SUPLANTACIÓN DE IDENTIDAD
PARA EDUCACIÓN PRIMARIA

Guía Didáctica

6

¿QUIÉN ES QUIÉN EN LA RED?

Suplantación de Identidad

PROGRAMA
EDUCATIVO
Foro
Nativos
DIGITALES

JUNTA DE EXTREMADURA

Todos los materiales del Programa Educativo **Foro Nativos Digitales** han sido creados por los siguientes componentes del **Grupo de Sotware Educativo de Extremadura (GSEEX)**:

Manuel Benítez Benítez
Cristina Blázquez Buenadicha
Alfonso Gaspar Hernández
Ricardo Málaga Floriano
Francisco Muñoz de la Peña Castrillo
Mª del Mar Paredes Maña
Arturo de Porras Guardo
Fco. Javier Pulido Cuadrado
Mª Milagros Rubio Pulido
Francisca Sánchez González.

Coordinados por Francisco López Blanco.

Contacto: nativosdigitales@educarex.es

Secretaría General de Educación

JUNTA DE EXTREMADURA

Consejería de Educación y Empleo

Mérida, noviembre de 2015.

FICHA TÉCNICA

Unidad Didáctica 6: ¿QUIÉN ES QUIÉN EN LA RED?

Justificación

De forma genérica podemos afirmar que la suplantación de identidad consiste en el uso de información personal para hacerse pasar por otra persona con el fin de obtener un beneficio propio. En Internet, esta práctica es cada vez más frecuente entre los jóvenes, y cada vez a edades más tempranas, por lo que se hace necesario que desde la escuela formemos en su prevención.

Objetivos

- Conocer qué es la identidad digital y cómo pueden suplantarla en la Red.
- Concienciar al alumnado sobre la importancia de controlar sus datos personales en la Red.
- Desarrollar el sentido crítico a la hora de confiar en la información de Internet.
- Aprender a configurar contraseñas seguras.

Contenidos

- Identidad digital y datos personales.
- Prevención de situaciones que favorecen la suplantación de identidad en la Red.
- Conductas digitales que vulneran la intimidad de las personas.
- Consejos para crear contraseñas seguras.

Destinatarios

Educación Primaria (6º curso)

Edad 11 - 12 años

Metodología

Potenciar el papel activo de los alumnos, favoreciendo su participación e implicación en todas las actividades, a través de diferentes agrupamientos.
El docente tendrá que moderar las sesiones, facilitar ejemplos para familiarizar a los alumnos con las actividades, orientar en la búsqueda de soluciones, actuar como guía y como animador para incentivar que los alumnos comuniquen sus opiniones, experiencias, necesidades, etc.
La actividades propuestas están interrelacionadas entre sí, pudiéndose adaptar según los intereses del grupo. El docente también puede flexibilizar las sesiones reduciendo o ampliando actividades, así como adaptando las existentes, según convenga.

Recursos

Pizarra digital o cañón proyector, conexión a Internet, vídeo didáctico, material fotocopiable, papel y lápiz.

Materiales de apoyo

La **presentación** servirá al profesor como instrumento para dinamizar las sesiones y suscitar el interés del alumnado, fomentando también su participación.
El dossier con **materiales complementarios** contiene referencias de recursos útiles para anticipar o profundizar en el tema, a través de actividades con los alumnos, que podrán realizar tanto desde el ámbito escolar como familiar.

Temporalización

2 sesiones de tutoría (45-60 minutos cada sesión).
En cada actividad, los tiempos previstos son orientativos.

Evaluación

El docente irá tomando conciencia del proceso de aprendizaje de los alumnos a través de la evaluación continua. Se valorará el nivel de implicación, motivación e interés del alumnado sobre la temática, mediante el desarrollo de las dinámicas establecidas y la observación directa del profesorado.

¿Qué es la suplantación de identidad?

Esta información ha sido recopilada de Red.es. "Monográfico Suplantación de Identidad". En *Chaval.es* [documento en línea: http://www.chaval.es/chavales/sites/default/files/Monografico%20Suplantacion%20de%20identidad_Red.es.pdf ; acceso 19 de noviembre de 2015].

