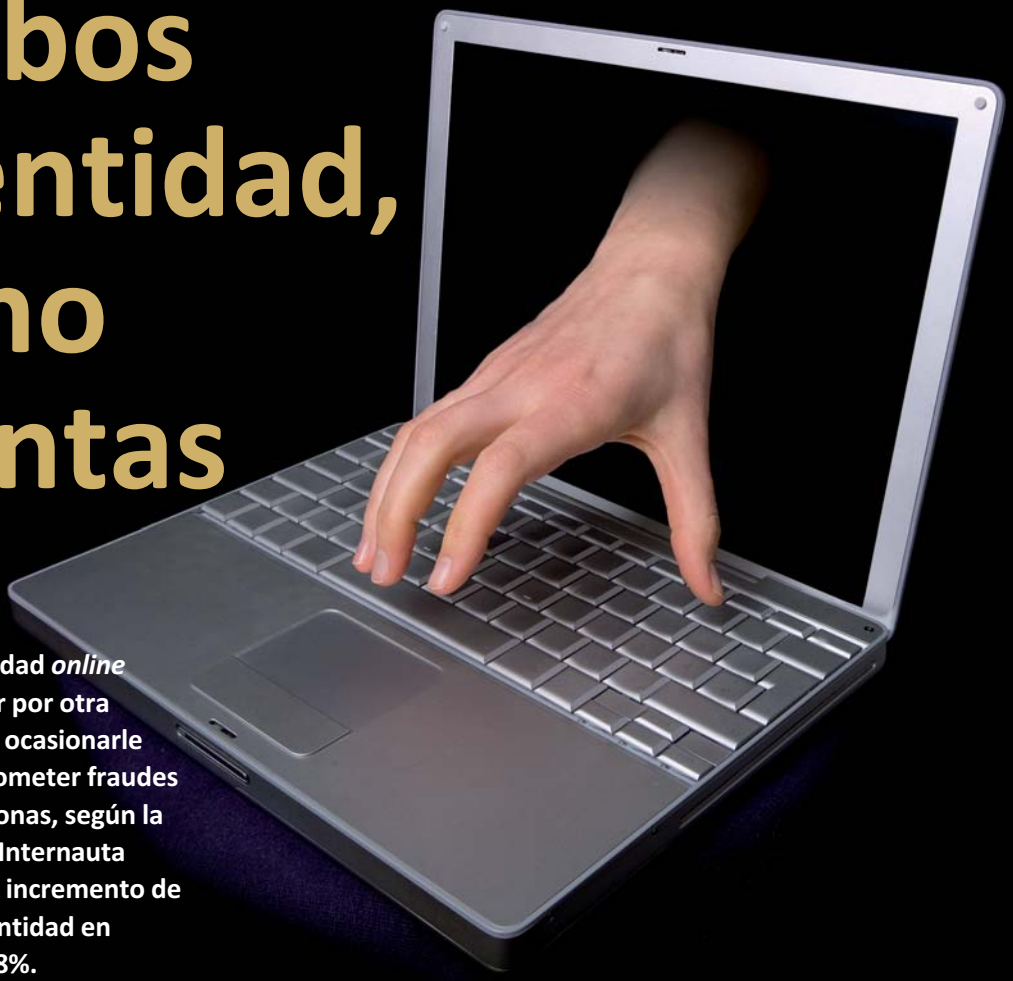
Los robos de identidad, en ocho preguntas



La suplantación de identidad *online* consiste en hacerse pasar por otra persona en internet para ocasionarle una molestia o daño, o cometer fraudes en nombre de otras personas, según la Oficina de Seguridad del Internauta (OSI), que subraya que el incremento de los casos de robos de identidad en internet ha subido un 178%.

