
“Capacitación en materia de **seguridad TIC** para padres,
madres, tutores y educadores de menores de edad”

[Red.es]

JUEGOS EN FAMILIA PRIMARIA (6-12 AÑOS) SUPLANTACIÓN DE IDENTIDAD

La presente publicación pertenece a Red.es y está bajo una licencia Reconocimiento-No comercial 4.0 España de Creative Commons, y por ello está permitido copiar, distribuir y comunicar públicamente esta obra bajo las condiciones siguientes:

- *Reconocimiento: El contenido de este informe se puede reproducir total o parcialmente por terceros, citando su procedencia y haciendo referencia expresa tanto a Red.es como a su sitio web: www.red.es. Dicho reconocimiento no podrá en ningún caso sugerir que Red.es presta apoyo a dicho tercero o apoya el uso que hace de su obra.*
- *Uso No Comercial: El material original y los trabajos derivados pueden ser distribuidos, copiados y exhibidos mientras su uso no tenga fines comerciales.*

Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra. Alguna de estas condiciones puede no aplicarse si se obtiene el permiso de Red.es como titular de los derechos de autor. Nada en esta licencia menoscaba o restringe los derechos morales de Red.es.

<http://creativecommons.org/licenses/by-nc/4.0/deed.es>

JUEGO Nº 1. ¿QUIÉN ES QUIÉN?

Ficha de consulta de la actividad

Recomendado para:

- Niños y niñas de entre 6 a 12 años.

¿Cuáles son los objetivos?

- Conocer en qué consiste la suplantación de identidad y qué formas son más frecuentes.
- Concienciar a los niños y niñas sobre el valor que tienen sus datos personales y los de otras personas, particularmente en medios digitales.
- Fomentar que los niños y niñas desarrollen una actitud consciente y activa en el control de la información personal, propia o de otras personas.
- Enseñar pautas para prevenir una posible suplantación de identidad.

¿Qué habilidades se desarrollan?

- Comunicación.
- Empatía.
- Escucha activa.

¿En qué consiste la actividad/juego?

- Visualización de web con ejemplos sobre suplantación de identidad de famosos (ídolos infantiles y juveniles).
- Reflexión sobre la gravedad de la suplantación de identidad a través de la participación en un juego de identidades.

¿Cómo trabajamos la prevención del riesgo?

- Detectando el conocimiento previo que nuestro hijo/a tiene acerca del valor que tienen sus datos personales y sobre la problemática de la suplantación de identidad.
- Proporcionándole información sobre el problema.
- Potenciando la reflexión de nuestro/a hijo/a acerca de la gravedad y las implicaciones que conlleva este riesgo TIC.

¿Qué material necesito?

- Ordenador y conexión a Internet.
- Tarjetas de papel y bolígrafos para el juego: "Quién es quién".
- Impresora para imprimir anexos (color/blanco y negro).

Otros

- Resultados esperados.
- Anexos 1 y 2.
- Más información.

Desarrollo de la actividad

Podemos comenzar la actividad preguntándole a nuestro/a hijo/a si sabe qué son los datos personales y cómo deben ser utilizados en Internet y redes sociales. Así mismo, le preguntaremos si sabe en qué consiste la suplantación de la identidad. Para poder explicarle mejor en qué consiste este fenómeno o aclararle posibles dudas al respecto, podemos apoyarnos en la información que se proporciona en el **Anexo 1**, adaptándola siempre a su edad y nivel madurativo.

A continuación, le propondremos visitar la siguiente web en Internet: <http://www.pandasecurity.com/spain/mediacenter/notas-de-prensa/justin-bieber-cristiano-ronaldo-e-isabel-pantoja-entre-los-mas-suplantados-en-twitter/>

A través de ésta, le mostraremos algunos perfiles falsos en Twitter de personajes famosos e ídolos juveniles que conoce, como Cristiano Ronaldo o Justin Bieber. Podemos preguntarle qué le parece la información que aparece en ellos, las fotos publicadas, etc. Para finalizar, le explicaremos que no se trata de perfiles creados por ellos, sino que han sido elaborados por terceras personas que han publicado información falsa, aprovechándose para ello de la fama de estos personajes. Ello nos facilitará el contexto para que podamos ampliarle a nuestro/a hijo/a la información relativa a las formas de suplantación de identidad en la red (**Anexo 2**).