La suplantación de la identidad digital, objeto de esta guía didáctica, tiene lugar cuando una persona malintencionada se apropia indebidamente de la identidad digital de otra, actuando en su nombre con distintas intenciones. Entendemos por identidad digital el conjunto de información que sobre un individuo está expuesta en Internet: datos personales, imágenes, registros, noticias, comentarios, etc.

Algunos **ejemplos** de suplantación de identidad son: registrarse en una red social con los datos de otra persona, acceder sin consentimiento a una cuenta ajena, publicar información en la Red en nombre de un tercero, etc.

Formas de suplantación de identidad en menores:

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 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.

Recomendaciones a los 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 discreto a la hora de publicar fotografías y vídeos en la web.
- Lleva a cabo una adecuada gestión de contraseñas. Modifícalas periódicamente.
- 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

- Ten precaución con las descargas que realizas: desconfía de remitentes desconocidos en correos y no abras ficheros adjuntos sospechosos.
- En el caso de juegos en línea, procura entrar en páginas oficiales.
- No accedas a enlaces online que resulten sospechosos
- Sé precavido cuando utilices dispositivos tecnológicos de forma compartida.
- Ten cuidado con las conexión en ordenadores públicos y con las redes Wi-Fi gratis.
- Bloquea el ordenador y cierra las sesiones al terminar de usar el equipo, como medida para "cerrar la puerta" a cualquier persona ajena al mismo.
- Bloquea las ventanas emergentes.
- Haz uso de los filtros antispam.
- Instala y habilita un cortafuegos en tu equipo.
- Mantén el antivirus actualizado en todos los dispositivos tecnológicos.

¿Cómo actuar en caso de suplantación de identidad?

- Denunciar 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 esta vía. El segundo paso, si tras denunciar los hechos al servicio el problema no se soluciona, sería interponer una denuncia ante las propias 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 de la Oficina de Seguridad del Internauta (OSI): "¿Cómo denunciar una suplantación de identidad en Internet?"

  https://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.
- Contactar con los buscadores que están enlazando a esa información para evitar la indexación a la misma.
- Denunciar el caso a la Agencia Española de Protección de Datos (AEPD): C/ Jorge Juan, 6 - 28001 Madrid. Teléfono: 901 23 31 44. Whatsapp: 616 172 204. Email de Canal Joven: canaljoven@agpd.es
- 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.
- 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):

https://www.policia.es/org_central/judicial/udef/bit_alertas.html

Correo electrónico (consultas genéricas): delitos.tecnologicos@policia.es

Correo electrónico (pornografía infantil): denuncias.pornografia.infantil@policia.es

Teléfonos: 915.822.751/752/753/754/75

Guardia Civil (Grupo de Delitos Telemáticos)

www.gdt.guardiacivil.es/webgdt/home_alerta.php

Teléfono: 900.101.062 (Oficina de atención al ciudadano)

Actividad 1:
SIGUIENDO TUS HUELLAS

Objetivo: familiarizar a los alumnos con el concepto de identidad digital.

Tiempo previsto: 20/25 minutos.

Desarrollo: **(diapositiva 5)** para conocer el concepto de "identidad digital" vamos a proponer un símil entre nuestra identidad física y nuestra identidad digital. Los alumnos, de forma individual, anotarán en un papel tres rasgos de tipo físico, tres rasgos de tipo psicológico y tres aficiones, gustos o intereses que les identifiquen. Tendrán por duplicado esta información (dos papeles o notas), de tal modo que cada alumno custodiará su información personal en un papel, y el otro papel, que será anónimo (no se indica nombre ni apellidos de ningún alumno), se incluirá en una bolsa.

Posteriormente el profesor reparte aleatoriamente esos papeles anónimos entre los estudiantes, y estos deben averiguar a qué compañero corresponden esas identidades analizando la información escrita. Cada alumno anota en el papel que ha recibido el nombre y apellido del compañero de clase al que cree que corresponde la información, pudiendo equivocarse o no. Posteriormente, en gran grupo, se leen todas las identidades para comprobar si la relación identidad-nombre es correcta o no. Para realizar adecuadamente estas comprobaciones, los alumnos utilizarán el papel que han estado custodiando desde el principio.

Tras esta actividad, se abre un debate de reflexión entre docente y alumnos, planteando las siguientes cuestiones:

1. En la Red, ¿compartes información personal tuya como fotografías vídeos, intereses, aficiones, nombre, dirección, nº de teléfono, email, información escolar, etc.?
2. ¿Pueden identificarte en la Red siguiendo el rastro de tu información personal?
3. ¿Puedes tú identificar fácilmente a tus amigos según la información personal que comparten ellos?, ¿cómo lo haces o podrías hacerlo?