LUIS MENÉNDEZ
luis.menendez@yahoo.es

¿Quién puede ser víctima? Aunque pueda parecer que el blanco principal de estas prácticas son personajes de la vida pública, cualquiera que tenga información personal publicada en internet –nombre, apellidos, edad, lugar de nacimiento, fotografías– puede ser objeto de una suplantación de identidad. Incluidas entidades. Recientemente la propia OSI fue objeto de estas prácticas con el objetivo de lograr credenciales de sus usuarios. El método seguido era el envío por un supuesto técnico de la OSI de mensajes para comunicar una infracción de los términos y condiciones de algún servicio, solicitando datos personales, contraseñas o avisando de la notificación de una multa.

¿Cómo se lleva a cabo? Generalmente, el robo de identidad *online* se lleva a cabo accediendo a la cuenta del usuario, para lo cual el atacante tendría que conseguir las claves de acceso de la víctima, adivinándolas o mediante técnicas de ingeniería social para adquirir información confidencial fraudulenta, también conocidas como *phishing*. Otra forma de hacerlo es crear un perfil falso con la información personal de la persona suplantada a partir de información recopilada en internet.

¿Es delito? Hay que tener en cuenta que en función de la conducta utilizada para robar la identidad de una persona podría hablarse incluso de delito. Si la suplantación consiste únicamente en el registro de un perfil falso en el que no se utiliza información personal del suplantado, no se considera delito y la única acción legal que puede tomarse es notificar esta situación a la red social implicada para que elimine dicho perfil de su página.

Por el contrario, en el caso de que alguien acceda a la cuenta de otro usuario y se haga pasar por él, se trata de un hecho denunciable al tratarse de una conducta que vulnera la privacidad de la víctima y porque el ciberdelincuente habría cometido un doble delito, ya que la obtención de las credenciales de acceso implica el uso de una práctica ilícita.

Cualquiera que tenga información personal publicada en internet puede ser objeto de una suplantación de identidad

La creación de un perfil falso en el que

se suplanta la identidad de otra persona utilizando para ello datos como su nombre, fotos, o edad, constituye una vulneración del derecho a la propia imagen recogido en el artículo 18 de la Constitución Española. En este caso se estaría produciendo una usurpación de la identidad de una persona, lo que podría ser penado por la ley con penas de cárcel según el artículo 401 del Código Penal.

¿Puedo reducir el riesgo? Existen varias formas de reducir los riesgos de sufrir un robo de identidad, como elegir una contraseña robusta que contenga al menos 8 caracteres y esté compuesta por mayúsculas, minúsculas, números y caracteres especiales ($, &, #...). No es aconsejable utilizar ejemplos débiles y fáciles de adivinar como 12345678, qwerty, aaaaa, o nombres de familiares. Tampoco lo es utilizar la misma contraseña en varios servicios y mucho menos compartirla con otras personas.

Una herramienta importante es siempre el conocimiento y conocer las prácticas de *phishing* puede ser de gran ayuda. Estos intentos de robo pueden llegar a través de correos electrónicos, mensajes SMS, MMS o por mensajería instantánea. Hay que ser cauto ante correos que simulan proceder de entidades bancarias y nos advierten de incidencias técnicas, problemas de seguridad, descuentos o regalos. También conviene estar alerta ante la llegada de mensajes que contengan errores gramaticales o insten a tomar una decisión en un corto espacio de tiempo.

Otros consejos de interés son configurar el perfil en las redes sociales con el mayor nivel de privacidad posible, no compartir fotos o vídeos comprometedores que puedan ser utilizados para extorsionar a las víctimas, y revisar la política de privacidad y las condiciones del servicio al que se está accediendo para conocer qué hace la red social con los datos, cómo los tratan y almacenan y si los comparten con terceros, etc.

Identity theft (robo de identidad)

17.600.000 estadounidenses, es decir un 7% de los residentes mayores de 16 años en los Estados Unidos fueron víctimas en 2014 de algún tipo de robo de identidad digital, según las estadísticas oficiales publicadas por la Oficina Estadística de la Justicia (http://www.bjs.gov/). Dos terceras partes sufrieron daños financieros. Se trata del delito más frecuente y costoso desde el punto de vista económico de los que se cometen el país, con una estimación total anual que supera los 50.000 millones de dólares. El problema afecta no solo a los ciudadanos, también a las empresas, en buena parte como consecuencia del acceso *online* de la información a los Registros mercantiles sin control de la autenticidad de los datos que se inscriben. Otros países con un sistema jurídico similar al de Estados Unidos padecen la misma lacra. Es el caso de Australia o el del Reino Unido. Lo advierten en este último algunas páginas web, como la del propio Registro http://cort.as/uKAY o la del Royal Bank of Scotland http://cort.as/uKAk.

