GUÍA **SUPLANTACIÓN DE IDENTIDAD EN EL ÁMBITO DEL MENOR**

Aprende a proteger tu privacidad en línea

Financiado por la Unión Europea
NextGenerationEU

GOBIERNO DE ESPAÑA
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

Plan de Recuperación, Transformación y Resiliencia

España | digital 2026

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

is4k INTERNET SEGURA FORKiDS

Índice

LICENCIA
DE CONTENIDOS

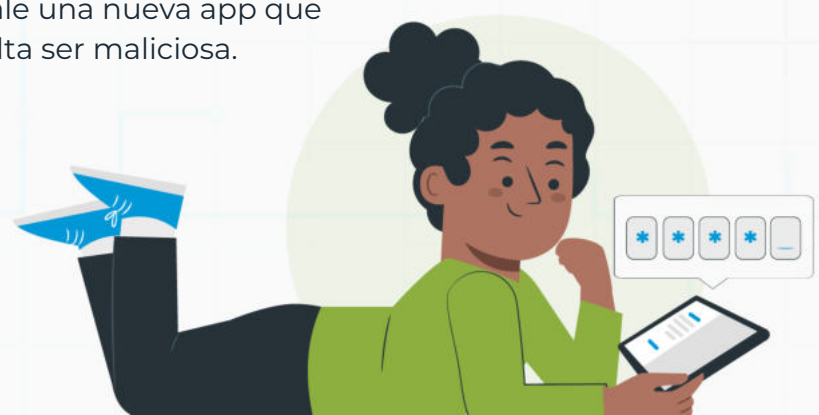
1. ¿Qué es la suplantación?
Robo de cuentas y perfiles falsos

La suplantación de identidad en Internet ocurre cuando un usuario se hace pasar por otra persona, de manera malintencionada, en su propio beneficio o para dañar a alguien, por ejemplo, robando dinero o información personal, con insultos, burlas, chantajes o amenazas.

Tipos de suplantación de identidad

1 Robo de cuentas

Se produce cuando una persona se hace pasar por otra al conseguir entrar en su cuenta.
Puede ocurrir entre menores cuando uno/a se deja la sesión abierta en el aula, si comparte su contraseña, si es muy fácil de adivinar o si la tiene escrita en un papel.
También cuando un ciberdelincuente emplea técnicas de ingeniería social o un *malware* para robar su contraseña, por ejemplo, con un mensaje fraudulento donde se le pide que haga clic en un enlace para recuperar su cuenta, para obtener un regalo virtual, llevándole a una web de *phishing*, o se instale una nueva app que resulta ser maliciosa.



2 Perfiles falsos

Cuando una persona crea un perfil falso en redes sociales usando información como el nombre y apellidos, número de teléfono, alguna foto de un/a menor, fingiendo ser él o ella para dañarle, o para engañar y dañar a otras personas.

2. ¿Quién y por qué realiza una suplantación?

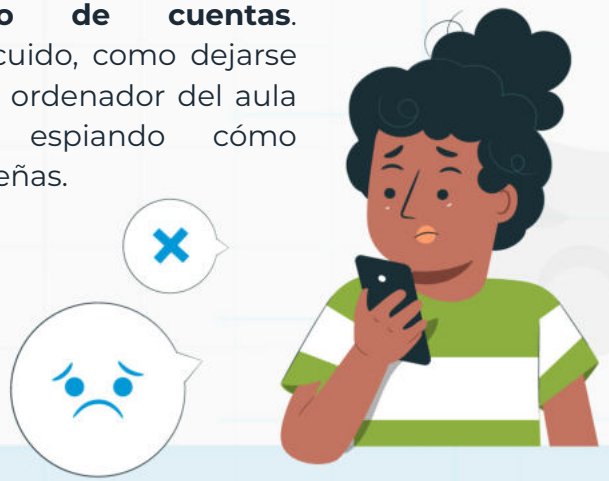
En ocasiones, la suplantación de identidad puede producirse entre iguales, como sería entre menores o a través de ciberdelincuentes.

1 Ciberdelincuentes

- **Objetivo económico.** Accediendo a los métodos de pago guardados en las cuentas online, o explotando la información del usuario.
- **Técnicas de ingeniería social y *malware*** para acceder a cuentas ajenas y obtener información personal.
- **Hacerse pasar por un/a menor** para mejorar sus engaños hacia otras personas.
- **Difusión de fraudes y *malware*** mediante cuentas robadas y perfiles falsos.
- ***Grooming***. Haciéndose pasar por alguien atractivo/a, ganarse la confianza de un/a menor, y chantajearle con fines sexuales.

2 Menores

- **Ciberacoso y otras situaciones de violencia online**. Robando cuentas o creando perfiles falsos para acosar a otros/as menores en línea.
- **Difusión de contenidos privados** tras acceder a la cuenta de un/a menor, con el objetivo de hacerle daño.
- **Técnicas de robo de cuentas**. Aprovechando un descuido, como dejarse la sesión iniciada en el ordenador del aula de informática, o espiando cómo introducen sus contraseñas.