Ampliación: para ayudar a que los alumnos conozcan cuáles son los datos personales, el profesor puede lanzar aleatoriamente ejemplos de datos que son personales y datos que no lo son, con el fin de que los alumnos los cataloguen de forma adecuada. El profesor debe incidir en la importancia de saber qué datos personales publicamos o no en la Red, dado que es una forma de dejar nuestro rastro, con el peligro de que en Internet la información puede perdurar años.

Ejemplos de datos personales y datos no personales:

Datos personales

- El nombre y los apellidos
- El domicilio
- El nº de DNI
- El nº de teléfono
- Fecha de cumpleaños - edad
- Dirección de correo electrónico
- El nº de la Seguridad Social
- La imagen (vídeos, fotografías)
- Matrícula del coche
- Dirección IP
- La voz
- Datos escolares: centro educativo, nivel, profesor
- Datos familiares: etnia, raza, nivel sociocultural...
- Datos de salud: enfermedades, pruebas médicas, tratamientos…
- Datos financieros: cuentas corrientes, tarjetas de crédito…
- Datos laborales: salario, categoría profesional, afiliación sindical…
- Gustos y aficiones
- Huellas dactilares

Datos NO personales

- Una marca de móvil
- Un código de barras de un producto que consumo
- Una entrada de cine
- El modelo de coche
- Un videojuego
- El nombre de una bebida
- Un ticket de compra
- El modelo de ordenador
- Tipo de gafas
- La marca de ropa
- El modelo de videoconsola
- Un cartucho de tinta para la impresora
- Un libro de texto

Ayuda para el docente

¿Qué es un dato personal?

La Ley Orgánica 5/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD) establece que un dato de carácter personal es cualquier información concerniente a personas físicas identificadas o identificables. Persona identificable es aquella cuya identidad puede determinarse, directa o indirectamente, mediante cualquier información referida a su identidad física, fisiológica, psíquica, económica, cultural y/o social.

Es importante **proteger los datos de carácter personal**, y ser precavidos al utilizarlos, especialmente en la Red, por diferentes motivos: dicen quiénes somos y cómo somos, facilitan que contacten con nosotros, pueden sugerir nuestra procedencia u origen, pueden revelar aficiones, preferencias y hábitos de consumo, pueden revelar información del entorno personal, etc. Y por ello pueden utilizarse con finalidades que no hemos previsto, que pueden resultar desagradables o perjudiciales, como es el caso de la suplantación de identidad.

Recomendamos consultar el enlace "Tú decides en Internet": http://www.tudecideseninternet.es/agpd1/ de la Agencia Española de Protección de Datos, con recursos interactivos, fichas didácticas, información y materiales complementarios para que los educadores (padres y profesores) puedan trabajar los riesgos asociados a la identidad digital de los menores.

Actividad 2:
DISFRACES VIRTUALES

Objetivo: reflexionar sobre el peligro de asumir una identidad falsa en la Red.
Tiempo previsto: 20/25 minutos.

Desarrollo: **(diapositiva 6)** la Red permite que las personas puedan "enmascarar" su verdadera identidad digital, mintiendo sobre los datos que publican y/o registran en Internet, incluso haciéndose pasar por otros. ¿Crees que toda la información que ves a través de Internet y las redes sociales es cierta? ¡Ten cuidado, porque no lo es!

Por parejas, los alumnos simularán comportarse asumiendo la identidad de otra persona (por ejemplo, un famoso o personaje de ficción), a través de comentarios y acciones propias del personaje seleccionado. El otro compañero de la pareja debe averiguar de qué famoso o personaje se trata: ¿es o no relativamente fácil suplantar la identidad de otros?

Tras esta actividad de *rol-play*, el docente puede ejemplificar casos de famosos que han sido suplantados en la Red.

El debate posterior puede encauzarse con las siguientes preguntas:

1. ¿Alguna vez han mentido en Internet? (Por ejemplo, facilitar una fecha de nacimiento falsa para poder loguearse en una red social o juego online).
2. ¿Se pueden identificar fácilmente las mentiras en la Red? ¿Y a quién miente?
3. ¿Qué peligros conlleva mentir en la Red?

