2. Suplantación de identidad

- 2.1 Definición y conceptos
- 2.2 Datos y ejemplos
- 2.3 Pautas y recomendaciones

Copyright 2026

2.1 Definición y conceptos

DEFINICIÓN Y CONCEPTOS

La “**Suplantación de Identidad**” en general consiste en el uso de información personal para hacerse pasar por otra persona con el fin de obtener un beneficio propio. Normalmente este beneficio genera un perjuicio a la persona que sufre dicha suplantación de identidad. En el caso de menores, es un riesgo cada vez más frecuente que se produce cuando una persona malintencionada actúa en nombre del menor haciéndose pasar por él mediante la utilización de diversas técnicas.

Hay que diferenciar entre dos conceptos:

- **Suplantación de identidad**. La suplantación de identidad consiste en la apropiación de derechos y facultades propias de la persona suplantada (por ejemplo, acceder a la cuenta de una red social).
- **Usurpación de la identidad**. La usurpación de identidad consiste en que una vez suplantada la identidad se empiece a interactuar como si realmente fuera propietario de esos derechos y facultades (por ejemplo, realizar comentarios o subir fotografías).

Ejemplos de suplantación de identidad:

- Registrar un perfil en una red social con el nombre de otra persona sin su consentimiento y utilizando datos o imágenes de la víctima, sería una suplantación de identidad y en principio se consideraría delito.
- Si únicamente se registra un perfil falso por medio del nombre/alias y no se utiliza información o imágenes personales de la persona suplantada, no se consideraría delito. Para considerarse delito la apropiación no se debe limitar al nombre, sino a todas las características o datos que integran la identidad de la persona.
- Acceder sin consentimiento a una cuenta ajena para tener acceso a la información allí almacenada. Sería una suplantación de identidad y en principio se consideraría delito (al menos un delito de descubrimiento y revelación de secretos).
- Acceder sin consentimiento a una cuenta ajena utilizando los datos personales y haciéndose pasar por el suplantado (por ejemplo, realizando comentarios o subiendo fotografías). Sería una usurpación de identidad y se consideraría delito
- Publicación sin consentimiento de anuncios o comentarios utilizando el nombre de un tercero o incluso utilizando sus datos personales para identificarse con terceras personas

Copyright 2026

a través, por ejemplo, de correo o mensajería instantánea (Whatsapp). Sería una usurpación de identidad y se consideraría delito.

Ejemplos de suplantación de identidad entre menores.

- Entrar sin consentimiento.
- Acceder a información sensible como puede ser el caso de una foto o un vídeo.
- Acosar o desprestigiar a la otra persona (casos de ciberbullying), por ejemplo, publicando comentarios polémicos o denigrantes que serán vistos por terceros.
- Ganarse la amistad de un menor con el fin de cometer un abuso sexual (casos de grooming donde el acosador utiliza la usurpación de identidad para acceder a cuentas que sirvan de “puente” para facilitar el contacto con la víctima).
- ***Hacerse pasar por otra persona.*** Crear una cuenta para hacerse pasar por otra persona. Aunque esta forma se suele dar en menores, es uno de los casos más frecuentemente utilizados para suplantar a gente famosa.

Técnicas más utilizadas para la suplantación de identidad

Las técnicas utilizadas para la suplantación de identidad tienen que ver con el concepto de **ingeniería social**, que se refiere al uso que hacen los ciberdelicuentes de la manipulación psicológica sobre las personas para conseguir sus fines, teniendo en cuenta la tendencia general de éstas a la confianza. Método basado en la persuasión y muy eficaz en el caso de los menores de edad que, debido tanto a su falta de experiencia y conocimientos relacionados con este tema como con su confianza e inocencia, son considerados especialmente vulnerables. Normalmente el motivo que impulsa a los adolescentes para la realización de suplantación de identidad es, habitualmente, la mera diversión. Las más utilizadas son el **Phishing , el Pharming y el SMiShing**.

Phishing. Es un término informático utilizado para denominar el fraude por suplantación de identidad, una técnica de ingeniería social. El término phishing procede de la palabra inglesa fishing (pesca) haciendo alusión a “picar el anzuelo”. Lo que significa que no aprovecha una vulnerabilidad en los ordenadores sino un "fallo humano" al engañar a los usuarios de Internet con un correo electrónico que aparentemente proviene de una empresa fiable, comúnmente de una página Web bancaria o corporativa.

Dado el cada vez más creciente número de denuncias de incidentes relacionados con el phishing en el contexto de los menores de edad, se hace necesaria la creación y utilización de métodos adicionales de protección dirigidos a los menores.