Existen varias formas de reducir los riesgos de sufrir un robo de identidad, como elegir una contraseña robusta que contenga al menos ocho caracteres

¿Qué hago si me pasa? Si una persona tiene conocimiento de que ha sido objeto de una suplantación de identidad en el marco de una red social debe dirigirse a esa plataforma para reportarlo. Estas poseen enlaces a través de los cuales puede denunciarse esta situación. Si pese a la acusación el problema persiste pueden denunciarse los hechos ante las Fuerzas y Cuerpos de Seguridad del Estado, para lo cual es necesario aportar alguna evidencia de que se está siendo víctima de una suplantación, por ejemplo, una captura de pantalla del perfil falso; si se recoge en acta notarial constituirá una prueba irrefutable. La creación de un perfil falso en una red social con datos personales de la persona suplantada constituye un tratamiento de datos sin el consentimiento del titular, por lo que también cabe acudir a la Agencia Española de Protección de Datos (AEPD) para poner en su conocimiento los hechos.

¿Y si es en el mundo *offline*? El mundo *offline* también está expuesto a las suplantaciones de identidad. La AEPD ha alertado de que la contratación irregular en servicios de telecomunicaciones mediante suplantación de identidad, que a menudo suele desembocar en una inclusión indebida en ficheros de morosidad, preocupa especialmente a los ciudadanos y es uno de los motivos más frecuentes por los que reclaman ante la agencia. De hecho, el sector de las telecomunicaciones aglutina más de la mitad de las sanciones que el organismo impone al año y uno de los principales ámbitos de reclamación ante las organizaciones de consumidores.

Por ello, la AEPD y el Consejo de Consumidores y Usuarios han llevado a cabo recientemente una acción conjunta para concienciar a los ciudadanos de cuáles son sus derechos en materia de privacidad y el uso de sus datos, có-

mo exigirlos y ante quién si son víctimas de este tipo de abusos.

En este sentido, ambas instituciones recuerdan que el primer paso es presentar una denuncia ante la Policía Nacional o la Guardia Civil por presunto fraude en la contratación y aconsejan enviar una copia de la misma a la compañía que presta el servicio, solicitando que cancelen sus datos. Asimismo, indican que si como consecuencia de la suplantación al afectado se le estuviera exigiendo el pago de una deuda, este puede reclamar ante las Juntas Arbitrales de Consumo, presentar una reclamación ante la oficina de atención al usuario de telecomunicaciones o acudir a la vía judicial.

En el caso de que el ciudadano tenga constancia de que sus datos han sido incluidos en un fichero de morosidad por negarse a abonar ese servicio, recuerdan que este deberá dirigirse al acreedor exigiendo la cancelación de sus datos, y si pese a haberlo solicitado continúa figurando en el fichero de morosidad, puede solicitar la tutela de la agencia. Existe otra opción de denunciar la suplantación de identidad ante la AEPD, para lo cual es preciso indicar el servicio cuya contratación se le atribuye, el número de línea asociada y añadir una copia de la reclamación enviada a la compañía.

¿Esto lo cubre el seguro? En 2016 las empresas españolas sufrieron 2,8 ciberataques de media al año, con pérdidas valoradas en 1,4 millones de dólares, según recoge la Encuesta Mundial sobre el Estado de la Seguridad de la Información de PwC. En este contexto no es de extrañar que hayan surgido *ciberpólizas* que ofrecen coberturas ante el robo o pérdida de información de usuarios o de la empresa, pérdidas de beneficios provocadas por fallos en los sistemas informáticos o ciberamenazas en los pagos electrónicos.

