SOCIEDAD

374 días en prisión

La identidad en las redes sociales

Libelo 2.0

Los adolescentes crean cada vez más perfiles falsos para dañar reputaciones

El cierre de una cuenta fraudulenta puede tardar de un día a más de un mes

ALBA G. LAGUNA
MADRID

La suplantación de identidades en las redes sociales está a la orden del día. Es fácil, barata y rara vez tiene consecuencias para el suplantador, aunque sus efectos pueden resultar devastadores para el que la sufre. Desde la atalaya de un perfil falso se puede insultar y criticar a todo el círculo de amistades del afectado, así como subir fotos que este no desea hacer públicas y hacer comentarios que lo dejen en evidencia o manifiesten una actitud arrogante. Cosas que harán que los contactos (estos sí, reales) que tienen acceso a su perfil se vuelvan en su contra.

El año pasado, la suplantación fue uno de los principales motivos de las denuncias relacionadas con internet investigadas por la Agencia Española de Protección de Datos (AEPD). Algunas de ellas se habían producido en páginas de contactos. Es uno de los casos más frecuentes. También los de exempleados dolidos con sus antiguos jefes y los de profesores que sufren en versión 2.0 las burlas de sus alumnos, que antes se limitaban al aula o al recreo. Porque los reyes indiscutibles de la suplantación son, con diferencia, los adolescentes.

DENUNCIAR ES IMPORTANTE // Lo confirma Juan Salom, jefe del grupo de delitos telemáticos de la Guardia Civil, quien destaca además la importancia de denunciar estas situaciones. Esto es poco habitual, ya que se suelen percibir como chiquilladas. «Pero en realidad se está cometiendo un delito», recuerda. Concretamente, el artículo 401 del Código Penal castiga la «usurpación de estado civil» con penas de seis meses a tres años de cárcel. Y apunta también que «quien recibe mensajes que en realidad no iban dirigidos a él está vulnerando el secreto de comunicaciones».

Como explica Jorge Flores, director de la fundación Pantallas Amigas, una entidad que promueve el uso seguro de internet, «se trata de una manera relativamente sencilla de hacer mucho daño a una persona, porque genera una reacción hostil de todo el entorno. Con el tiempo puedes lograr explicar que no eras tú, pero para entonces la reacción en contra ya se ha producido y deshacerla es bastante duro».

cuentas reales

GARANTÍA SOLO PARA FAMOSOS

CELEBRIDADES EN TWITTER

➲ Alejandro Sanz, Mariano Rajoy, Barack Obama, Shakira, Gerard Piqué, Andreu Buenafuente… ¿Qué tienen en común estas personas? Son conocidas por el gran público, sí. Y también se han apuntado a la red social de mensajes cortos Twitter, una de las más utilizadas por los internautas. Pero no solo eso.

CUENTAS VERIFICADAS

➲ En sus casos, la propia compañía garantiza la identidad de quién está detrás del canal de Twitter mediante lo que se conoce como cuentas verificadas, que aparecen marcadas con un distintivo junto a la imagen del perfil. Para llevar a cabo esa verificación, la compañía contacta con la persona en cuestión y certifica que es quien asegura ser.

FAMOSOS SUPLANTADOS

➲ Algunos suplantados ilustres han sido la Moncloa, los futbolistas del Real Madrid Iker Casillas (cuyo perfil falso llegó a contar con más de 260.000 seguidores) y Cristiano Ronaldo, la escritora Lucía Etxebarría y el hasta hace unos días presidente de la SGAE, Teddy Bautista. De Andrés Calamaro, justamente uno de sus principales defensores en el escándalo de desvío de fondos de la entidad de gestión, hay al menos dos cuentas que dicen ser las oficiales. Ninguna tiene el estatus de verificada.

MECANISMOS DE CONTROL

➲ La Agencia Española de Protección de Datos (AEPD) solicita que las empresas establezcan más mecanismos de seguridad para evitar este tipo de casos, no solo cuando se trate de famosos, porque «una suplantación de identidad puede suponer un daño extraordinario para la víctima».

El experto en seguridad informática Chema Alonso asegura que «abrir un perfil falso es facilísimo». Con una simple foto y algo de información, como el centro de estudios o la ciudad de residencia, se puede crear un perfil creíble en un cuarto de hora. Nadie va a pedir que se pruebe que se es quien se dice ser, razón por la que también abundan los perfiles falsos que no se corresponden con ninguna identidad real. Sin embargo, cerrarlos requiere algo más de tiempo.