Posteriormente, le propondremos la realización de un juego en familia, similar al famoso juego: “Quien es quien”, pero con algunas variaciones. Lo ideal es contar con al menos 5 jugadores.

Todos los jugadores pondrán sus nombres en un papel y tras plegarlo, lo colocarán en un lugar para que todos puedan coger uno. Tras esta primera elección, pondremos una nueva ronda de papeles, que estarán en blanco excepto uno que pondrá: “Identidad Falsa”. Todos elegirán dos papeles, lo leerán en secreto y "adoptarán" el papel de la persona que les ha tocado (si a alguien le toca ser él/ella mismo/a, volverá a escoger). A quien le toque el papel que indica: “Identidad Falsa”, deberá adoptar la identidad de algún otro personaje que elija y que no sea un miembro de la familia.

Por turnos, cada jugador le hace una pregunta al jugador que desee sobre su personaje para intentar adivinar quién es. Como los jugadores se conocen muy bien pueden formular preguntas más personales, como: ¿Cuál es tu comida favorita?, ¿vas al colegio?, etc.

Cuando un jugador cree saber el nombre del personaje de algún participante lo dice cuando le toque el turno, pero nunca después de hacer una pregunta (si lo sabe

después de preguntar una característica debe esperar a que le vuelva a tocar el turno para decirlo). Si lo adivina, la persona que ha sido descubierta queda eliminada, pero si no lo acierta, es quien ha hecho la predicción quien sale del juego.

Ganará la partida el jugador que quede en último lugar o el que identifique primero al personaje “falso”.

De forma posterior al juego, es importante reflexionar con nuestro/a hijo/a acerca de la dificultad que ha tenido poder identificar al personaje “falso”, ya que su identidad era diferente a la del resto de miembros de la familia. Podemos extrapolar estas conclusiones a la importancia de que llevemos a cabo una adecuada gestión de nuestros datos personales en la red y que podamos prevenir posibles situaciones negativas de vulnerabilidad de nuestros datos y suplantación de la identidad.

A continuación podemos leer juntos el **Anexo 3** sobre recomendaciones para prevenir la suplantación de identidad. Para hacerlo de un modo más ameno el padre o madre leerá cada punto y seguidamente el menor debe explicarle lo que significa e incluso pediremos que nos ponga algún ejemplo que podría darse. Este ejercicio ayudará a la comprensión y asimilación de las pautas preventivas.

Cómo evaluamos los resultados

- Para evaluar si nuestro/a hijo/a entiende el grado en que afecta y cuáles son las consecuencias negativas de la vulneración de nuestros datos personales y más concretamente de la suplantación de identidad, debemos asegurarnos que entiende las principales características de este riesgo TIC. Para ello, le formularemos las siguientes preguntas:
 - ¿Crees que toda la información que ves a través de Internet y las redes sociales es cierta?, ¿Le facilitarías tus claves de acceso a una web a un amigo/a que te las pida?
- Para asegurarnos que nuestro/a hijo/a se ha sensibilizado con el riesgo y que es capaz de prevenir una futura situación de suplantación de la identidad, analizaremos los comentarios y conclusiones que realiza tras su participación en el juego y observaremos qué explicación nos da de cada pauta preventiva en la parte final de la actividad.

Anexos

Anexo 1. Definición de suplantación de la identidad



(Si lo deseas, puedes imprimirlo para que te sea más cómoda su lectura)

¿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.

La suplantación de identidad en Internet en menores es 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.

Anexo 2. Formas de suplantación de identidad



(Si lo deseas, puedes imprimirlo para que te sea más cómoda su lectura)

Formas de suplantación de identidad

Las dos formas principales de suplantación de identidad entre menores 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. 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.

Anexo 3. Recomendaciones para trasladar a los menores



(Si lo deseas, puedes imprimirlo para que te sea más cómoda su lectura)

Los datos personales son aquellos que pueden servir para identificarnos en un contexto determinado.

Hay que tener en cuenta que, quizás, un dato aislado en un determinado momento o contexto no es suficiente para identificar a una persona. Sin embargo, si existen otros datos en otros lugares de la Red y es posible relacionarlos entre sí, pueden llegar a identificar a la persona. En ese caso, la privacidad se puede ver comprometida si terceras personas usan esa información sin nuestro conocimiento con intenciones de gastarnos una broma, reírse un rato, obtener un beneficio, etc. Aunque todos los datos personales son importantes, quizás la imagen, nuestra fotografía, es el que nos identifica con mayor claridad.