¿Me puede suplantar un *software*? La amenaza de suplantación de identidad no solo puede proceder de atacantes de carne y hueso sino también de programas informáticos. Un grupo de investigadores del University College London ha desarrollado un *software* capaz de reproducir la escritura humana, que puede ser utilizado para falsificar documentos, con el consiguiente riesgo a la hora de aceptar documentos con firmas o textos manuscritos en una causa jurídica.

La solución si existen dudas sobre la veracidad de una prueba pasa por solicitar un estudio pericial que certifique la autoría original de una forma o documento manuscrito. Respecto a la forma del texto o firma, el perito calígrafo Rafael Martín considera que la creación de un texto presentaría dificultades insalvables porque "a un mismo grafema no se le da el mismo diseño según en qué posición de la palabra se encuentre".

En relación con la formación, otro aspecto gráfico sustancial, el experto recuerda que en la generación de los manuscritos, sean firmas o textos, hay que tener en cuenta dónde ejercen presión los dedos con el útil y durante cuánto recorrido; en qué zonas de los grafismos se produce; cómo se sostiene el útil de escritura; con qué rapidez se ejecutan cada uno de los elementos constitutivos de los grafemas y, finalmente, qué características de todo ello quedan registradas en los trazos. A todo esto hay que añadir que no se tiene siempre el mismo tono muscular y que el ánimo puede variar notablemente de un día a otro e incluso en muy breve plazo.

"Hasta saber si este sistema informático podría reproducir los matices dinámicos de los dedos, creo que el análisis de un manuscrito creado así solamente podría tener visos de credibilidad en una apreciación somera, pero sin lugar a dudas un peritaje descubriría su origen espurio", considera Martín.●

Y en Twitter, ¿qué opinan?

Policía Nacional La usurpación de identidad en #RedesSociales no es una broma, puede ser un DELITO. Si eres víctima, #Denuncia

INCIBE La suplantación de identidad en Internet es algo muy técnico, no lo puede hacer cualquiera… ¿o sí? vía @is4kids

Guardia Civil Intentos de suplantación de identidad en medios sociales, haciéndose pasar por @osiseguridad. Para más información: https://www.osi.es/es/actualidad/avisos/2017/02/nos-intentan-suplantar-para-robar-credenciales…

Artico Consultores Artico Consultores @ArticoSLL
Consejo de Consumidores y Usuarios y la AEPD nos recuerdan cómo actuar ante una suplantación de identidad en… http://www.portalartico.es/consejo-de-consumidores-y-usuarios-y-la-aepd-nos-recuerdan-como-actuar-ante-una-suplantacion-de-identidad-en-servicios-de-telecomunicaciones/ …

En 2016 las empresas españolas sufrieron 2,8 ciberataques de media al año, con pérdidas valoradas en1,4 millones de dólares

Generalmente el robo de identidad *online* se lleva a cabo accediendo a la cuenta del usuario.

VÍCTOR DOMINGO,
presidente de la Asociación de Internautas

presidente@internautas.org
www.facebook.com/victor.domingo
@victordomingo

¿Por qué es importante salvaguardar nuestra identidad digital?

UNO DE LOS DELITOS QUE MÁS se están prodigando en la Red en los últimos tiempos en el mundo digital es el robo de identidad o usurpación de identidad. Es decir: la apropiación de la identidad virtual de una persona por un tercero en sus distintas categorías, cómo hacerse pasar por esa persona; asumir su identidad ante otras personas en público o en privado, en general o para aprovechar ciertos recursos como el acceso a la cuenta corriente bancaria, o la obtención de créditos o contratación de servicios y/o productos en nombre de la personalidad robada.

Otro supuesto de usurpación de identidad, posiblemente no delictivo, pero muy engorroso y perjudicial para la imagen, es el utilizado con el fin de perjudicar a una persona, es decir, difamarlo o manchar su nombre con diversos fines que el usurpador busque. En cualquier caso lo más común en estos últimos tiempos se da cuando un tercero, por medios informáticos o personales, obtiene información personal y la utiliza ilegalmente.

