



CIBER EXPERT@



FORMACIÓN EN EL USO
SEGURO DE INTERNET

SÉ INTELIGENTE, CONVIÉRTETE EN CIBEREXPERT@



Tema 4

Suplantación de Identidad



www.ciberexperto.org
seguridadescolar@policia.es

organiza



apoya

Telefonica



SUPLANTACIÓN DE IDENTIDAD

OBJETIVOS DEL TEMA

Hacer uso de las tecnologías de la información y la comunicación puede conllevar ciertos peligros, especialmente para los menores. Uno de ellos es la suplantación de identidad.

El objetivo del tema es sensibilizar y concienciar al menor sobre el fenómeno de la suplantación de identidad en internet:

- Qué es.
- Formas de suplantación.
- Posibles motivos.
- Problemas que puede causar.
- Técnicas para llevarlo a cabo.
- Prevención.
- Contraseñas seguras.
- Actuación ante un caso.

Ayudar a que el menor adquiera una serie de habilidades y conocimientos que le ayude a protegerse de la suplantación de la identidad y a saber actuar en el caso de que ésta se produzca.



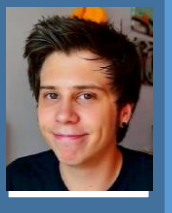


1. SUPLANTACIÓN / USURPACIÓN

Cuando se habla de **suplantación de identidad**, existe la obligación de definir dos conceptos diferentes: la creación de perfiles falsos y la **usurpación del estado civil**.

Hablamos, en ambos casos, de que se pretende enmascarar la identidad real, de las distintas maneras posibles. Lo que define si esa actitud llega o no a ser delito, es la intención detrás de los actos. En el caso de que se cree un perfil falso en una red social con un nombre y apellidos que no concuerdan con los reales, no tiene necesariamente que significar que exista una intención de hacerse pasar por otra persona, sino que simplemente se pretenda proteger los propios datos personales. Si la información aportada es inventada, no sería delito, ya que no se pretende hacer uso de los derechos de nadie.

Sin embargo, cuando existe una apropiación de la identidad de otra persona y el usurpador hace uso de los derechos y obligaciones que corresponden únicamente al usurpado, se trata de **usurpación del estado civil**, delito recogido en el artículo 401 del Código Penal.

| Perfil Falso | Copia del nombre | Suplantación |
|--|---|---|
|  <p>NOMBRE: Simpático</p> <p>APELLIDO: Rodríguez</p> <p>OCUPACIÓN: Jugador de tenis.</p> |  <p>NOMBRE: Rubén</p> <p>APELLIDO: Rubius</p> <p>OCUPACIÓN: Profesor de música.</p> |  <p>NOMBRE: Rubén</p> <p>APELLIDO: Rubius</p> <p>OCUPACIÓN: YouTuber.</p> |

A pesar de lo recomendable que sería que los menores no utilizaran sus verdaderos datos en las redes sociales, la gran mayoría, en sus Condiciones de Uso, aclaran que no estarán permitidos los perfiles falsos, así que podrán ser eliminados por la plataforma si esta los detecta (por medio de comprobaciones aleatorias o por la denuncia de otros usuarios).



2. CÓMO Y POR QUÉ SUPLANTAR UNA IDENTIDAD



Accediendo a la cuenta del usuario.

- El usurpador debe conseguir las claves de acceso.
- Acceden a la información privada.
- Pueden usar el acceso para acosar, humillar, desprestigiar...



Crear perfil falso (con información del suplantado).

- El usurpador debe recopilar información sobre la persona usurpada y crear una cuenta.
- Cuanta más información consiga (nombre, apellidos, edad, fotos...), más creíble será la usurpación.

Para obtener las claves que permitan entrar en las cuentas ya creadas, existen multitud de fórmulas de conseguir las contraseñas. Existen un tipo de software o programa, llamado **de fuerza bruta**, que hace un rastreo de las contraseñas empleando bases de datos con diccionarios de distintos idiomas. También hay estafas planeadas para obtener nuestros datos.

Phishing: envío de mensajes que, aparentando provenir de fuentes fiables, intentan obtener tus datos confidenciales.