Recomendaciones a trasladar a los/as menores para evitar la suplantación de identidad

- Limita la difusión de datos personales y privados en redes sociales, juegos online, mensajería instantánea, formularios y aplicaciones.
- Configura de forma correcta las opciones de privacidad de los diferentes sitios web que frecuentas.
- Debes ser discretos 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.
- Cuenta con cuentas de usuario diferentes para cada una de las personas que utilizan el equipo compartido con contraseñas personales para regular el acceso a éste, cuando compartas ordenador con amigos y sobre todo con desconocidos.
- Bloquea las ventanas emergentes.
- Haz uso de los filtros *antispam*.

- Lleva a cabo una adecuada gestión de contraseñas. Modifícalas periódicamente.
- 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 debes 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.
 - “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: debes estar seguro 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, presta 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.
- Ten cuidado con los mecanismos de recuperación de contraseñas. 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.
- 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.
- Ten cuidado con las conexión en ordenadores públicos y las redes WiFi gratis.
- Instala y habilita un cortafuegos en tu equipo.

- Actúa con cautela ya que no todos los datos que se encuentran en la web han de ser ciertos.
- Establece una contraseña para el bloqueo de la pantalla del teléfono.

Más información

Los siguientes recursos son de utilidad para ampliar el conocimiento sobre la suplantación de identidad:

Monográfico de suplantación de identidad

Marco teórico de referencia para 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.

Disponible en el portal de Chaval.es: <http://www.chaval.es>

Curso en línea Seguridad TIC y Menores

Curso de 30 horas de duración bajo metodología **MOOC** (*Massive Online Open Course* - Curso en línea masivo y abierto-) dirigido a padres y educadores. Sensibiliza sobre los riesgos a los que se enfrentan los menores en el uso de Internet y las nuevas tecnologías, ofreciendo estrategias, pautas y recomendaciones para su prevención y respuesta en caso de producirse un incidente. Contiene un módulo exclusivo de suplantación de identidad.

Disponible en: <http://www.chaval.es>

JUEGO Nº 2. “PAPÁ Y MAMÁ TE AYUDARÁN”

Ficha de consulta de la actividad

Recomendado para:

- Niños y niñas de entre 6 a 12 años.

¿Cuáles son los objetivos?

- Dar pautas al menor sobre cómo debe actuar en un caso de suplantación de identidad.
- Ayudar al menor a identificar los indicios de suplantación de identidad.
- Fomentar una conducta preventiva desarrollando buenas prácticas en el uso de las TIC.
- Desarrollar la confianza para denunciar en caso de ser víctima de una suplantación de identidad.

¿Qué habilidades se desarrollan?

- Confianza.
- Comunicación.
- Escucha activa.

¿En qué consiste la actividad/juego?

- Recorrer el tablero de juego en el que se identificarán tres tipos de casillas: personas a las que debemos recurrir, indicios para sospechar de una suplantación de identidad y pautas para prevenir el riesgo.

¿Cómo trabajamos los mecanismos de actuación del riesgo?

- Informando sobre el concepto de suplantación de identidad.
- Dando a conocer los indicios que nos ayudan a identificar una suplantación de identidad.
- Haciendo hincapié en la importancia de hablar con un adulto ante cualquier sospecha de suplantación.

¿Qué material necesito?

- Ordenador y conexión a Internet.
- Impresora para imprimir el tablero (color).
- Una ficha de color diferente por cada jugador.
- Un dado

Otros

- Resultados esperados.
- Anexos 1 y 2.
- Más información.

Desarrollo de la actividad

Antes de comenzar el juego conceptualizaremos el riesgo, de modo que nuestro/a hijo/a conozca qué es la suplantación de identidad. Tomamos de referencia la información del **Anexo 1**.

A continuación comenzamos el juego, primero imprimiremos el tablero del **Anexo 2** y explicamos las reglas:

El mecanismo del juego es similar al Juego de la Oca. Los participantes se sitúan en la casilla de SALIDA y deben ir avanzando en las casillas del juego, para ello tirarán los dados y avanzarán tantas casillas como indique el número del dado.

