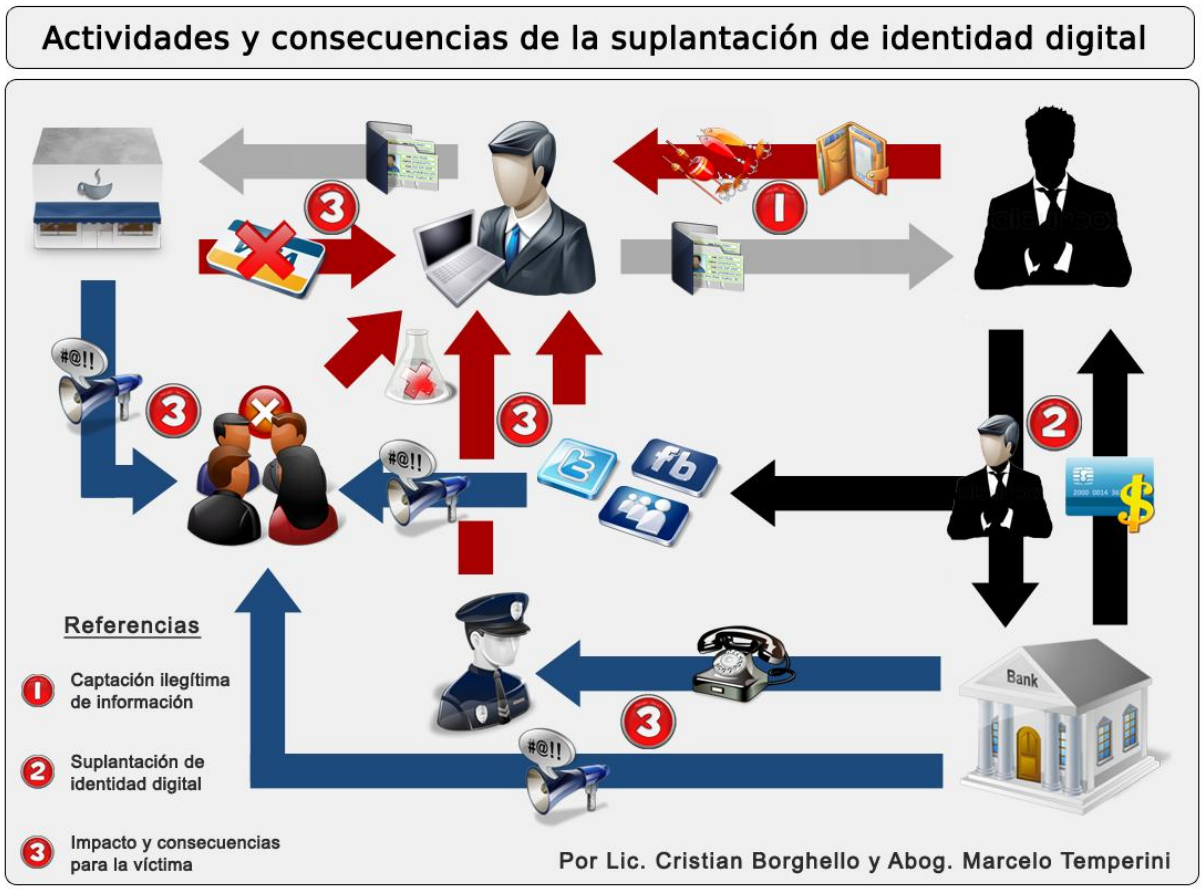
Identidad Digital

La **Identidad Digital**, puede ser definida como el conjunto de rasgos y características particulares que una persona expresa a través de internet, la cual forma una parte inescindible de la identidad personal de cada sujeto, en su faz dinámica, y más precisamente en su aspecto psicológico, social y moral. Esta identidad digital se encuentra actualmente en situación de crisis, debido a los constantes y crecientes embates por parte de ciberdelincuentes en todo el mundo.