- Por ejemplo, un mensaje que aparenta ser de Facebook: *“Tu cuenta será desactivada porque ha sido denunciada. Para evitar la desactivación debes acceder a este link e introducir tus datos”.*

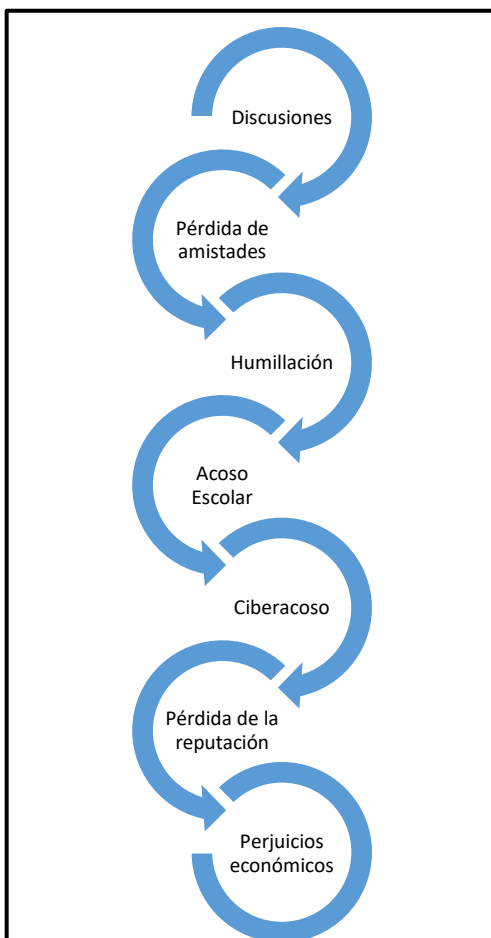
Pharming: infectar el ordenador del usuario y redirigirle automáticamente a otras páginas web falsas creadas por el delincuente imitando el aspecto de las originales que suele visitar la víctima. De esta manera se obtienen los nombres y contraseñas de acceso.

Spoofing: el atacante simula la identidad de otra máquina, con la que la víctima tiene establecido algún tipo de confianza (basada en el nombre o la dirección IP) para conseguir acceso a sus recursos.

- Por ejemplo, utilizando una dirección IP falseada.



3. CONSECUENCIAS



Los menores no son conscientes no sólo del daño que pueden hacer a sus compañeros suplantando su identidad, sino que la mayoría de las ocasiones ni siquiera saben que este hecho está penado por la ley.

La suplantación de identidad es la primera arma que las personas malintencionadas pueden esgrimir contra los usuarios de Internet. Puede ser el daño planeado en sí, o puede convertirse en la puerta de entrada para muchos otros problemas: grooming, ciberacoso, estafas, etc.



4. DÓNDE DENUNCIAR SUPLANTACIÓN EN RR.SS.

- Denunciar suplantación en Facebook
(<https://es-es.facebook.com/help/181495968648557>)
- Denunciar suplantación en Twitter
(<https://support.twitter.com/forms/abusiveuser>)
- Denunciar suplantación en Google+
(<https://support.google.com/plus/answer/1253377?hl=es>)
- Denunciar suplantación en LinkedIn
(<https://www.linkedin.com/help/linkedin/safety/report-a-problem>)
- Denunciar suplantación en Snapchat
(<https://support.snapchat.com/es/i-need-help>)
- Denunciar suplantación en Instagram
(<https://es-es.facebook.com/help/instagram/547601325292351>)
- Denunciar suplantación en Badoo
(<https://badoo.com/es/help/?section=89>)
- Denunciar suplantación en Flickr
(<https://www.flickr.com/abuse>)
- Denunciar suplantación en Pinterest
(<https://help.pinterest.com/es/articles/report-something-pinterest#Web>)

Si tras denunciar los hechos el problema no se soluciona, puedes interponer una denuncia ante las Fuerzas y Cuerpos de Seguridad del Estado.



5. CIBER CONSEJOS

Prevenir

- 1 • Uso de contraseñas robustas.
- 2 • Conocer los métodos más comunes para acceder a nuestros perfiles.
- 3 • Mantener una buena configuración de privacidad.
- 4 • No compartir vídeos o fotos comprometedoros.
- 5 • Revisar las condiciones de uso del servicio al que se acceda.
- 6 • Evitar publicar datos personales o sensibles.
- 7 • Usar antivirus, antimalware y antispam.
- 8 • Utilizar un sistema de doble autenticación (confirmación mediante SMS).
- 9 • No dejar las sesiones en correos o redes sociales abiertas.
- 10 • Activar el bloque de pantalla en el teléfono móvil.



Actuación ante un caso

- 1 • Contárselo a un adulto de confianza.
- 2 • Denunciar en el lugar correspondiente (sitio web, servidor de correo, red social...)
- 3 • Si se hace necesario, denunciar en la Agencia Española de Protección de Datos (AEPD)
- 4 • Si el problema persiste, acudir a las Fuerzas y Cuerpos de Seguridad del Estado para denunciar los hechos.