida.
- Mucho cuidado con la información sobre tu cuenta bancaria.
- Instala programas y archivos que provengan de fuentes fiables.
- Guarda los datos más importantes usando copias de seguridad externas. Si tu ordenador se infecta y necesitas eliminar un malware tendrás que formatearlo.
- Evita los enlaces que contengan promociones o cualquier oferta dudosa.

## ESTAFAS DIGITALES

Sin duda alguna el método más exitoso es el Phising: Los ciberdelincuentes se hacen pasar por una entidad real y conocida y te invitan a acceder a un enlace, cuando accedes parece que estás en la página web real, sin embargo no lo es, se trata de una página cuya única función es captar tu nombre de usuario y contraseña.

**¡CUIDADO!**

El Phising permite a los ciberdelincuentes hacerse con el acceso de muchas cuentas de redes sociales, incluidas entidades financieras

## ¿CÓMO RECONOCER UN CORREO DE PHISHING?

- El mensaje no está personalizado, suele ir dirigido de forma genérica: "Estimado usuario/a" o "Querida amiga/o".
- Duda si ves **faltas de ortografía.**
- **Verás que hay diferencias entre el texto del enlace y la URL a la que apunta.** Si sitúas el ratón sobre el enlace podrás ver que el texto que aparece difiere con el enlace que parece a simple vista.
- **La URL no comienza con HTTPS.**
- **Adjunta documentos muy largos** que puedes identificar antes de abrirlos por el formato en el que están guardados. Por tanto desconfía de los archivos comprimidos tipo .ZIP ("nombre.doc.zip") o ejecutable tipo .exe.
- Pon atención a los argumentos que se usan suelen estar **redactados en tono alarmista** por lo que te incita a actuar ya, con extrema rapidez para solucionar el supuesto problema.

## ROBO DE IDENTIDAD

Diariamente usas las redes sociales y tanto tu como tus contactos compartís información personal aparentemente inocente, pero que puede ser muy útil para los atacantes que buscan hacer un robo de identidad, uno de los delitos informáticos que más ha crecido estos últimos años. Una vez acceden a tu perfil es muy fácil conseguir la información necesaria para crearse un perfil falso similar al tuyo, con tus fotos, tu nombre y demás datos personales. Estas cuentas falsas se usan con fines fraudulentos, es habitual, por ejemplo:

Suelen pedir dinero a tus contactos fingiendo que eres tu y que te encuentras en una situación límite, por lo que necesitas un ingreso con urgencia.

Suelen adueñarse de una cuenta para emitir mensajes falsos y/o insultantes hacia otros miembros de la red sin que la persona propietaria de la cuenta pueda recuperar el control de la misma hasta que contacta con la Red Social y esta decide intervenir.

Hay dos mecanismos cruciales para la creación de un perfil social similar al tuyo:

**SE ACERCAN A TI DE FORMA PERSONAL**

Los ciberdelincuentes buscan tener un contacto directo contigo para extraer la información que necesitan a través de vuestra "amistad" o cualquier comunicación que permita la red social.

**INFORMACIÓN PÚBLICA**

La configuración de las redes sociales puede facilitar que tus datos personales sean visibles para cualquier persona con una cuenta en la red social. Los cibercriminales buscan este tipo de perfiles por su fácil accesibilidad.

**¡CONTACTA CON ADICAE CV!**

Si te han suplantado la identidad en alguna de tus redes sociales podemos ayudarte.


## ¿QUÉ HAGO SI DESCUBRO QUE HAN SUPLANTADO MI IDENTIDAD EN LAS REDES SOCIALES?

**1. Documenta todo lo ocurrido.**
Recaba copias de correos o mensajes con capturas de pantalla.

**2. Revisa todas tus cuentas** para averiguar cuales han sido afectadas.

**3. Alerta a tus contactos.**
Contacta con tus familiares y amistades para avisarles de lo ocurrido y evitar que terminen siendo víctimas de otro fraude, es aconsejable que hagas una publicación oficial en tus redes sociales para que todo el mundo se entere, aunque les escribas de forma individual.

**4. Recupera tus cuentas** en el caso de que te hayan robado las claves de acceso y cambia las contraseñas de aquellas a las que puedes acceder.