Es necesario que los/as menores sean conscientes de que cualquier información personal, datos o fotos que compartan en Internet puede hacerse pública, quedando en manos de cualquier persona, por lo que también la podrían utilizar para crear un perfil falso con el que suplantar su identidad.

3. En situación

1 Las amistades de Mariona están enfadadas con ella por los insultos que han recibido desde su cuenta en una conocida red social, y ella lo niega. En realidad, ella inició sesión en la red social en el aula de ordenadores del instituto, y no se dio cuenta de que dejó que recordara su contraseña. Vino otra persona más tarde y entró en su cuenta.

- **No recordar contraseñas en dispositivos de uso compartido.**
- **Acordarse siempre de cerrar sesión.**

2 Alex ha recibido un correo de su red social, aparentemente, alertándole de que su cuenta está en riesgo. Ha hecho clic en el enlace, y ha introducido su usuario y contraseña en la que parecía ser la página de inicio de sesión. Sin embargo, el correo era falso y el enlace llevaba a una página de *phishing*. Han cambiado su contraseña, y ya no puede entrar.

- **Comprobar a dónde lleva un enlace antes de hacer clic.**
- **Asegurarse de que la dirección es del dominio oficial.**
- **Pasar los enlaces por un analizador online**

3 Ana ha recibido una solicitud de amistad de un chico muy atractivo. Parece que tienen algún amigo/a en común, aunque él tiene pocos seguidores. Después de chatear un tiempo, y compartir alguna confidencia, él empieza con exigencias, chantajes y amenazas. En realidad, no era quien decía ser, había sacado las fotos de otro perfil en redes sociales.

- **Desconfiar de solicitudes de amistad de quien no conoces en persona.**
- **No compartir confidencias ni fotos privadas con amistades online.**

4 Eric lo está pasando mal, alguien de clase ha creado un perfil con su nombre y se dedica a compartir fotos suyas retocadas de manera humillante, y comentarios ofensivos.

- **Limitar la exposición online, compartir con sentido común.**
- **Utilizar las opciones de bloquear y reportar comentarios o perfiles.**

4. ¿Cómo puede afectar la suplantación de identidad?

La suplantación de identidad puede tener graves consecuencias no solo para la víctima, sino también para quien finge ser quien no es mediante el robo de cuentas o la creación de perfiles falsos.

1 Para la víctima

- **Pérdidas económicas**
  Al acceder a sus medios de pago.
- **Daño a la reputación**
  Cuando se publica contenido falso o humillante, información privada sin consentimiento o contenido inapropiado en su nombre.
- **Ciberacoso**
  Utilizando su identidad o la de otro/a menor para insultar, humillar y herir a otra persona.
- ***Grooming***
  Al ganarse su confianza para exigir el envío de contenido íntimo.
- **Pérdida de privacidad**
  Con el acceso a información personal, como fotos o mensajes privados en su cuenta, o con la exposición pública de fotos o información personal en un perfil falso.

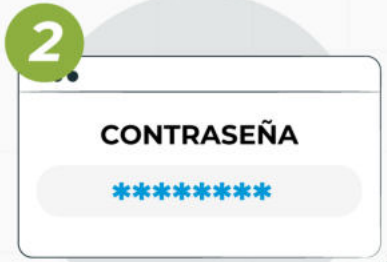
2 Para quien suplanta su identidad

Puede tener consecuencias legales relacionadas con varios delitos, como el uso de imagen para crear un perfil falso, descubrimiento y revelación de secretos, estafa.

5. PREVENCIÓN:
Proteger las cuentas frente al robo

Proteger el dispositivo con un método de desbloqueo seguro (contraseña, pin o patrón complejos, biometría).

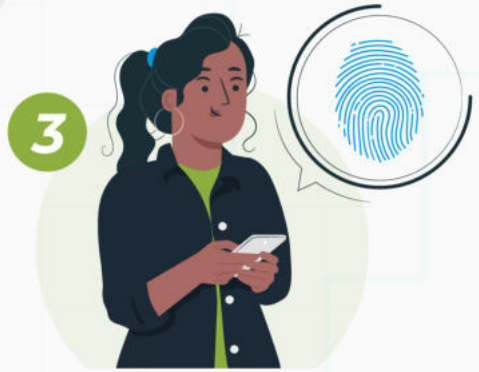
Vigila siempre tu dispositivo, no lo dejes en espacios públicos.



Utilizar contraseñas robustas, largas y únicas para cada cuenta.

Configura unas opciones de recuperación de contraseñas seguras.

Para recordarlas más fácilmente puedes usar un gestor de contraseñas.



Activar el doble factor de autenticación con la intención de añadir una capa extra de seguridad a las cuentas.

Puedes navegar en modo incógnito, o borrar los datos de navegación.

