GOBIERNO DE ESPAÑA
MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO

red.es

"Capacitación en materia de seguridad TIC para padres, madres, tutores y educadores de menores de edad"

[Red.es]

MONOGRÁFICO SUPLANTACIÓN DE IDENTIDAD

MONOGRÁFICO: SUPLANTACIÓN DE IDENTIDAD

1. Objetivo del monográfico

"Sensibilizar sobre los riesgos de la suplantación de identidad y ofrecer pautas a padres, madres, tutores y educadores para su prevención entre los menores, así como mecanismos de actuación en caso de producirse".

2. Conceptualización y descripción del riesgo

¿Qué es la "Suplantación de identidad"?

A nivel 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 tema que se aborda, la **suplantación de identidad en Internet**[1] en menores, un riesgo cada vez más frecuente y que tiene lugar en edades progresivamente más tempranas, se produce cuando una persona malintencionada actúa en nombre del menor haciéndose pasar por él mediante la utilización de diversas técnicas – desarrolladas a lo largo del presente monográfico.

Para abordar el término con mayor exactitud se ha de diferenciar entre dos conceptos, la suplantación de identidad y la usurpación de identidad, dos preceptos no tan alejados en cuanto a significado se refiere, ya que los dos constituyen una apropiación de derechos y facultades que proceden de la persona perjudicada siendo éstos de uso exclusivo de la misma, como pueden ser sus datos personales: su imagen o su propio nombre y apellidos.

La diferencia principal entre ambos conceptos es el uso que se haga de la apropiación de estos derechos y facultades. La suplantación de identidad consiste en la apropiación de esos derechos y facultades propias de la persona suplantada (por ejemplo, acceder sin consentimiento a la cuenta de una red social), mientras que 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 desde dicha cuenta).

[1] PortalLey.com. *Suplantación de identidad en internet. Riegos legales* [recurso web]

Para facilitar su comprensión veamos más en detalle algunos 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. En cualquier caso, todavía se tendría la posibilidad de denunciar el perfil en la propia red social para su eliminación, la mayoría de redes sociales consideran la suplantación de identidad un incumplimiento de sus términos y políticas de uso.
- 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 a través, por ejemplo, de correo o mensajería instantánea (WhatsApp). Sería una usurpación de identidad y se consideraría delito.

Las dos **formas principales** de suplantación de identidad entre menores tanto de primaria (6-12 años) como de secundaria (13-17 años) son:

1. Entrar sin consentimiento en la cuenta de otro menor para:
    - Acceder a información sensible como puede ser el caso de una foto o un video.
    - 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[2]).

2. 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.

En este sentido, se ha de tener siempre presente que exponer información y datos personales sensibles aumenta de forma considerable los riesgos de sufrir una suplantación o usurpación de identidad.

A pesar de ello, este riesgo que supone exponer públicamente información privada o confidencial, es a veces difícil de comprender para los adultos, riesgo que se ve incrementado, en el caso de los menores, ante su mayor ingenuidad y por tanto vulnerabilidad al facilitar datos personales, tanto suyos como de familiares o de compañeros, lo que obliga a aumentar la precaución.

La ingeniería social como herramientas para la suplantación de identidad

Un aspecto interesante a destacar en este punto es el concepto de ingeniería social[3], que se refiere al uso que hacen los ciberdelincuentes de la manipulación psicológica sobre las personas para conseguir sus fines, teniendo en cuenta la tendencia general de éstas a la confianza. La meta del ciberdelincuente en este caso es manipular a la persona objetivo mediante diferentes técnicas para que realice determinadas acciones en su provecho. Por ejemplo, obtener información que le permita un acceso no autorizado a un sistema y, por lo tanto, a la información que resida en el mismo. A pesar de que los objetivos generales de la Ingeniería Social suelen implicar actividades y contextos en los que habitualmente se relacionan adultos, también es posible encontrar situaciones en las que pueden verse implicados los menores.

---

[2] Encontramos un ejemplo de ello en el marco de la operación «Kurier» llevada a cabo por el Equipo de Investigación Tecnológica (Edite)[2] gracias a la cual se pudo detener a un vecino de Ortigueiraque, haciéndose pasar por su hijo, supuestamente actuaba como «ciberacosador» de chicas menores de edad que accedían a mostrarse en ropa interior ante la webcam y a las que luego chantajeaba con difundir dichas imágenes si no accedían a hacer lo que él quería. Tal como podemos observar en este caso, el paso previo al *grooming* por medio del cual se accede al menor no es otro que la propia usurpación de identidad).
Rescatado de: http://www.lavozdegalicia.es/noticia/ferrol/2014/06/11/detenido-hombre-ortigueira-hacerse-pasar-hijo-ciberacosar-menores/00031402476694815983848.htm#.U5qlEg2tb2E.twitter

[3] Granger, Sarah (2001)*Social Engineering Fundamentals*, Part I: Hacker Tactics

Internet se ha configurado como uno de los espacios donde los ingenieros sociales actúan mayoritariamente para buscar contraseñas tanto de redes sociales, donde los menores participan habitualmente de forma activa, como en otros espacios como pueden ser el correo electrónico y los entornos de juegos online. Además, los métodos básicos empleados por las personas que utilizan esta técnica, esencialmente marcados por la persuasión, son altamente eficaces 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.

Así, vía Internet o a través de la web se usa, adicionalmente, el envío de solicitudes de renovación de permisos de acceso a páginas web que solicitan respuestas e incluso las famosas cadenas de mensajes, llevando así a revelar información sensible o comprometer la seguridad de los sistemas..

