2.3 Pautas y recomendaciones

PAUTAS Y RECOMENDACIONES PARA FAMILIAS Y EDUCADORES (OSI)

A continuación presentamos una serie de medidas que podemos realizar en caso de detectar una suplantación de identidad en nuestros menores.

- En caso de detectar que alguien se hace pasar por un menor, creando una cuenta similar a la suya, tenemos derecho a denunciarlo ante la misma web del servicio, notificando esta situación a la red social o sistema implicado para solicitarles que tomen las medidas necesarias para restaurar el nivel de seguridad anterior a la suplantación de identidad.
- Es importante saber que si nos encontramos ante un caso de usurpación de identidad, si el incidente no se considera muy grave se recomienda proceder a su denuncia en el correspondiente servicio contactando con los responsables y/o administradores de las redes sociales o sitios web. La mayoría de ellos ponen a nuestra disposición mecanismos de denuncia de este tipo de situaciones. El segundo paso, si tras denunciar los hechos al servicio la problemática no se soluciona, sería interponer una denuncia ante las propias las autoridades, como son las Fuerzas y Cuerpos de Seguridad del Estado.
- En caso de denuncia, es necesario recopilar todas las pruebas y evidencias relacionadas con la suplantación de identidad producida en el menor, como capturas de pantalla, copias de correos, copias de ficheros, etc.
- Denunciar el caso a la agencia de protección de datos.
- Como medida de seguridad, sería conveniente cambiar todas las contraseñas que piense le hayan podido interceptar.

En caso de requerir denunciar un caso de suplantación de identidad en menores ante los cuerpos de seguridad del estado, debemos conocer los siguientes grupos especializados:

- **Policía Nacional (Brigada de Investigación Tecnológica)** http://www.policia.es/bit. delitos.tecnologicos@policia.es

Copyright 2026

- **Guardia Civil (Grupo de Delitos Telemáticos)**
  https://www.gdt.guardiacivil.es/webgdt/home_alerta.php. Teléfono: 900.101.062

Desde el ámbito familiar tenemos que concienciar a los menores sobre la importancia de limitar la difusión voluntaria de datos personales y privados en redes sociales configurando de forma correcta las opciones de privacidad de las diferentes redes sociales que utilicen, pero también manteniendo los equipos seguros con las actualizaciones de software oportunas. Además la familia debe fomentar entre sus hijos la discreción a la hora de publicar fotografías o comentarios en la red.

De acuerdo con la **Oficina de Seguridad del Internauta (OSI)** para usar el ordenador de una manera organizada y segura se recomienda crear una cuenta por cada usuario que vaya a utilizar el ordenador. De esta forma, cada usuario podrá tener su propio escritorio, con una configuración y preferencias personalizadas. Se recomienda además:

- Bloquear las ventanas emergentes.
- Hacer uso de filtros antispam ya que filtran el correo electrónico que consideran basura a una carpeta donde lo almacenan.
- Es importante no utilizar la misma contraseña para varios servicios, deben ser secretas, robustas y modificadas periódicamente.
- Debemos tener precaución frente a enlaces sospechosos, las descargas que realizamos, desconfiar de correos de desconocidos, sobre todo con ficheros sospechosos.
- Tener precauciones al utilizar ordenadores públicos y conectarse a redes WiFi públicas, como tener instalado y habilitado un cortafuego, así como personalizar la configuración de red de nuestro equipo.
- Establecer una contraseña para el bloqueo de la pantalla del teléfono además de los propios números de seguridad PIN y PUK para el acceso a la tarjeta SIM del mismo como medida de prevención ante un posible robo o pérdida de dispositivos móviles.

> El país: Han suplantado mi identidad en Internet o en redes sociales ¿qué hago?
>
> http://economia.elpais.com/economia/2016/04/29/actualidad/1461949659_081309.html

Revision #1
Created 2022-02-01 12:07:28 CET by Equipo CATEDU
Updated 2022-02-01 12:07:28 CET by Equipo CATEDU

Copyright 2026