CIERRE DEL PERFIL // Ante la dificultad de prevenir estas situaciones y la imposibilidad para las redes sociales de comprobar todas y cada una de las altas que se registran cada día, todos los expertos consultados destacan la importancia de contar con buenos mecanismos de denuncia. El fenómeno no se ceba solo con personas físicas. Asociaciones, partidos políticos y empresas también son susceptibles de ser suplantados. Les ha ocurrido, entre otros, a la Moncloa y al partido navarro Nafarroa Bai.

Estas páginas suelen contar con formularios para denunciar la usurpación de identidad, en los que piden datos básicos, aunque para el cierre efectivo de un perfil solicitan por lo menos la presentación del DNI en pasos posteriores. El cierre puede llevar desde 24 horas hasta más de un mes, según las particularidades del caso y de la red social en la que se ha producido el problema.

ACEPTAR AMIGOS CON CUIDADO // Tuenti, que recibe cada día cerca de 10.000 denuncias de perfiles –de las que 800 aproximadamente acaban en la clausura de la cuenta–, es la que mejor responde. Al ser una empresa radicada en España, está sujeta a las leyes españolas, más estrictas. Suele tardar uno o como máximo dos días desde la denuncia. Una vez acreditada la suplantación, se limita a cerrar el perfil, aunque conserva toda la información que contenía por si se inicia una investigación judicial y le es requerida en el futuro.

María de Sousa-Valadas, mánager de soporte a usuarios de la empresa, da algunos consejos para curarse en salud: «Aceptar solamente peticiones de amistad de personas a las que conoces de verdad. Así evitas que desconocidos se hagan con tus fotos y tengan material para crear un perfil falso a tu nombre». ≡

Condenadas dos chicas a pagar 12.800 € por suplantar a una amiga en Tuenti

►► La Audiencia de Segovia impuso hace mes y medio 12.400 euros de indemnización y una multa de 400 a dos jóvenes por los problemas psicológicos que causaron a una antigua amiga al crear un perfil falso suyo en Tuenti. Utilizaron su nombre, fecha de nacimiento y centro de estudios y subieron una foto de la víctima con un amigo, por lo que «nadie dudaría de la autenticidad del mismo». Durante cinco meses, socavaron la autoestima y las relaciones sociales de la víctima al llamarla «friqui» a ella o «niñatas» y «payasas» a sus amigas. También subieron 56 imágenes con comentarios que la ridiculizaban.

►► Esta actuación, según recoge la sentencia, provocó «una reacción en cadena» contra la suplantada, que causó «su aislamiento total del grupo». Su círculo social le retiró la palabra y el saludo. Todo ello produjo en la víctima un «trastorno ansioso depresivo moderado» que la tuvo bajo tratamiento médico durante más de un año. Los tribunales condenaron a las dos acosadoras al considerar que sus actos eran constitutivos de una falta continuada de vejaciones injustas. Este es un caso extremo, pero poco a poco se empiezan a conocer nuevas resoluciones judiciales por asuntos similares.

WW123RF

menores desprotegidos

INICIO TEMPRANO

96% de los jóvenes de entre 12 y 16 años poseen un perfil en una red social. La edad media para iniciarse en estas plataformas es de 13 años, pese a que en general no pueden acceder a ellas los menores de 14.

INFRAVALORAN EL RIESGO

79% de las personas que utilizan las redes sociales dicen no haber sentido nunca su intimidad atacada, lo que choca con que el 45% conoce a alguien que sí ha tenido una experiencia contraria en este sentido.

PROTECCIÓN INSUFICIENTE

3 de cada 10 jóvenes han pedido alguna vez a los administradores que eliminen una foto, un grupo o un comentario. Según la UE, solo dos redes sociales protegen por defecto la intimidad de los menores.

las denuncias de los usuarios

MÁS QUEJAS

168 investigaciones relacionadas con la web llevó a cabo en el 2010 la Agencia Española de Protección de Datos. Entre los motivos principales se encontraba la suplantación de identidad.

DIFICULTAD DEL CIERRE

24 horas se tarda en clausurar una cuenta, en el mejor de los casos. Sin embargo, suele ser bastante más. En función de la red social y del canal utilizado para denunciar pueden ser hasta varios meses.

Los menores suplantados no piden ayuda

El robo de identidad tiene los efectos psicológicos más duros en los adolescentes

A. G. L.
MADRID

Estrés, ansiedad, depresión, bajada del rendimiento académico. Los efectos de la suplantación de identidad en los menores presentan un alto grado de coincidencia con los del acoso cibernético. Después de todo, no deja de ser una de sus modalidades. Y es que las nuevas generaciones están al otro lado de la brecha digital. Se manejan casi con más soltura en la red que en la vida diaria y parte de sus relaciones sociales se desarrollan ahí, en los chats, en los muros y los grupos de Facebook. Parecen todo ventajas, pero también tiene sus inconvenientes. Los adolescentes son quienes más sufren la suplantación en las redes sociales y, por lo general, no solo no son conscientes del riesgo, sino que no se atreven a pedir ayuda.