Motivaciones para la realización de suplantación de identidad

La suplantación de identidad se puede producir por varios motivos, aunque en el caso de los jóvenes lo más común es hacerlo por mera diversión, para “burlarse” de un compañero/a o con motivos de venganza, en los adultos los motivos suelen ser más profundos, y suele pretenderse crear un daño en la reputación de una persona a través de la publicación de fotografías o información falsa.

Estos actos pueden ocasionar graves problemas a las víctimas relacionados con la vulneración de su intimidad, daños directos a su reputación o con problemas sociales motivados por las actuaciones realizadas por la persona que usurpa la identidad de la misma, ya que una vez que se publica algo en la red su difusión es inmediata, haciendo que se pierda el control sobre el contenido y que sea muy complicado solucionarlo.

Además de los problemas de reputación, existen casos en los que se suplanta la identidad de un tercero para cometer algún tipo de delito bajo esa identidad. En este caso, su solución pasa por un proceso más largo. También es muy común que estos hechos causen perjuicios económicos a las víctimas, cuando se suplanta su identidad para realizar algún tipo de compra o transacción económica.

Técnicas más utilizadas para la suplantación de identidad

A continuación detallamos cuáles son las técnicas más utilizadas para la suplantación de identidad:

- ***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".

  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 especialmente a la presencia de este tipo de técnicas en aquellos escenarios de mayor participación infantil y juvenil. Se han creado leyes que castigan este tipo de delitos y campañas para prevenir y sensibilizar a los usuarios para que apliquen esas medidas de seguridad.

  Así, en lo concerniente al contexto relacionado con menores, uno de los servicios más utilizados por los ciberdelincuentes para suplantar la identidad de los mismos son las redes sociales. Para ello suelen emplear una serie de excusas para engañar al usuario tales como enviar un mensaje privado en el que se comunique que se han detectado conexiones extrañas en la cuenta por lo que, para mantener la seguridad, se recomienda que se cambien las claves. En otras ocasiones, como en el caso de la imagen aportada, crean sitios web falsos con la apariencia de la página de inicio de sesión de Facebook para que cuando se introduzca el correo electrónico y la contraseña se grabe y conserve esta información. De un modo u otro, el objetivo en este caso es conseguir el acceso a la cuenta del menor para obtener sus datos privados y suplantar o usurpar su identidad.

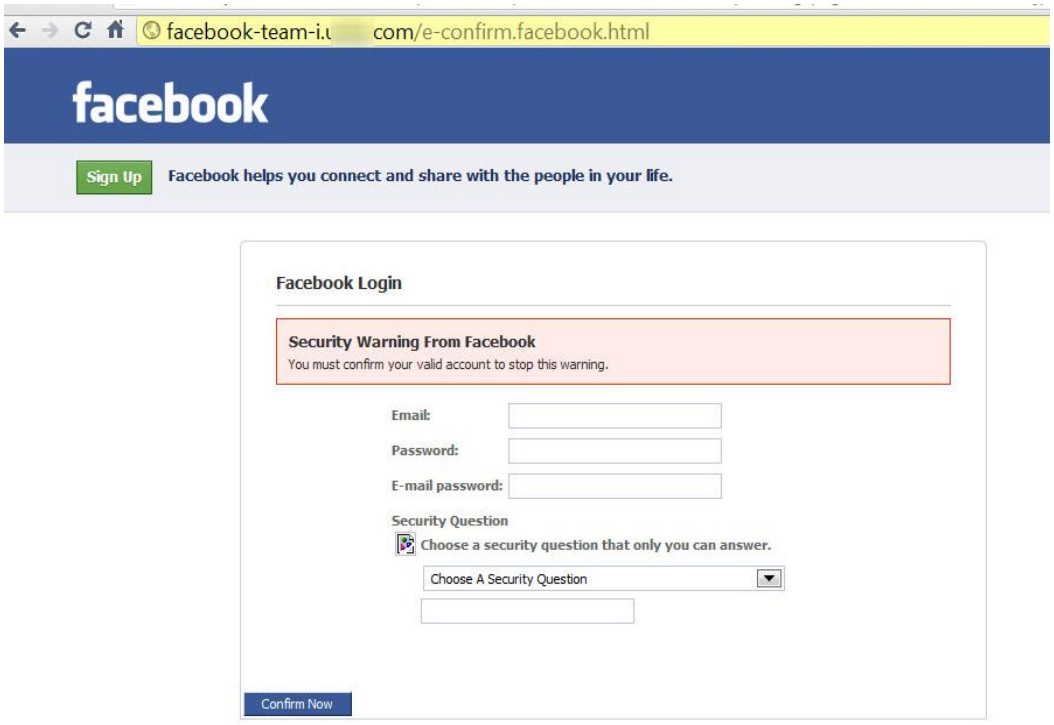

IMAGEN DE INTERNET. Ejemplo de *phishing* en Facebook[4]

En el caso que ocupa en este monográfico, el riesgo se materializa del mismo modo a través del uso de este tipo de aplicaciones a través del móvil ya que también se han creado aplicaciones que imitan el procedimiento de identificación en redes sociales.

Igualmente, se detectan cada vez más campañas masivas de correos fraudulentos que utilizan como excusa el envío de un documento falso a través de Google Docs. Así, para engañar al usuario, ya sea adulto o menor, solicitan que se identifique para poder visualizar dicha información y así obtener sus datos de acceso a todos los servicios de Google.

Finalmente, se encuentran casos de phishing a menores a través de juegos online. Al igual que en los anteriormente descritos, 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.