En menores de edad, uno de los servicios más utilizados por los hackers suplantar la identidad de los mismos son las redes sociales. Suelen emplear una serie de excusas para engañar al usuario tales como enviar un mensaje privado en el que le recomiendan cambiar la contraseña. En otras ocasiones crean sitios web falsos para que cuando se introduzca el correo electrónico y la

Copyright 2026

contraseña se grabe y conserve esta información.

Ejemplo de Phishing en Facebook.



Finalmente, encontramos casos de phishing a menores a través de juegos online. El objetivo sigue siendo apropiarse de cuentas, datos privados, bancarios y suplantar la identidad de los usuarios. Normalmente, la excusa que suelen emplear para engañar a los menores se encuentra relacionada con fallos de seguridad en la plataforma del juego o en la cuenta de los usuarios.

Pharming. Es una modalidad más peligrosa de phishing, por medio de la cual el ciberdelincuente infecta el ordenador del usuario de forma que se acaba redireccionando el tráfico web de una página legítima, utilizada habitualmente por el usuario, hacia otra página falsa creada por el ciberatacante.

La diferencia principal con phishing es que en el caso de pharming la redirección a la página falsa es automática, sin que sea necesario que el usuario necesite pulsar ningún enlace. Así, los estafadores pueden entrar en nuestro ordenador para modificar nuestros ficheros a través de virus de forma que, cuando escribamos en nuestro navegador una dirección determinada, entremos directamente en otra sin saberlo.



Resultado de imagen de pharming informatico

Fuente. https://es.slideshare.net/joycesalas/delitos-informaticos-15846183

SMiShing. Es una estafa en la que por medio de mensajes SMS, se solicitan datos o se pide que se llame a un número de teléfono o que se entre a una web. El objetivo del fraude puede ser suscribir al usuario a un servicio SMS Premium, ofreciéndole por ejemplo una oferta o premio especial, que llame a un número con coste adicional o estafarle con algún producto o servicio inexistente.

En este caso, al jugar en muchas ocasiones con premios y grandes oportunidades, los menores pueden caer fácilmente en la trampa accediendo a las solicitudes de los estafadores sin dudar de la autenticidad de dichos mensajes.

Copyright 2026



Resultado de imagen de smishing ejemplos

Hacking o intrusismo informático, consistente en el acceso no autorizado, por lo general violando los mecanismos de seguridad allí donde los haya, a los archivos y bases de datos contenidos en los sistemas informáticos ajenos, normalmente de grandes empresas o instituciones. “Las conductas de mero hacking acceso a los a los sistemas informáticos perpetrados con la única finalidad de acceder al password o puerta lógica no son actualmente constitutivos de delito pues carecen del elemento subjetivo del injusto”. (Manuel Marchena).

Cracking, también conocido como sabotaje informático. No debemos confundirlo con el password cracking o rompimiento o desciframiento de claves (passwords) que se asimila al hacking. En el primer sentido, Manuel Marchena en “El sabotaje informático: entre los delitos de daños y los desórdenes públicos” los define como conducta consistente en la destrucción o en la producción generalizada de daños en su sistema, datos, programas informáticos o telemáticos.

Indicios de suplantación de identidad

Los menores deben conocer la existencia de ciertos indicios para detectar la posibilidad de que hayan sufrido suplantación de identidad. Algunos de los más importantes son:

- Accesos o usos anómalos de las cuentas. En este caso, por ejemplo, el indicio de suplantación lo tendríamos si nuestros contactos reciben mensajes de nuestra cuenta sin que nosotros los hubiéramos enviado.
- Inminente desactivación de algún servicio que tuviéramos activado sin que hayamos procedido a ello.
- Cambios en el estado de los juegos online sin que los haya realizado por sí mismo.

Las redes sociales suelen tener mecanismos de denuncia a través de los cuales ellos mismo eliminan perfiles que se consideran falsos. Si ninguna de estas dos acciones tienen el final esperado, se debe acudir a las Fuerzas y Cuerpos de Seguridad del Estado o autonómicas para interponer una denuncia.

La suplantación de personalidad es un delito, pero hay que saber cuándo se ha cometido realmente para tipificarlo como tal, pues en ocasiones produce confusión. Según el artículo 401 del Código Penal, sólo se considera delito si lo que se usurpa es el estado civil de otro (es decir, hacerse pasar por otro), y puede conllevar una pena de prisión entre seis meses y tres años.

Ateniéndonos al Código Penal si se crea un perfil falso, entonces no se puede considerar un delito de suplantación de personalidad, porque participar en una red social con datos falsos no implica un

delito de usurpación de estado civil.