LOS AMIGOS, BÁSICOS // «Para ellos los amigos son fundamentales», cuenta Raquel García, psicóloga especialista en infancia y adolescencia. Los reales, pero también los virtuales. El deseo de contar con un gran número de contactos en su lista mueve a muchos a agregar o aceptar solicitudes de amistad sin control, lo que incrementa los riesgos.

«Se trata de un acoso constante, ya que todo el rato se están generando mensajes negativos, no solo en momentos concretos. Esa falta de momentos de paz causa un gran estrés al menor. Además, el anonimato del suplantador agrava la sensación de impunidad. Al no saber contra quién dirigir su enfado, la confianza del niño cae en picado, lo que redunda en tendencia al aislamiento, ansiedad e incluso depresión», añade. Y esos problemas acaban afectándole en otros ámbitos, como la familia o los estudios: «Los adolescentes tienden a pensar que las cosas solo les pasan a ellos, lo que aumenta su sensación de soledad y les bloquea a la hora de buscar ayuda».

ASIGNATURA PENDIENTE // Petra María Pérez, catedrática de Teoría de la Educación de la Universidad de Valencia y miembro del observatorio para la convivencia escolar y contra la violencia, subraya que las razones para este tipo de acoso son variopintas. «Cuando les preguntas por qué lo han hecho, algunos contestan que porque la víctima saca buenas notas, va de chulo o es nuevo. No existe un patrón». También destaca que es un comportamiento más común entre las chicas que entre los chicos: «Ellos recurren más a la fuerza».

Miguel Comín, director de la Fundación Alia2, que combate la pornografía infantil y el ciberacoso, insiste en que el control de la intimidad en las redes sociales es «la asignatura pendiente». «La gente –agrega– no está acostumbrada a protegerse y con frecuencia deja todos los contenidos abiertos, de manera que queda totalmente expuesta».

Análisis

Jaime **Delgado**
CATEDRÁTICO DE LA UPC

Hay soluciones, pero no se aplican

Para atajar el problema hay que cambiar el funcionamiento, lo que supone cambiar el modelo de negocio

Pocos pueden discutir hoy en día las múltiples ventajas de las redes sociales, centradas sobre todo en facilitar la comunicación rápida y flexible dentro de grupos de personas, sean pequeños o grandes. Pero también son conocidos los problemas que pueden generarse si no se usan adecuadamente y no se toman las debidas precauciones.

Es muy frecuente tener en estas redes muchos *amigos*, es decir, personas que están al corriente de tu vida: lo que haces, lo que piensas, tus planes, tus gustos, etcétera. También tus amigos verán lo que otros te dicen. Un comentario inoportuno o desafortunado puede claramente perjudicar a más de una persona. Y todo esto ¡sin intención de hacer daño!

¿Qué más puede pasar? El siguiente nivel de problemas es cuando alguien quiere perjudicar a otro públicamente y sin esconderse. Un insulto, una difamación, descubrir algo secreto o íntimo, lo puede hacer cualquier conocido. Si lo hace a través de una red social, el efecto maligno se multiplica llegando rápidamente a todos sus *amigos*. Luego está la credibilidad de lo divulgado, pero esta es otra cuestión. El primer daño puede estar hecho.

Pasemos ahora a los ataques encubiertos, es decir, aquellos en los que el atacante intenta esconderse. De entre todos los posibles, concentrémonos en la suplantación de personalidad. Esta puede hacerse básicamente de dos maneras. En la primera, el suplantador accede a una cuenta existente de otra persona y, haciendo creer a los demás que es el suplantado, publica información o vierte comentarios para dañarle. El mecanismo que use el suplantador para obtener acceso a la cuenta es otro tema, pero hay muchas formas de *robar* (o perder por descuido) una contraseña, que es básicamente lo único que se necesita.

La segunda manera de llevar a cabo una suplantación requiere que la víctima no tenga cuenta en la red social donde se comete el ataque. Cualquiera puede darse de alta tomando otra personalidad, que puede ser la de una persona que existe. Lamentablemente, en este caso (en aras de simplificar el acceso), los proveedores de redes no verifican los datos cuando un usuario se da de alta.

Recursos tecnológicos

La última cuestión es esta: ¿qué puede hacer la tecnología para evitar estos problemas? La realidad es que la tecnología ya dispone de soluciones, pero el problema es que para aplicarlas se deben cambiar los modelos de funcionamiento, que implican cambios de modelo de negocio en los proveedores y cambios de comportamiento en los usuarios, lo que no siempre es fácil.