[4] Recuperado de: http://dataprotectioncenter.com/security/avoiding-facebook-phishing/

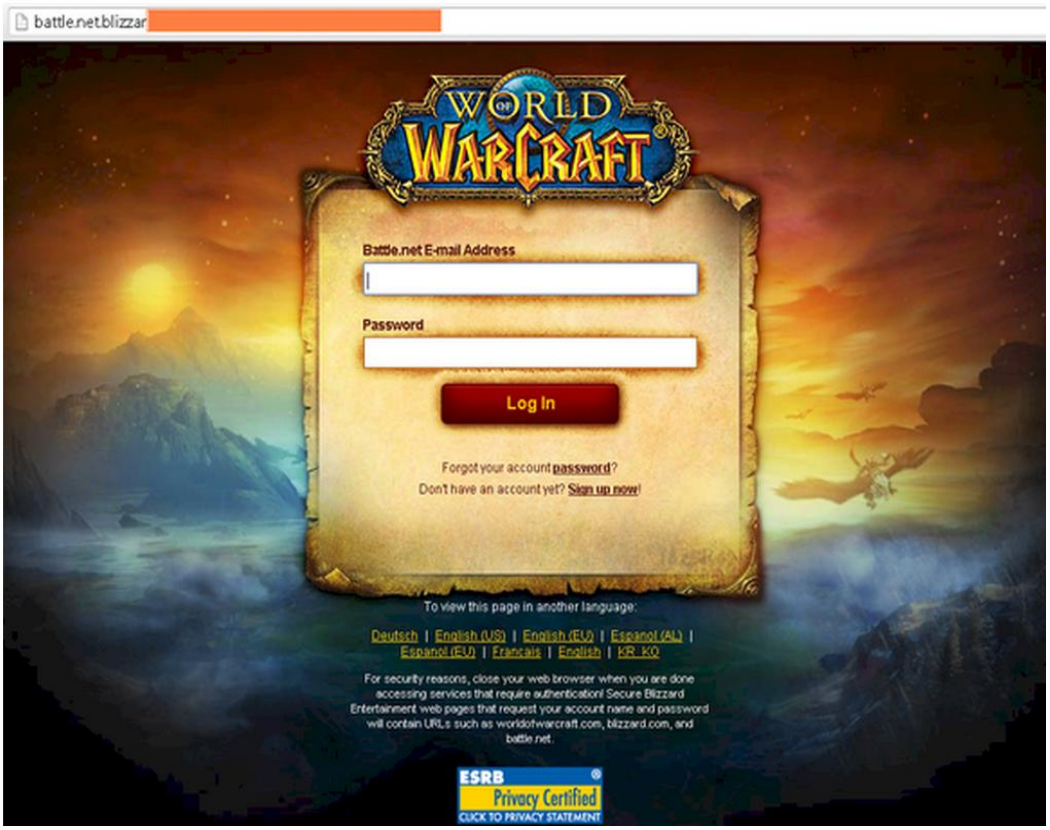

IMAGEN DE INTERNET. Ejemplo de *phising* en juegos online.[5]

- ***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 equipo para modificar los ficheros a través de virus de forma que, cuando se escribe en nuestro navegador una dirección determinada, se entra directamente en otra sin saberlo.
- ***SMiShing***: aunque menos habitual en la actualidad debido al menor uso de SMS entre los usuarios, como variante del phishing, se configura como un tipo de delito o actividad criminal que emplea técnicas de ingeniería social y mensajes de texto dirigidos a los usuarios de telefonía móvil. Es una estafa

[5] Recuperado de: https://www.osi.es/es/actualidad/blog/2014/04/11/aprendiendo-identificar-los-10-phishing-mas-utilizados-por-ciberdelincuen.

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, de este modo, 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.

Indicios para pensar que han suplantado la identidad

Los menores deben conocer la existencia de ciertos indicios para detectar la posibilidad de que hayan sufrido suplantación de identidad. Entre ellos podemos destacar los siguientes:

- **Accesos o usos anómalos de las cuentas**. En este caso, por ejemplo, el indicio de suplantación se manifestaría si los contactos de la cuenta reciben mensajes de la cuenta del implicado sin que los hubiera enviado. Del mismo modo ocurriría si le aseguran que estaba en “línea” sin que fuera cierto.
- **Inminente desactivación de algún servicio** que se tuviera activado sin que se haya procedido a ello.
- En el caso de los menores**, cambios en el estado de los juegos online** sin que los haya realizado por sí mismo**.**

3. Datos de situación y diagnóstico

Se exponen a continuación los resultados de una serie de estudios en referencia al tema de suplantación de identidad que se han seleccionado tanto a nivel nacional como europeo y que a nivel estadístico arrojan resultados esclarecedores sobre dicho riesgo:

A nivel nacional

"España es número uno europeo en casos de suplantación de identidad. U**n** 7% de los usuarios españoles de Internet han sido víctimas de problemas que tienen relación con información privada y datos personales**,** un 3% más que la media europea"[6]

Por otro lado según el estudio sobre "Los riesgos de la red, según las personas adultas"[7] a través de una encuesta a la población adulta seleccionada en la que se realizaba la siguiente pregunta "*¿Cuáles son los riesgos que se presentan a los menores en Internet?*", el resultado obtenido revelaba según la encuesta que los adultos opinaban que de todos los riesgos a los que pueden exponerse los menores en la red, al riesgo de suplantación de identidad o identidad falsa le asignaban un valor del 5 %.

A nivel europeo

Según datos obtenidos del estudio "*Releasing children's potential and minimizing risks: ICT's Internet and violence against children*[8]" realizado por las Naciones Unidas, se reconoce el riesgo de suplantación de identidad como uno de los riesgos que tienen los menores asociado al uso de Internet y las redes sociales.

Por último, según datos obtenidos por el estudio "*Risk and safety on the Internet: the perspective of european children*[9]**"**, el 12% de los menores europeos entre 9 y 16 años han sido víctimas de estos riesgos a través de Internet, tal y como se desprende de un estudio de la Comisión Europea realizado con una muestra de 23.420 jóvenes (y sus padres/madres) de los 25 países europeos.