- Cada vez que caigan en una casilla de peligro –Naranjas- (son casillas que nos hacen pensar que han suplantado nuestra identidad, es decir, reflejan indicios de suplantación de identidad) deben retroceder dos casillas.
- Cada vez que caigan en una casilla animada avanzarán dos casillas más. En este caso se hace referencia a una persona a la que pueden recurrir para denunciar. Ejemplo: Papá, Mamá, Hermano/a mayor o amigos.
- El resto de casillas hacen referencia a conductas adecuadas para prevenir el riesgo de suplantación. Por ello, cuando se caiga en ellas se deben leer y asegurarnos de que el menor entiende esa pauta de prevención. Ganará el jugador que llegue antes al centro del tablero LLEGADA.

A través del juego nuestro/a hijo/a identificará aquellos indicios que nos lleven a pensar que están suplantando nuestra identidad y se concienciará que ante cualquier indicio deben avisar a un adulto responsable.

Cómo evaluamos los resultados

Para evaluar si nuestro/a hijo/a sabe qué hace en caso de ser víctima de suplantación de identidad y si tiene suficiente confianza en nosotros para denunciar, al terminar el juego debemos preguntar: ¿qué harías si alguien se hace pasar por ti o por otra persona para engañarte a través de Internet? Su respuesta debe ser: acudir a un adulto (mamá, papá, mi profesor/a, mi hermano/a mayor...).

Para comprobar que nuestro/a hijo/a lleva a cabo pautas para prevenir el riesgo debemos repasar con él las pautas que se facilitan en el juego (casillas blancas) y confirmar si las está llevando a cabo.

Para saber si nuestro/a hijo/a sabe cómo detectar que alguien está suplantando su identidad le preguntaremos directamente ¿cómo sabrías que alguien se ha hecho pasar por ti?

Anexos

Anexo 1. Definición de suplantación de la identidad



(Si lo deseas, puedes imprimirlo para que te sea más cómoda su lectura)

¿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.

La suplantación de identidad en Internet en menores es 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.

Anexo 2. Tablero de juego



(Recomendada impresión a color)

SALIDA	1. No todos los datos de la red son verdaderos	2. Encuentro una foto en mi perfil que yo no he publicado	3. Modifica periódicamente tus contraseñas	4. Configuración correcta en mis cuentas		5. Ser discreto al publicar fotografías	6. Un servicio que no es activado me envía un mensaje al móvil
17. Bloquea ventanas emergentes		18. Haz uso de los filtros <i>antispam</i>		19. Evito enlaces disfrazados	20. Examinó los enlaces, por si están disfrazados, antes de acceder		7. Confirmando que los correos llegan a mi cuenta
16. "Piensa antes de publicar"	26. El ordenador de clase tiene una sesión para cada usuario		27. Evito acceder a enlaces sospechosos	28. Tengo más puntos en un juego online desde mi último acceso	LLEGADA ¡¡HAS GANADO!!	21. No hago caso de mensajes tipo "tu cuenta está a punto de ser eliminada"	8. Siempre cierro la sesión de mi equipo
15. No difundir mis datos personales		25. Tengo cuidado al conectarme a redes WiFi	24. No hago caso de mensajes tipo "Es urgente que actúes"	23. Tengo contraseña de acceso al teléfono, además del PIN		22. Siempre descargo los <i>plugins</i> oficiales para los juegos	9. Tengo precaución cuando utilizo ordenadores públicos
	14. Mi vecina dice que le he etiquetado en una foto y yo no he sido	13. Adecuada gestión de contraseñas		12. No puedo acceder a mi cuenta, alguien ha cambiado mi contraseña	11. Tengo cuidado con los mecanismos de recuperación de contraseñas	10. Mi amigo me dice que ayer le envié un mensaje y no es cierto	

Más información

Los siguientes recursos son de utilidad para ampliar el conocimiento sobre la suplantación de identidad:

Monográfico de suplantación de identidad

Marco teórico de referencia para 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.

Disponible en el portal de Chaval.es: <http://www.chaval.es>

Curso en línea Seguridad TIC y Menores

Curso de 30 horas de duración bajo metodología **MOOC** (*Massive Online Open Course* - Curso en línea masivo y abierto-) dirigido a padres y educadores. Sensibiliza sobre los riesgos a los que se enfrentan los menores en el uso de Internet y las nuevas tecnologías, ofreciendo estrategias, pautas y recomendaciones para su prevención y respuesta en caso de producirse un incidente. Contiene un módulo exclusivo de suplantación de identidad.

Disponible en: <http://www.chaval.es>