Con el mundo digital se han cambiado las tornas, pues si en el mundo físico cuando alguien robaba la cartera o los documentos de identidad la utilización de estos valores tenía unas consecuencias limitadas, en el mundo digital este hecho que se limita al acto de robar determinadas claves de acceso al correo electrónico, cuentas bancarias o acceso al perfil en las redes sociales, cobra una importancia inusitada porque la presencia física y virtual van de la mano a la hora de acceder a un sinfín de prestaciones de servicios y productos por el mero hecho de que el ladrón no tiene que hacerlo presencialmente.

Uno de los más graves inconvenientes es que la persona a la que se le ha robado su identidad no se entera de que esto ha sucedido hasta que no se encuentra con las consecuencias que produce el delito cometido.

Las formas en que podemos ser víctimas del robo de nuestra identidad es mediante los correos falsos que recibimos y las técnicas denominadas de *phising*. Esta técnica hace pasar a un atacante por una organización, banco o empresa verdaderas para obtener información que garantice acceso a algún recurso que usted utilice en esa organización, banco o empresa.

Cualquier persona con malas intenciones podría obtener información que escuchó o vio de usted y que le garantice acceso a algún recurso valioso y más directamente acceso a la clave de acceso a internet en general y determinados servicios en particular.

Como forma habitual de proceder, los atacantes acceden a alguno de los servicios de los que somos clientes y utilizan directamente los recursos de esa compañía con nuestros datos personales y secretos, como puedan ser contraseñas, DNI o cuentas bancarias.

Pero ante grandes males existe una buena dosis de remedios que pueden prevenir este tipo de ataques a la identidad personal en el mundo digital y entre los que caben destacar los que recomiendan los expertos y especialmente los que ofrece la Oficina Pública de Seguridad del Internauta:

– En materia de redes sociales, hay que comprobar los contactos o validar amigos y seguidores antes de agregarlos a nuestros perfiles.

– Obligado es tener mucho cuidado con las redes WiFi públicas a las que te conectas, para no compartir datos sensibles cuando accedes a internet y por supuesto no compartir desde esos lugares archivos, fotos o vídeos comprometedores o personales.

– Tratar de que la información que se emita viaje cifrada y utilizar cuando se emita información personal solo páginas cuya URL comience por htpps.

– Prestar atención a las políticas de privacidad y las condiciones de uso de los servicios transaccionales antes de utilizarlos.

– Y muy importante es utilizar claves robustas en todos y cada uno de los servicios que utilicemos en internet. Una clave robusta tiene como mínimo 8 dígitos en los que se deben combinar números, símbolos y letras y por supuesto no compartir esas claves con nadie. Con nadie.

«Si nuestra identidad ha sido utilizada para realizar delitos es necesario denunciarlo y acompañar la denuncia preferiblemente con un acta notarial de estos hechos»

Y si después de todo nos enteramos que nuestra identidad ha sido robada y/o usurpada solo nos queda actuar de la siguiente manera:

– Si la suplantación o robo de identidad consiste en la publicación de datos personales en internet, el primer paso es dirigirse a la misma página donde estos aparecen y exigir su cancelación.

Todos los sitios web o redes sociales tienen apartados para denunciar este tipo de casos.

– Si se trata de que nuestra identidad ha sido utilizada para realizar delitos, fraudes o comportamientos deshonestos es necesario denunciarlo inmediatamente a las fuerzas de seguridad del Estado, ya sean los grupos de delitos informáticos de la Policía Nacional o de la Guardia Civil. Acompañando la denuncia con las correspondientes capturas de pantallas y preferiblemente con acta notarial de estos hechos.

– Y por último, y en función de si las consecuencias habidas en el hecho del robo y la suplantación tienen repercusión de carácter legal y jurídico, ponerse en manos de un abogado experto en la resolución de este nuevo tipo de delitos tecnológicos. En cualquier caso la extensión de este delito llama a que la ciudadanía digital, que ahora se conforma, se prevenga en buena medida para salvaguardar su identidad digital, tan importante como la identidad física tradicional.

"Salvemos nuestra privacidad"