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.

[6] Eurostat (2011).*Informe Safer Internet Day*.Recuperado de: http://epp.eurostat.ec.europa.eu
[7] Pantallas Amigas (2012). *Estudio "Los riesgos que hay en internet según las personas adultas".*
[8] UN (2014).Releasing Children's Potential and Minimizing Risks: ICT's, the internet and violence against children.
[9] London School of Economics and Political Science (2010) *Informe Risks and safety on the internet*.

4. Ejemplos de casos reales

A continuación se muestran casos reales de suplantación de identidad, con el fin de ilustrar con algunos ejemplos este riesgo en materia de seguridad TIC en menores:

Dos chicas multadas con 12.400 euros por crear un perfil falso de otra en Tuenti[10]

Dos chicas deberán pagar 12.400 euros de indemnización y 200 euros de multa cada una por haber abierto un perfil falso de una tercera en la red social Tuenti, frecuentada principalmente por adolescentes y jóvenes, cometiendo una falta de vejaciones injustas, según una sentencia de la Audiencia Provincial de Segovia. La víctima era menor de 20 años en el momento de los hechos y que fue dada de alta en 2009, debido a los problemas psicológicos causados.

Al igual que el juzgado, la audiencia segoviana entiende que se ha registrado una falta continuada de vejaciones injustas y, salvo recurso extraordinario de amparo ante el Tribunal Constitucional, no cabe otro contra este fallo, según fuentes judiciales.

Detenida una joven de 17 años por usurpar el perfil de otra persona en una red social[11]

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.

[10] El País. (2011). Sociedad. Recuperado de: http://sociedad.elpais.com/sociedad/2011/05/30/actualidad/1306706408_850215.html

[11] SER. (2010). Ciencia y Tecnología. Recuperado de: http://cadenaser.com/ser/2010/11/18/ciencia/1290050665_850215.html

Dos jóvenes detenidos por robar fotos de una menor y crearle un perfil falso en Internet[12]

La Guardia Civil ha detenido en Motril a dos jóvenes de 18 y 17 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 le 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, denunció que **s**u hija había descubierto un perfil en la red social 'Tuenti' con su fotografía.

Ese perfil era de una mujer que decía ser de Motril y a la que su hija no conocía de nada. Dentro de ese perfil había más de 300 fotografías de su hija, las cuales habían sido sustraídas de un álbum de otro perfil, este auténtico y gestionado por la propia menor, en esa misma red social.

5. Estrategias, pautas y recomendaciones para su prevención

Las recomendaciones y buenas prácticas que se deben tener en cuenta a la hora de navegar en Internet permiten aumentar en los padres, madres, tutores y educadores el conocimiento de estrategias sobre seguridad informática, para ser aplicadas con los menores en los entornos escolares o familiares. En el caso de la suplantación de identidad, la única forma de lograr que los menores estén menos expuestos a esta situación de riesgo, es la prevención y el uso de una serie de estrategias que minimicen las posibilidades de sufrirlo. La familia ha de enseñar a sus hijos una serie de reglas básicas sobre seguridad informática.

El desconocimiento sobre los riesgos en seguridad informática y sobre los mecanismos de protección, hacen que el menor actúe sin precaución al manejar la información a través de los medios tecnológicos. A esto se suma el desconocimiento

[12] El mundo. (2012). *Dos jóvenes detenidos por robar fotos de una menor y crearle un perfil falso en Internet*. Recuperado de: http://www.elmundo.es/elmundo/2012/11/23/andalucia/1353676945.html

que los padres y docentes aún presentan en materia de riesgos y seguridad informática, la llamada "brecha digital" que les separa de ellos y que afortunadamente cada vez va siendo menor.

Por tanto, se debe tener muy claro que el problema, como otros muchos que se presentan en nuestra sociedad actual, es de educación y por ello es fundamental la creación de alternativas educativas que capaciten al menor para utilizar apropiadamente los recursos tecnológicos y al mismo tiempo estar completamente informados sobre todos los peligros y riesgos a los que se exponen al interactuar con dichas tecnologías y manejar su información por medio de ellas[13].

Recomendaciones para prevenir la suplantación de identidad

Entre las recomendaciones que se pueden realizar tanto a padres como a menores y educadores para prevenir el robo de identidad se encuentran las siguientes:

- Para lograr **minimizar la exposición de datos sensibles** resulta necesario concienciar a los menores sobre la importancia de limitar la difusión voluntaria de datos personales y privados en redes sociales, juegos online, mensajería instantánea, formularios y aplicaciones. Para ello:
    - Se debe ayudar a configurar de forma correcta las **opciones de privacidad** de los diferentes sitios web frecuentados por los menores a su cargo. Para obtener más información, se puede consultar el monográfico Gestión de Privacidad.
    - Desde el propio ejemplo del adulto, se traslada la idea de que se debe ser discreto a la hora de publicar fotografías en la web y, sobre todo, de que se debe **«pensar antes de publicar»** de forma impulsiva para poder valorar las posibles consecuencias del comportamiento en la red.
- Con el objetivo de minimizar los riesgos que puedan afectar a los equipos y servicios que se utilizan no sólo se debe educar a los menores para mantener un **equipo seguro** a través de actualizaciones de software y antivirus sino que además se recomienda:

[13] Savethechildren (2010). Informe "*La tecnología en la preadolescencia y adolescencia"*. Recuperado de: http://www.deaquinopasas.org/docs/estudio_riesgos_internet.pdf [recurso web]

- **Contar con cuentas de usuario limitadas** para cada una de las personas que utilizan el equipo compartido con contraseñas personales para regular el acceso a éste. De esta forma, cada usuario podrá tener su propio escritorio -con aquellos archivos y carpetas a los que pueda acceder- de forma que tan solo el usuario administrador, con permiso para poder administrar las diferentes cuentas, pueda instalar aplicaciones o modificar aspectos importantes de la configuración. Así, se minimiza el riesgo de infección por virus y, por tanto, del robo de contraseñas de los servicios.

