

# LA SUPLANTACIÓN DE IDENTIDAD Y EL ROBO DE CUENTAS

La **suplantación de identidad** es hacerse pasar por otra persona para obtener un beneficio económico, información privada, o para dañar a alguien con insultos, burlas, chantajes o amenazas.



## Se puede dar por parte de **ciberdelincuentes**:

- Robando una cuenta con mensajes de **phishing**, virus, **malware** y otros engaños para **conseguir dinero con los datos de pago almacenados**, pedir un rescate, chantajear amenazando con difundir información privada, o acceder a otras cuentas.
- Creando un **perfil falso para difundir malware y fraudes**, o acercarse a un/a menor para pedir fotos y vídeos íntimos e información personal, y luego venderlos, chantajearle o tratar de abusar sexualmente de él/ella.

## Pero también entre **niños/as y adolescentes**:

- Para **burlarse de un compañero/a**, como arma para el ciberacoso, para difundir información privada sin consentimiento.
- **Robando su contraseña**, o entrando en una sesión iniciada en un descuido, o creando un perfil falso con sus datos.



## ¡SIGUE ESTAS PAUTAS PARA EVITAR ENGAÑOS!

### USA MEDIDAS DE SEGURIDAD



1

Configura un **desbloqueo seguro** en tus dispositivos, y evita que puedan ver tu contraseña cuando la escribes.



Usa **contraseñas seguras** y diferentes en cada videojuego, red social, etc. Puedes usar un **gestor de contraseñas** para tener que recordar una única contraseña maestra.

2

3

Configura el **doble factor de autenticación** (así será necesario introducir un código de verificación además del usuario y la contraseña).



En un **dispositivo compartido** navega en modo privado o de incógnito, no dejes que guarde contraseñas o que deje la sesión abierta, cierra sesión siempre y borra los datos de navegación.

4

5

Mantén tu **dispositivo actualizado y seguro** (sistema operativo, aplicaciones y antivirus).



**Desconfía de enlaces y archivos adjuntos**, también a través de chats de videojuegos y redes sociales. Analízalos con un **antivirus online**.

6



### CUIDA TU INFORMACIÓN PERSONAL

Piensa antes de publicar, cualquiera podría verlo en Internet. **Evita compartir:**

- Información privada, sensible, fotos íntimas.
- Datos personales, número de teléfono, correo electrónico.
- El lugar donde estás, vives, estudias, juegas.
- Datos o fotos de otras personas.

- Usa las **opciones de privacidad de la cuenta**. Limita quién puede mencionarte, etiquetarte y ver tus publicaciones.
- **Acepta como amigos solo a contactos conocidos previamente** y confirma su solicitud en persona.
- **Di no** ante peticiones o exigencias de información personal (rechaza pruebas de confianza, desconfía de sorteos o regalos).
- **Activa alertas en los buscadores con tu nombre a modo de egosurfing.**

Buscar nuestro nombre en Internet para detectar posibles suplantaciones, comentarios o información relacionada.

## CÓMO ACTUAR FRENTE A UNA SUPLANTACIÓN

### SI **ROBAN** TU CUENTA

### SI **ENCUENTRAS UN PERFIL FALSO**

Puedes buscar más información en la ayuda o el centro de seguridad.

1 **Reporta** el perfil, y los contenidos tuyos que muestre, a la plataforma.

- 1 Usa las **opciones de recuperación de contraseña**.
- 2 **Cambia la contraseña** de la cuenta, y de otras cuentas vinculadas, o con contraseñas similares.
- 3 Activa el **doble factor de autenticación**.
- 4 Analiza los dispositivos con un **antivirus** (por si accedieron con algún virus o *malware*).

- 2 Si difunde mensajes, fotos, vídeos privados, íntimos o violentos hacia un/a menor, **solicita su retirada** mediante el Canal Prioritario de la AEPD (<https://www.aepd.es/es/canalprioritario>).
- 3 Trata de **informar a la persona suplantada**.
- 4 Si la persona detrás del perfil falso es otro/a menor, infórmale de que es algo **ilegal**, pide que lo elimine.



Puedes apoyarte en tu familia y solicitar asesoramiento y mediación al centro educativo.



### SI TE ENCUENTRAS CON UNA DE ESTAS **SITUACIONES**

- 1 **Entran en tu cuenta sin tu consentimiento.**
- 2 **Están usando tu nombre y/o fotos en Internet.**
- 3 **Se hacen pasar por un/a amigo/a.**
- 4 **Te han engañado haciéndose pasar por otra persona.**

## ¡PIDE AYUDA!



Habla con tu familia o profesores/as. Podéis llamar de forma gratuita y confidencial al **017**, la **Línea de Ayuda en Ciberseguridad de INCIBE**.

- Teléfono 017
- WhatsApp 900 116 117
- Telegram @INCIBE017
- Formulario web



TU AYUDA EN CIBERSEGURIDAD **365 días**  
 Recuerda que tu consulta se realizará de forma anónima. De 8.00 a 23.00h  
 Más información en [www.incibe.es/menores](http://www.incibe.es/menores)