Ampliación: puede proponerse el diseño de un montaje, por escrito, publicando algo en nombre de otra persona, es decir, haciéndose pasar por otro a través de comentarios, publicación de datos personales del suplantado, etc. Estos montajes pueden ser anónimos dentro del grupo-clase, para comprobar a posteriori la dificultad o facilidad de desenmascarar a los farsantes que están detrás de dichos montajes.

Ayuda para el docente

Ejemplos de suplantación de identidad de famosos:

"Justin Bieber, Cristiano Ronaldo e Isabel Pantoja, entre los más suplantados en Twitter":
http://www.pandasecurity.com/spain/mediacenter/notas-de-prensa/justin-bieber-cristiano-ronaldo-e-isabel-pantoja-entre-los-mas-suplantados-en-twitter/

"Los famosos sufren usurpaciones de identidad en Facebook y Twitter":
http://www.que.es/ultimas-noticias/espana/201106062052-famosos-sufren-usurpaciones-identidad-facebook-cont.html

"Famosos suplantados en Twitter: las cuentas falsas y los peligros de las redes sociales":
http://www.zoomnews.es/142765/actualidad/tecnologia-y-ciencia/peligros-las-suplantaciones-twitter-y-facebook

Actividad 3:
PICAR EL ANZUELO

Objetivo: concienciar a los alumnos sobre la necesidad de ser precavidos al compartir sus datos personales en la Red.

Tiempo previsto: 15/20 minutos.

Desarrollo: **(diapositivas 7 y 8)** seguramente que en Internet has visitado páginas o servicios donde debes facilitar algunos de tus datos personales. Debes saber que compartir esos datos entraña una serie de peligros para ti, como es el hecho de que con ellos pueden suplantar tu identidad digital. Por eso debes ser precavido al hacerlo. A continuación vas a leer una serie de mensajes en los que debes facilitar datos personales, para que señales la conveniencia de hacerlo o no: ¿cuándo picarás el anzuelo?

- Para jugar online de forma gratuita rellena el cuestionario y acepta.
- Si eres mi amigo, me pasarás tu usuario y contraseña de Rayuela.
- Dale a mamá/papá los datos que te pida para crear tu cuenta de Play.
- Esta app requiere acceder a tus datos personales, fotos, listado de contactos, etc.
- Incluye un número de cuenta bancaria para finalizar la compra, ¡enhorabuena!
- Un amigo me pide permiso para compartir una fotografía donde salgo en una red social en la que tiene 22 amigos.
- Me voy a suscribir a mi revista favorita de videojuegos, solo tengo que dar mi correo electrónico.
- Mi compañero quiere conocer una web chulísima donde hay que registrarse y me pide mis claves para ver de qué va.
- Puedo descargarme gratis una aplicación de mi juego favorito si antes facilito nombre, apellidos, fecha de nacimiento, dirección postal y teléfono.
- Te llega un mensaje a tu email para que cambies las claves porque se ha detectado una conexión extraña.
- Etc.

Actividad 4:
PUEDE QUE SÍ O PUEDE QUE NO

Objetivo: identificar situaciones que vulneran la intimidad de las personas.

Tiempo previsto: 15/20 minutos.

Desarrollo: **(diapositivas 9 y 10)** hay muchas acciones digitales que suponen un daño o peligro para la intimidad de las personas. En una escala del 1 al 4, los alumnos señalarán cuáles de estas situaciones son menos o más peligrosas, teniendo en cuenta que el 1 indica poco peligro y el 4 un peligro extremo. Además de las situaciones planteadas, hay muchas otras que pueden suponer un ataque para la intimidad de los demás, ¿qué otros ejemplos se te ocurren?

PUEDE QUE SÍ / PUEDE QUE NO

	1	2	3	4
Me roban la contraseña y acceden a mi correo				
Tengo precaución cuando utilizo los equipos del colegio, dado que son públicos				
Un amigo ha estado en mi ordenador y no ha cerrado su sesión de correo, podré ver todo lo que le escriben				
Saco una fotografía de mi familia en Navidad				
Facilito todos los datos necesarios en una app para el móvil				
Dejo que un compañero me pase de nivel en un juego online en el que estoy registrado				
He subido la foto de un amigo en una web pública				
Cuando navego por Internet tengo la webcam tapada				
Siempre cierro la sesión de mi equipo				
Siempre que puedo me conecto a redes Wi-Fi gratis				
En las fotos que subo a Internet, etiqueto a mis amigos				
Siempre descargo los plugins oficiales para los juegos				
Me preocupo por visitar páginas web con la “s” en https de la barra de dirección				

Actividad 5:
¡QUÉ TE LO HAS CREÍDO!