# MALAS PRÁCTICAS EN LAS REDES SOCIALES

| | |
|---|---|
| **GROOMING:** | Formas delictivas de acoso a través de la red. Se trata de un adulto que se pone en contacto con un niño, niña o adolescente con la intención de ir ganándose poco a poco su confianza y luego involucrarle en una actividad sexual. |
| **CYBERBULLING O CIBERACOSO:** | Se da cuando al hacer uso de los medios digitales (teléfonos, internet, videojuegos online…) se insulta, acosa o persigue a otra persona. |
| **SEXTING:** | Consiste en enviar mensajes, fotos o vídeos eróticos o sexuales mediante aplicaciones o redes sociales. Normalmente se realiza de manera íntima no obstante es habitual que estos contenidos acaben siendo virales especialmente si las imágenes son de mujeres. |

**ADICAE CV te aconseja de forma general…**

—A la hora de elegir tu **CONTRASEÑA**

➡ **No repitas contraseñas, tener una o dos para todo es tan sencillo como peligroso.**

➡ **Evita poner tu nombre, el de tu mascota preferida, fecha de nacimiento o cualquier dato personal evidente.**

➡ **Intenta no usar ordenadores públicos para ingresar en tus redes sociales y si no tienes más remedio ¡CIERRA SESIÓN SIEMPRE!**

—Piensa dos veces antes de descargarte cualquier contenido ¡Puede ser una Trampa!

—Configura un segundo factor de autentificación

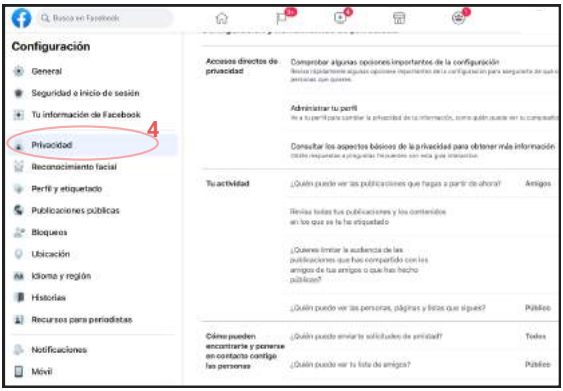
—Mantén tus cuentas personales privadas

# ¿CÓMO PUEDO CONFIGURAR MI PERFIL PARA AUMENTAR MI SEGURIDAD?

## FACEBOOK


**1-** Pincha en la foto de perfil que te aparece en la esquina superior derecha.

**2-** Ve a **configuración**.


**3- "Seguridad e Inicio de sesión"**

—En "Configurar seguridad adicional" Activa las alertas sobre "inicios de sesión no reconocidos". Así si alguien accede con tu clave lo sabrás.

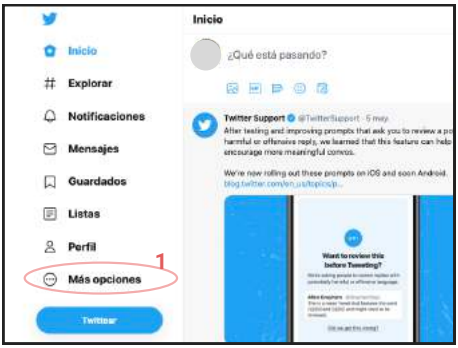
**4-** Pincha en la pestaña de "Privacidad" y elige

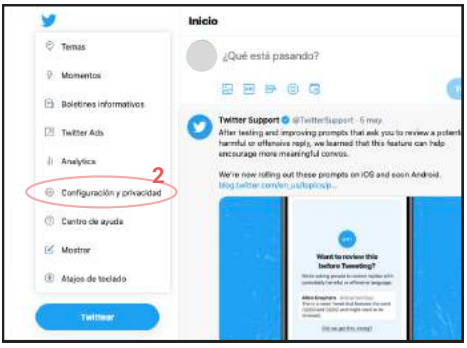
—**Quien puede ver tus comentarios y publicaciones.** Selecciona "solo yo". Así Podrás revisar cada post antes de que des permiso a tu amistades para verlo.

—**Quien puede ponerse en contacto contigo:** Es más seguro reducir el contacto a personas conocidas.