En equipos compartidos, no recordar sesiones, ni contraseñas, y acordarse de cerrar sesión de todas las cuentas una vez se finalice con él.

Descarga solo aplicaciones fiables y de tiendas oficiales.

Puedes ver antivirus y *cleaners*

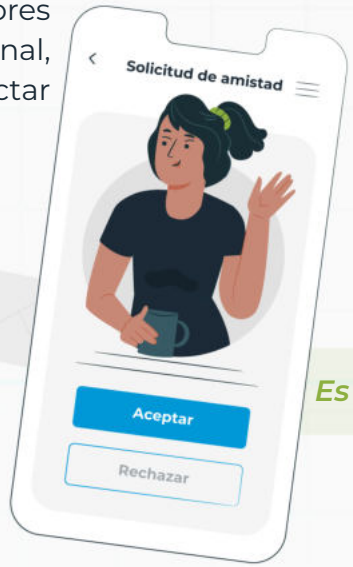
Mantener actualizado el sistema y aplicaciones del dispositivo, incluido el antivirus.

Puedes ver analizadores de URL y archivos

Desconfiar de mensajes de chats, redes sociales o correos electrónicos que contengan enlaces o archivos adjuntos. Antes de hacer clic o descargarlos es recomendable analizarlos con un antivirus.

6. PREVENCIÓN:
Reducir la exposición frente a perfiles falsos

- **Concienciar** sobre la importancia de publicar contenido con responsabilidad y pensamiento crítico, cuidando su privacidad e identidad digital.
- **Establecer** la cuenta privada en redes sociales, y revisar las configuraciones de privacidad (evitar que personas desconocidas puedan ver tus movimientos, te etiqueten, etc.).
- **Aceptar** solicitudes de amistad solo de quien conozcas previamente en persona.
- **Rechazar** peticiones o exigencias de información confidencial, ni por insistencia, ni como prueba de amistad o confianza.
- **Activar** alertas en buscadores sobre información personal, como el nombre, para detectar posibles suplantaciones.



¿Cómo identificar perfiles falsos en redes sociales?

Desconfiar:

1. De **perfiles con poco contenido**, o sospechoso (por ejemplo, si únicamente publica promociones).
2. Si la **forma de hablar** no coincide con su perfil (por ejemplo, con vocabulario adulto).
3. Ante una **insistencia** en pedir información personal, fotos o vídeos.
4. Si **coincide sospechosamente** en gustos e intereses.

Es recomendable contrastar las solicitudes de amistad en persona, antes de aceptarlas.

7. Reacción ante un robo de cuenta, o ante un perfil falso.

1 Robo de cuentas

Si se detecta un inicio de sesión no autorizado o inusual, o no puede entrar en su cuenta, o en su perfil se están publicando contenidos, enviando mensajes, agregando contactos sin su permiso:

- **Emplear** los mecanismos de recuperación de cuenta (he olvidado mi contraseña, no puedo acceder a mi cuenta).

Puedes informarte en la ayuda o el centro de seguridad de cada aplicación o red social.

- **Cambiar la contraseña de la cuenta.** También las contraseñas de las cuentas vinculadas (por ejemplo, con el mismo correo electrónico), o las de las cuentas que tengan una contraseña similar.
- **Establecer** medidas de seguridad adicionales como sería el doble factor de autenticación.
- **Rechazar** peticiones o exigencias de información confidencial, ni por insistencia, ni como prueba de amistad o confianza.
- **Analizar y limpiar** los dispositivos con un antivirus, por si se hubiera producido el robo mediante un *malware*.

En caso de necesitar presentar una denuncia, conviene recopilar las pruebas y certificarlas mediante un servicio de testigo online.

Más información sobre testigos online

2 Perfil falso:

Si se sospecha que un perfil es falso, por utilizar nuestra información, o suplantar a otra persona o entidad:

- **Reportarlo** a la plataforma y solicitar su retirada.

Más información sobre cómo reportar

- Si se ha difundido información comprometida, íntima o violenta de o hacia una persona menor de edad, **solicitar su retirada** mediante el **Canal Prioritario de la AEPD**.
- **Informar** a la persona suplantada.
- Si el perfil falso lo ha creado un niño/a o adolescente, **informarle de que se trata de algo ilegal y pedirle que lo retire**.

Recuerda que siempre puedes acudir a Tu Ayuda en Ciberseguridad, llamando al 017, donde te guiaremos y asesoraremos sobre cualquier tema relacionado con la suplantación de identidad.

TU AYUDA EN CIBERSEGURIDAD 017

GUÍA SUPLANTACIÓN DE IDENTIDAD EN EL ÁMBITO DEL MENOR

Teléfono
017

WhatsApp
900 116 117

Telegram
@INCIBE017

Más información en **www.incibe.es/menores**

Financiado por la Unión Europea
NextGenerationEU

GOBIERNO DE ESPAÑA
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

Plan de Recuperación, Transformación y Resiliencia

España | digital 2026

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

is4k INTERNET SEGURA FORKiDS