  Para obtener más información sobre cuentas de usuario y su configuración, consultar: www.osi.es/es/cuentas-de-usuario

- **Bloquear las ventanas emergentes.** A pesar de que normalmente los navegadores de Internet tienen activado el bloqueador de ventanas emergentes por defecto, se pueden administrar definiendo excepciones en particular accediendo a las opciones de configuración del navegador.

- **Hacer uso de los filtros *antispam*.** Activados por defecto en la mayoría de servicios web, filtran el correo electrónico que consideran basura a una carpeta donde lo almacenan. El correo electrónico es una de las formas de comunicación más utilizadas en la actualidad y por tanto un medio muy atractivo para la propagación de virus, mensajes fraudulentos, *spam,* etc.

- **Llevar a cabo una adecuada gestión de contraseñas**. En este sentido se debe tener en cuenta la importancia de no utilizar una misma contraseña para varios servicios ya que, de ser así, será mucho más fácil acceder a todos ellos una vez que se haya conseguido vulnerar la primera. Además de utilizar contraseñas diferentes, éstas deben ser seguras, es decir, deben ser secretas, robustas (de mínimo ocho caracteres, que combine mayúsculas, minúsculas, números y símbolos) y modificadas periódicamente.

  Ejemplo de ello puede ser el reciente caso de robo de fotos y videos de famosas almacenados en la nube de Apple.

  www.lasexta.com/noticias/cultura/apple-dice-que-hackeo-fotos-famosas-fue-culpa_2014090300186.html

Además de lo anterior, se deben modificar periódicamente nuestras contraseñas. Para ello, la mayoría de servicios de Internet permiten cambiar la contraseña desde el panel de gestión de la propia cuenta. Del mismo modo, se debe trasladar a los menores que, aunque lo ideal sería no guardar nuestras contraseñas en el navegador para que nadie pueda acceder a nuestras cuentas de forma directa, en caso de que las guarden deben tomar ciertas precauciones. Así, se recomienda utilizar una contraseña maestra en el navegador o, al menos, una contraseña de acceso al dispositivo (por ejemplo, contraseñas de acceso al ordenador o patrón de desbloqueo en móviles) y advertir que nunca debe facilitar dichas contraseñas a nadie.

- Para poder llevar a cabo una **buena práctica en el uso de servicios** tales como el correo electrónico, las redes sociales, la mensajería instantánea o la propia navegación no se debe olvidar que no es recomendable acceder a enlaces que resulten sospechosos. Igualmente se debe tener precaución con las descargas que se realizan, desconfiar de remitentes desconocidos en correos y no abrir ficheros adjuntos sospechosos.

  Así mismo, algunos indicios que se deben tener en cuenta para sospechar que un correo electrónico tiene fines maliciosos son:

  - **Enlaces disfrazados:** en este caso, los enlaces en el correo electrónico estarán presentados de forma que parezcan auténticos. A pesar de ello, existen algunos indicios a los que se ha de atender para poder discriminar su talante engañoso: las URL pueden ser similares a las auténticas pero se intercambian letras parecidas entre sí (por ejemplo, en lugar de www.spotify.com se podría enlazar a www.spotifi.com), el texto del enlace e hiperenlace pueden ser diferentes o se pueden introducir cambios en los acortadores de URL de modo que finalmente redireccionan a sitios web no seleccionados intencionadamente.
  - "**Es urgente que actúes":** se debe ser cautelosos con los correos que den sentido de urgencia, con mensajes tales como: "tu cuenta está a punto de ser eliminada", "tu cuenta debe ser actualizada", etc. Se trata de un claro ejemplo de técnica de

ingeniería social, al apremiar al lector y dificultar que pueda tomar una decisión razonada.

- **Cuenta equivocada**: se debe estar seguro de que los correos llegan a la cuenta adecuada y a la que se ha facilitado de entre las varias que se pueden tener para ello. De lo contrario se podría sospechar que se trata de un fraude.

- En el caso de **juegos en línea**, se ha de prestar atención al software del juego utilizando el programa oficial del mismo y asegurarse también de que los *plugins* (programas que se anexan a otros para aumentar sus funcionalidades) que se descarguen sean realmente oficiales.

- Se recomienda valorar, en función de la importancia del servicio y de las situaciones de contexto en las que se accede al mismo (por ejemplo, cuando se utilizan ordenadores públicos, compartidos o WiFis ajenas) el uso de medidas de seguridad con **segundos factores de autenticación o verificación**, ya que las contraseñas por sí solas no son suficientemente seguras para proteger la información y documentos que se consideran importantes. Por tanto, una de las posibilidades que se tienen al alcance actualmente y que ya está implementada en los principales servicios web es la verificación en dos pasos o segundo factor de autenticación (*Two Factor Authentication 2FA*).Este método conlleva la exigencia al usuario on-line de la introducción de dos contraseñas separadas antes de ser autorizado para iniciar sesión en una cuenta. La primera contraseña es la contraseña de la cuenta principal del usuario, que no cambia salvo que el usuario la cambie voluntariamente. La segunda contraseña se envía normalmente a una ubicación separada (por ejemplo, al teléfono móvil) como un *token* de seguridad único (un generador de códigos) que caduca en un período muy corto de tiempo (por ejemplo, 30 minutos). Esto hace que a un atacante que esté le sea prácticamente imposible detectar el segundo factor de autenticación a menos que tenga físicamente el dispositivo al que se envía el código.