—**Quién puede buscarte:** Evita que los motores de búsqueda alcancen tu perfil, así las fotos que publicas no aparecerán al poner tu nombre en Google.

# TWITTER

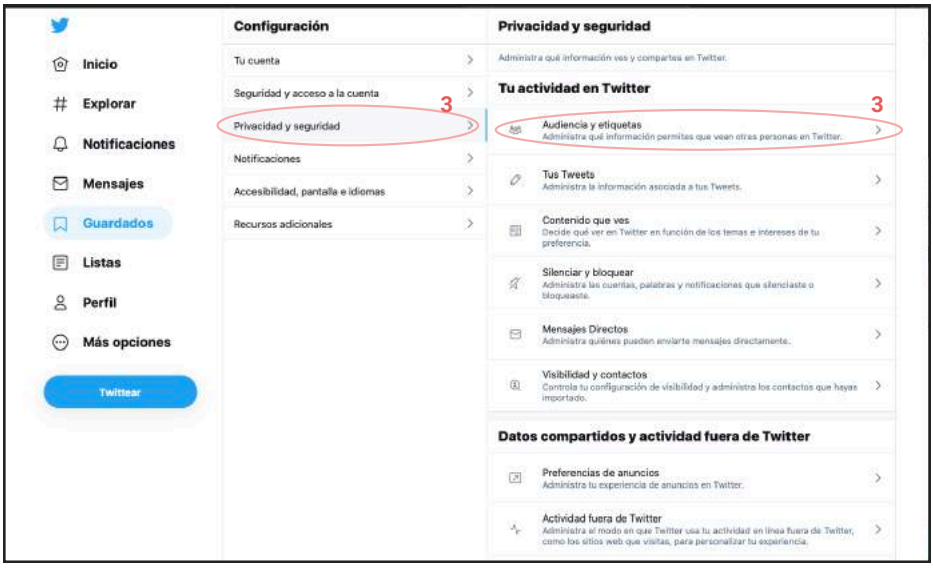



**1-** Una vez dentro de tu cuenta haz click en **"más opciones"**

**2-** Ve a **"Configuración y**

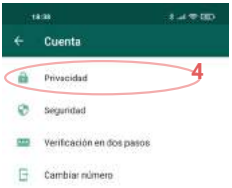
**3-** Pincha en **"Privacidad y seguridad"**
—En "Audiencia y etiquetas" selecciona "proteger tus tweets" para que solo tus amistades puedan leerte
—Puedes decidir que nadie te etiqueten en su foto.
—Desactivar la pestaña "añadir ubicación" nadie tiene la necesidad de saber donde estás en cada momento.



## WHATSAPP

La nueva política de WhatsApp implica que de forma automática todas las personas usuarias tienen los grupos configurados de forma que personas que no conoces te puedan incluir en grupos de chats de apuestas, grupos dudosos, usureros, grupos de fraude financiero, etc. Para evitarlo debes alterar tu configuración:






**1** Ve a WhatsApp
**2** Ajustes

**3** Cuenta

**4** Privacidad



**5** Grupos y cambia de “todos” a “mis contactos”

**¡CUIDADO!**

¡Alerta a tus contactos y amigos!
¡Si tienes dudas contacta con ADICAE CV!

**Infórmate y participa para ser un consumidor crítico, responsable y solidario con Adicae CV. Únete a la fuerza colectiva de los consumidores y consumidoras.**

## NUESTRAS REDES SOCIALES

@ADICAE AdicaeConsumidores user/ADICAE1

## NUESTRA PÁGINA WEB

comunidadvalenciana.adicae.net

## VEN A NUESTRAS SEDES EN:

**VALENCIA**
C/ Navarra 9, bajo
46008 . Valencia (Zona Abastos, metro Ángel Guimerá)
963 540 101

**ALICANTE**
C/ Arquitecto Guardiola, 15, Entresuelo A.
03007 - Alicante (Barrio Benalúa)
965 286 538

## CONTACTA CON ADICAE COMUNIDAD VALENCIANA:

coordinacionvalencia@adicae.net
963540101

ADICAE CV
Asociación de Usuarios de Bancos, Cajas y Seguros

GENERALITAT VALENCIANA
Conselleria d'Economia Sostenible, Sectors Productius, Comerç i Treball