Otra cosa es que un individuo entre en una cuenta o perfil de otra persona, ya que se estaría cometiendo un delito contra el derecho a la privacidad debido a que se considera como una forma de revelación de secretos (caso que se recoge a partir del artículo 197 de Código Penal y se contempla como hacking). Y al mismo tiempo. Si para el acceso a la cuenta privada de un ajeno se ha tenido que cometer algún otro delito como el conseguir claves y contraseñas o provocar algún daño en el sistema informático del propietario, el delito se recoge en el artículo 264 del Código Penal y se considera cracking.

Copyright 2026

2.2 Datos y ejemplos

ALGUNOS DATOS Y EJEMPLOS DE SUPLANTACIÓN DE IDENTIDAD

Según datos obtenidos por el estudio “Risk and safety on the internet: the perspective of european children”, el 12% de los menores europeos entre 9 y 16 años han sido víctimas de estos riesgos a través de Internet.

Los resultados de estos estudios resaltan la importancia y la necesidad del diseño de programas de prevención y de campañas de concienciación y sensibilización para garantizar una navegación segura por la Red y evitar en la medida de lo posible la exposición ante estas amenazas de los menores.

Veamos algunos ejemplos de casos reales de suplantación de identidad publicados en los medios de comunicación.

Ejemplo 1. Detenida una joven de 17 años por usurpar el perfil de otra persona en una red social.

Una joven de 17 años ha sido arrestada en Tudela (Navarra), junto con un menor de edad que ha sido puesto a disposición del correspondiente tribunal, acusada de usurpar el perfil de una persona en una red social, publicar fotos íntimas suyas y extorsionarle.

Ambos fueron interceptados por la Policía Foral cuando recogían el dinero exigido a la víctima para devolver las claves de acceso y acusados de los delitos de usurpación de estado civil, contra la intimidad, extorsión y amenazas, según ha informado este jueves el Gobierno de Navarra en un comunicado. La víctima descubrió los hechos cuando, al intentar acceder a una red social de Internet, vio que no podía hacerlo utilizando sus claves habituales, y al entrar desde otra cuenta constató que alguien había usurpado su perfil, colgando además fotos íntimas suyas acompañadas de comentarios desagradables, por lo que presentó una denuncia.

http://cadenaser.com/ser/2010/11/18/ciencia/1290050665_850215.html

Ejemplo 2. Dos jóvenes detenidos por robar fotos de una menor y crearle un perfil falso en Internet.

Copyright 2026

La Guardia Civil ha detenido en Motril a dos jóvenes de 18 y 17 años de edad, como presuntos autores de los delitos de usurpación de identidad y de descubrimiento y revelación de secretos a través de Internet, por usurpar la identidad de una menor a la que crearon un perfil falso en internet a través del que engañaban a terceras personas. El mayor ha pasado a disposición del Juzgado de Guardia y el menor a Fiscalía de Menores.

En concreto, los dos jóvenes detenidos se apoderaron de las fotografías de una menor granadina y con ellas crearon un perfil falso en la red social “Tuenti”. Este perfil lo utilizaban para engañar a compañeros de clase. La madre de la menor, residente en la localidad granadina de Maracena, denuncio que su hija había descubierto un perfil en la red social “Tuenti” con su fotografía.

http://www.elmundo.es/elmundo/2012/11/23/andalucia/1353676945.html

Ejemplo 3. Imputado un menor por usurpación de identidad en una red social.

Aunque actualmente el aún presunto autor de este delito ya se encuentra dentro de la mayoría de edad, contaba con 16 años en el momento en que decidió abrir un nuevo perfil en una conocida red social. Hasta aquí, nada que nos deba extrañar sin embargo este chico utilizó para crear dicho perfil tanto la fotografía como los datos personales de una tercera persona que, una vez se percató de los hechos, lo denunció a la Guardia Civil.

http://www.delitosinformaticos.com/05/2015/delitos/usurpacion-de-identidad/imputado-menor-usurpacion-identidad-una-red-social

Ejemplo 4. Desarticulada una banda que estafaba en internet con suplantación de identidad.

Agentes de la Guardia Civil han desarticulado en Zaragoza una banda criminal formada por siete adultos y un menor que robaban documentos para suplantar la identidad sus víctimas y crear cuentas bancarias a su nombre con las que extraer dinero y adquirir productos de lujo a través de internet.

http://cadenaser.com/emisora/2017/01/31/radio_zaragoza/1485861767_855722.html

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