- Explicar al menor los **riesgos de los mecanismos de recuperación de contraseñas** tales como la pregunta secreta que piden al crear la cuenta. En este sentido hay que tener presente que se deben establecer preguntas

secretas que solamente sean conocidas por la propia persona como medida de seguridad.

Ejemplo de ello podría ser el caso real relacionado con la vulneración de la cuenta T-Mobile de Paris Hilton al descubrir el ciberdelincuente la respuesta a su pregunta secreta. Puedes acceder a la noticia a través del siguiente enlace: www.microsiervos.com/archivo/seguridad/el-crackeo-de-paris.html

- **Bloquear el ordenador y cerrar las sesiones** al terminar de usar el equipo como medida para "cerrar la puerta" a cualquier persona ajena al mismo.

- Es importante educar a los menores para que tomen precauciones al utilizar **ordenadores públicos y al conectarse a redes WiFi públicas**. Por eso nunca se debe utilizar redes WiFi no confiables para acceder a servicios donde se intercambie información sensible o un componente importante de privacidad. Para proteger de estos riesgos en redes donde los demás usuarios son desconocidos podemos aplicar una serie de medidas de seguridad tales como:

    - tener instalado y habilitado un cortafuegos.
    - personalizar la configuración de red en nuestro sistema.

  Ver más información en: www.osi.es/es/wifi-publica

- 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. Igualmente, apunte el número identificativo del teléfono (IMEI) para utilizarlo en caso de pérdida y sea cauto en el uso del *bluetooth.* Como ya se sabe, son muchos los datos de carácter personal (fotografías, mensajes de texto, acceso a aplicaciones de redes sociales y correo electrónico o agenda de contactos) a los que se pueden acceder a través de nuestro móvil.

Recomendaciones para padres, madres y tutores

En líneas generales, destacar que las recomendaciones como padres, madres o educadores han de partir siempre desde el diálogo y la participación ya que, si se imponen normas como una forma de control y prohibición, probablemente resulte más

difícil la interiorización de este tipo de pautas por parte de los menores. Por el contrario, se debe de enfocar la intervención como un modo de despertar el sentido crítico de éstos para que, progresivamente, sean cada vez más autónomos a la hora de instaurar las medidas abordadas anteriormente.

Se debe trasladar al menor la importancia de todos los aspectos expuestos para la protección de su propia identidad, teniendo en cuenta también el uso que los adultos mismos como padres y madres hacen de las redes o de cualquier otro dispositivo, ya que para los menores somos modelos a seguir. Por lo tanto es recomendable que los menores vean en sus figuras de referencia, predicando con el ejemplo, buenos hábitos y prácticas en el uso de las tecnologías en nuestro día a día.

No hay que olvidar que una labor fundamental dentro del entorno familiar es llegar a negociaciones con el menor y saber poner límites, es decir, es conveniente que se compatibilicen actividades no tecnológicas con las virtuales, para evitar con ello en la medida de lo posible, que el comportamiento del menor sea únicamente digital; a modo de sugerencia y recomendación se podría potenciar y motivar hacia actividades de ocio saludable por parte de los menores, como el deporte, lectura, actividades al aire libre, etc.

Recomendaciones para educadores

Del mismo modo en el caso de los educadores, se ha de trasladar igualmente la importancia de estos aspectos para la protección de su identidad en la actividad docente, incorporando para ello éstas prácticas en la medida de lo posible en las políticas y reglamentos TIC del centro.

Para poder cumplir con los objetivos propuestos, se recomienda que se organicen de manera periódica talleres de sensibilización y formación para menores, padres, madres y comunidad educativa general.

También señalar que los centros educativos tienen la posibilidad de participar en el **Plan Director para la Convivencia y Mejora de la Seguridad en los Centros Educativos y sus Entornos**[14], que pretende potenciar actuaciones preventivas en

[14] Ministerio del Interior. Instrucción nº 7/2013 de la Secretaría de Seguridad, sobre el "Plan Director para la Convivencia y Mejora de la Seguridad en los Centros Educativos y sus Entornos". Recuperado de: http://www.interior.gob.es/documents/642012/1568685/Instruccion_7_2013.pdf/cef1a61c-8fe4-458d-ae0d-ca1f3d336ace

relación con los riesgos a los que se ven sometidos los menores y los jóvenes, en temas tan importantes como el uso de Internet y las nuevas tecnologías, entre otros. En el marco de este Plan los miembros de las Fuerzas y Cuerpos de Seguridad realizan charlas, visitas y actividades en centros escolares, dirigidas tanto al alumnado como al resto de la comunidad educativa (directivos, personal docente y Asociaciones de Madres y Padres de Alumnos). Como medidas adicionales, se contemplan acciones de sensibilización y formación dirigidas a concienciar sobre el "uso responsable de las nuevas tecnologías y los riesgos que las mismas pueden implicar, promoviendo, a su vez, la comunicación a su entorno familiar, educativo o a las Fuerzas de Seguridad de los hechos de los que pueden ser víctimas o testigos.