Objetivo: aprender a crear claves seguras para servicios de Internet que requieren credenciales de acceso.

Tiempo previsto: 20-25 minutos.

Desarrollo: **(diapositivas 11 y 12)** una clave o contraseña segura es como una puerta blindada, es decir, que dificulta que los "ladrones digitales" puedan robarte tus datos personales. Vamos a aprender a crear claves seguras para loguearnos en la Red. Algunos de los trucos que puedes utilizar son:

- Cambiar las vocales por números. Por ejemplo: a=1, e=2, i=3, o=4, u=5 (donde guitarra sería g53t1rr1).
- Emplear reglas nemotécnicas, como elegir la primera letra de cada palabra en un refrán. Ejemplo: "No hay mal que 100 años dure" = Nhmq100ad.
- Utilizar otros idiomas, como por ejemplo palabras o expresiones del inglés. Ejemplo: nickname = apodo o nombre en clave.
- Escribir palabras con las sílabas invertidas. Ejemplo: compañero = mocapeñor.

Ahora te toca a ti proponer un truco: crea una clave segura con tus reglas, ¿crees que podrán "robártela" los demás?

Para complementar la actividad, el profesor facilitará los siguientes consejos para crear contraseñas seguras en la Red:

Consejos para crear contraseñas seguras

- Nunca compartas tus claves con los demás. Nadie debe conocerlas. Una vez que las compartes dejan de ser secretas.
- Elige una contraseña fuerte y robusta: longitud mínima de ocho caracteres, que combine mayúsculas, minúsculas, números y símbolos.
- Cambia de forma periódica las claves.
- Utiliza claves diferentes en servicios diferentes.
- Evita datos que puedan conocer los demás, como fechas de cumpleaños o aniversarios, edad que tienes, tu nombre de pila, matrícula del coche, etc.
- No utilices la opción de "Recordar contraseña" en dispositivos digitales que emplean diferentes personas.

Ayuda para el docente

Oficina de Seguridad del internauta (OSI)-Contraseñas: https://www.osi.es/es/contrasenas

Bibliografía:

Para elaborar esta guía se ha utilizado material procedente de:

● Red.es. “Monográfico Suplantación de Identidad”. En Chaval.es [documento en línea: http://www.chaval.es/chavales/sites/default/files/Monografico%20Suplantacion%20de%20identidad_Red.es.pdf ; acceso 19 de noviembre de 2015].

● Red.es. “Unidades didácticas. Primaria (6-12 años). Suplantación de Identidad”. En Chaval.es [documento en línea: http://www.chaval.es/chavales/sites/default/files/Unidades%20Didacticas%20Suplantacion%20de%20identidad_Primaria_Red.es.pdf; acceso 20 de noviembre de 2015]

● Red.es. “Juegos en familia. Primaria (6-12 años). Suplantación de Identidad”. En Chaval.es [documento en línea: http://www.chaval.es/chavales/sites/default/files/Juegos%20Suplantacion%20de%20identidad_Primaria_Red.es.pdf ; acceso 20 de noviembre de 2015].

● Clan RTVE: “El consejillo - Seguridad en Internet. Consejillo 1: no facilitar datos personales por Internet” [Archivo de vídeo, disponible en: http://www.rtve.es/infantil/serie/consejillo-seguridad-internet/video/consejo1-070915w-rtve-izqmaster/3272980/ (0:49); acceso 18 de noviembre de 2015].

● Agencia Española de Protección de Datos: “Ficha didáctica 01: Los datos personales y la privacidad. Nuestros derechos y obligaciones. Principales riesgos en la Red” En Tudecideseninternet.es [documento en línea: http://www.tudecideseninternet.es/agpd1/index.php?option=com_content&view=article&id=63&Itemid=119 ; acceso 20 de noviembre de 2015].

Agradecemos a sus autores la posibilidad de usarlos.