6. Mecanismos de respuesta y soporte ante un incidente

A continuación se presentan una serie de medidas que se pueden realizar en caso de detectar una suplantación de identidad en nuestros menores:

- En primer lugar, advertir que 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 plataforma o el servicio a través del cual haya tenido lugar, 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 ante un caso de usurpación de identidad y una vez detectado dicho delito en el menor, hay que proceder a su denuncia en el correspondiente servicio (contactando con los responsables y/o administradores de las redes sociales, sitios web, servidores de correo, buscadores de información, blogs, wikis, etc.). La mayoría de ellos ponen a disposición del usuario mecanismos de denuncia de este tipo de situaciones. Así, si el incidente no se considera muy grave, resulta recomendable intentar gestionarlo primero a través de ésta vía. 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, que disponen de grupos específicos especializados en este tipo de delitos. Para obtener más información sobre los procedimientos de denuncia para cada servicio puedes acceder al siguiente enlace:

www.osi.es/es/actualidad/blog/2014/05/14/como-denunciar-una-suplantacion-de-identidad-en-internet

- 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. Esta labor puede ser más sencilla en casos de menores de secundaria, ya que suelen tener un mayor conocimiento que en el caso de los menores de primaria.

- Contactar con los buscadores que están enlazando a esa información para evitar la indexación a la misma.

- 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 (Ej.: Redes sociales, correo electrónico, etc.), y en la medida de lo posible, tratar de deshacer lo que haya realizado el agresor en nuestro nombre.

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

- Policía Nacional (Brigada de Investigación Tecnológica)
    - www.policia.es/bit
        - Correo electrónico (consultas genéricas):
            - delitos.tecnologicos@policia.es
        - Correo electrónico (pornografía infantil):
            - denuncias.pornografia.infantil@policia.es
        - Teléfonos: 915.822.751/752/753/754/755
- Guardia Civil (Grupo de Delitos Telemáticos)
    - www.gdt.guardiacivil.es/webgdt/home_alerta.php
    - Teléfono: 900.101.062 (Oficina de atención al ciudadano)

7. Marco legislativo aplicable a nivel nacional y europeo

En España se encuentra una legislación anticuada que a veces no da solución a los problemas planteados con las nuevas tecnologías ya que no existe una regulación

específica concretamente referida a suplantación o robo de identidad en menores. No siempre se puede utilizar el tipo penal del artículo 401 del Código Penal para denunciar una suplantación de identidad, por lo que debemos recurrir a otros caminos como por ejemplo la **Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal,** por utilizar los datos de una persona sin el debido consentimiento, ya que el artículo 6 de esta Ley dispone que los datos deben ser proporcionados con el consentimiento inequívoco del afectado, algo que evidentemente en un perfil falso producido por un tercero no sucede o también la utilización de la Ley Orgánica 1/1982, de 5 de mayo, sobre Protección civil del Derecho al Honor, a la Intimidad Personal y Familiar y a la propia Imagen. No obstante, este tipo de prácticas se circunscriben en la jurisdicción penal como delito de usurpación del estado civil del artículo 401 del Código Penal Español (Ley Orgánica 10/1995, de 23 de noviembre. El código penal usa el concepto 'civil' como 'identidad' o 'personalidad').

Desde el punto de vista penal ha de partirse del hecho de que no existe ningún tipo penal que expresamente regule esta situación como tal.[15] Ahora bien, sí encontramos referencias expresas a la "suplantación del estado civil", regulada en el artículo 401, donde se dispone que: *"El que usurpare el estado civil de otro será castigado con la pena de prisión de seis meses a tres años."*[…]

Si todo ello se traslada las conductas más habituales en Internet en relación a la suplantación de identidades digitales, se ha de tener presente que si bien el *crackeo* de una cuenta de Facebook o Twitter, por ejemplo, por sí misma no es una suplantación de identidad constitutiva del delito de usurpación del estado civil, sí podría ser constitutiva de un delito de descubrimiento y revelación de secretos, regulado expresamente en los artículo 197 y siguientes del Código Penal o incluso un delito de daños en "redes, soportes o sistemas informáticos" expresamente reconocido en el artículo 264.2 del Código Penal.

Ahora bien, si además de llevarse a cabo la "ciberocupación" de la cuenta de Facebook, Twitter o cualquier red social o blog de un usuario, se utiliza la misma para dar la sensación al resto de usuarios que quien escribe es la persona titular de la misma, llevando a cabo acciones "que solo puede hacer esa persona por las facultades, derechos u obligaciones que a ella solo corresponden", entonces sí

[15] Hurtado, A. (2011). "*Suplantación de identidad en Internet. Aspectos penales*" Recuperado de https://www.incibe.es/blogs/post/Seguridad/BlogSeguridad/Articulo_y_comentarios/Post_suplantacion [recurso web]

estamos ante una auténtica suplantación de identidad, o usurpación del estado civil propia del artículo 401 del Código Penal.

Por tanto, la suplantación de identidad está considerada como un delito, perseguido por la ley independientemente de la forma en que se lleve a cabo. Sin embargo, el hecho de que ocurra a través de las TIC, permite que el rastro que se deja por Internet constituya un agravante a tener en cuenta. En este caso la conducta puede ser castigada con pena de prisión de seis meses a tres años. Ahora bien, para que exista una verdadera suplantación de identidad debe darse una usurpación de todas las características que integran la identidad de una persona, asumiéndolas el suplantador como propias (crear un perfil inventado o con datos falsos no se considera un delito, al igual que inventarse datos para participar en una red social, por ejemplo).

Ante este tipo de situaciones se recomienda a los usuarios acudir de forma inmediata ante las fuerzas y cuerpos de seguridad, para interponer la correspondiente denuncia. En ella, deben reflejarse los hechos propios de la suplantación de identidad, así como los –más que habituales– posibles presuntos delitos derivados de las acciones llevadas a cabo por el suplantador, como son posibles delitos de amenazas, estafas, o semejantes. Se daría así inicio a la vía de investigación correspondiente para su posterior puesta a disposición judicial, donde se llevará cabo la instrucción para determinar la persona física concreta que llevó a cabo dicha acción, así como el enjuiciamiento de la misma –en caso de determinarse la existencia del delito de "usurpación del estado civil" y cualesquiera otro que pudiera haberse producido derivado de éste–."

Como se puede ver, al igual que en otros tipos de delitos, no se habla del medio a través del que se lleve a cabo (online u offline), sin que esto sea un obstáculo para que en caso de darse los requisitos del tipo penal, pueda ser apreciado por el Juez que conozca sobre el caso concreto.

En el marco de la **Unión Europea**, se cuenta con diversas directivas relativas a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos [95/46/CE, de 24 de octubre], la protección de la intimidad en el sector de las comunicaciones electrónicas [2002/58/CE, de 12 de julio] o las operaciones de pago con dinero electrónico [2007/64/CE, de 13 de noviembre] pero aún no existe ninguna disposición comunitaria que armonice la regulación en materia de suplantación de la identidad digital ni que establezca unos requisitos mínimos a las empresas proveedoras de estos servicios.

8. Organismos, entidades y foros de referencia

A continuación se detallan una serie de organismos, entidades y foros relacionados con la suplantación de identidad en Internet en menores:

ORGANISMO / DETALLE
Chaval.es (www.chaval.es) Iniciativa del Ministerio de Industria, Energía y Turismo, puesta en marcha por Red.es para responder a la necesidad de salvar la brecha digital entre padres, madres, tutores y educadores respecto al avance de los menores y jóvenes en el uso de las TIC. Ofrece recursos de sensibilización y formación sobre la suplantación de identidad.
Oficina de Seguridad del Internauta (www.osi.es) Proporciona información y soporte necesarios para evitar y resolver los problemas de seguridad que pueden existir al navegar por Internet.
Pantallas Amigas (www.pantallasamigas.net) Iniciativa que tiene como misión la promoción del uso seguro y saludable de las nuevas tecnologías y el fomento de la ciudadanía digital responsable en la infancia y la adolescencia. Algunas de sus actividades principales son la creación de recursos didácticos, sesiones y jornadas formativas y estudios, con especial énfasis en la prevención del ciberbullying, el grooming, el sexting, la sextorsión y la protección de la privacidad en las redes sociales. Dispone de una línea de ayuda para niños y adolescentes ante situaciones de peligro en Internet.
Instituto Nacional de Ciberseguridad (www.incibe.es) Sociedad dependiente del Ministerio de Industria, Energía y Turismo (MINETUR) a través de la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información (SETSI). Es la entidad de referencia para el desarrollo de la ciberseguridad y de la confianza digital de los ciudadanos, la red académica y de investigación española (RedIRIS) y las empresas, especialmente para sectores estratégicos.
INSAFE (www.saferinternet.org) Organización europea para la promoción del uso seguro, responsable tanto en Internet como en los dispositivos móviles por los jóvenes.

9. Más información

Se puede obtener más información sobre suplantación de identidad en:

RECURSO / DETALLE
Guía para usuarios sobre identidad digital y reputación online (INTECO) Guía que analiza los conceptos de identidad digital y reputación online desde el punto de vista de la privacidad y la seguridad. Dedica apartados específicos a la suplantación de identidad, describiendo el riesgo y aportando recomendaciones y pautas para evitarlo. https://www.incibe.es/CERT/guias_estudios/guias/Guia_Identidad_Reputacion_usuarios
Guía de menores en Internet (INTECO) Guía que ofrece recomendaciones y pautas para menores a la hora de navegar por Internet; advirtiendo de los principales problemas con los que pueden encontrarse y cómo evitarlos. https://www.incibe.es/extfrontinteco/img/File/intecocert/Proteccion/menores/guiapadresymadres.pdf
Portal Navegación segura (INTECO y Páginas Amigas) Se trata de un recurso educativo online sobre navegación segura en Internet, con recomendaciones para proteger la privacidad e intimidad en la Red, estar a salvo de chantajes, timos, etc. http://www.navegacionsegura.es

10. Bibliografía

Data Protection Center (2011).*Avoiding Facebook Pishing.* Recuperado de: http://dataprotectioncenter.com/security/avoiding-facebook-phishing/

Eurostat (2011).*Informe Safer Internet Da*y.Recuperado de: http://epp.eurostat.ec.europa.eu/

Granger, Sarah (2001)*Social Engineering Fundamentals*, Part I: Hacker Tactics

Hurtado, A. (2011). *Suplantación de identidad en Internet. Aspectos penales.* Recuperado de: https://www.incibe.es/blogs/post/Seguridad/BlogSeguridad/Articulo_y_comentarios/Post_suplantacion

Instituto Nacional de Tecnologías de la Información INTECO (2009). *Guía de menores en Internet*.

London School of Economics and Political Science (2010).*Informe Risks and safety on the Internet.*

Oficina de Seguridad del Internauta (2014). *Aprendiendo a identificar los diez phishing más utilizados por los ciberdelincuentes*. Recuperado de: https://www.osi.es/es/actualidad/blog/2014/04/11/aprendiendo-identificar-los-10-phishing-mas-utilizados-por-ciberdelincuen.

Pantallas Amigas (2012). *Estudio "Los riesgos que hay en Internet según las personas adultas".*

PortalLey.com. *Suplantación de identidad en Internet. Riegos legales* [recurso web]

Save the children (2010).*Informe La tecnología en la preadolescencia y adolescencia*. Recuperado de: http://www.deaquinopasas.org/docs/estudio_riesgos_internet.pdf [recurso web]

UN (2014).*Releasing Children's Potential and Minimizing Risks: ICT's, the internet and violence against children.*

Wikipedia (2015). *Ingeniería social*. Recuperado de: http://es.wikipedia.org/wiki/Ingenier%C3%ADa_social_%28seguridad_inform%C3%A1tica%29