Según la **OECD (Organización para la Economía, Cooperación y Desarrollo)** la suplantación de identidad ocurre cuando una parte adquiere, transfiere, posee o utiliza información personal de una persona física o jurídica de forma no autorizada, con la intención de cometer fraude u otros delitos relacionados.



Por definición, la identidad es aquel conjunto de rasgos propios de un individuo que lo caracteriza frente a los demás. Así, la Identidad Digital es la extensión virtual de esa personalidad, expresada y transmitida a través de los diferentes medios electrónicos. A título de ejemplo, se pueden mencionar como datos de identificación personal el nombre, apellido, documento de identidad, números o códigos de cuentas y servicios, contraseñas, datos biométricos, firmas digitales, etc.

Según el **Prof. César Valderrama**, la identidad digital es todo aquello que identifica un individuo en el entorno Web. Agrega además que la identidad digital personal, definida como la habilidad de

gestionar con éxito la propia visibilidad, reputación y privacidad en la red como un componente inseparable y fundamental del conjunto de habilidades informacionales y digitales, las cuales se han convertido en fundamentales para vivir en la sociedad informacional. De forma activa, se realiza aportando textos, imágenes y vídeos a Internet, participando, en definitiva, del mundo web. En los sitios de redes sociales se construye a partir de un perfil de usuario, que a menudo se enlaza a perfiles de otros usuarios o contactos. Una identidad digital bien gestionada y homogénea con la identidad analógica no sólo repercute en una vida más activa en todos los ámbitos sino que también tiende a consolidar un entramado social más sólido fuera de Internet.

La **Dra. en Psicología Keely Kolmes**, pionera de la "ética de los medios digitales y sociales para psicoterapeutas", advierte sobre los daños potenciales de la suplantación de de identidad online: "Esta es una forma de acoso y el estrés emocional puede conducir a la ansiedad, depresión, trastornos del sueño u otros problemas graves para el bienestar de una persona. Se podría afectar significativamente el funcionamiento diario de una persona en la escuela, el trabajo o las relaciones. También puede tener un efecto sobre la estructura social de alguien si los demás no se dan cuenta de que el individuo está siendo suplantado. "

De acuerdo a la **Home Office Identity Fraud Steering Committee**, existe cuando suficiente información sobre una identidad es obtenida para facilitar la usurpación de identidad, independientemente de si la persona está viva o ha fallecido.

En febrero de 2012, la **Federal Trade Commission (FTC)** publicó su lista sobre las quejas más comunes de los consumidores de EE.UU.5 y, por cuarto año consecutivo, el robo de identidad encabezó la lista: de **1,8 millones de denuncias presentadas en 2011, el 15% fueron sobre de robo de identidad**.

América Latina y sobre todo **Argentina**, no es ajena a estas estadísticas y la carencia de números oficiales no es excusa para evitar el problema e ignorar a la gran cantidad de personas que cada día ven afectados su honor, su reputación, su trabajo, su imagen, su salud social y psicológica y sus actividades financieras y económicas, debido a que terceros han usurpado su identidad.

Entre las raíces de este delito, se encuentra una gran facilidad en la **captación Ilegítima de datos de identificación personal**, inexistencia de legislación en la materia, falta de controles adecuados por parte de las entidades, así como los bajos niveles de educación en los usuarios en internet.

Por ello, se considera apropiado aunar esfuerzos hacia el futuro, buscando la defensa de los usuarios afectados, buscando que se considere a la identidad digital como un bien jurídico protegido. En este sentido, existe una propuesta legislativa para tipificar en Argentina el delito de suplantación de identidad digital, así como el de la captación u obtención ilegítima de datos confidenciales (phishing). Para más información sobre los textos, ingresa a la sección **Proyecto**.

Qué hacer si te roban la identidad

Por Daniel Monastersky

Aunque no existe ningún método que le asegure a usted que nunca será víctima de robo de identidad, los siguientes consejos pueden ayudar a minimizar su riesgo.

- Lleve consigo solamente las tarjetas que necesita. Minimice los documentos de identidad y el número de tarjetas de crédito que lleva en su cartera o billetera. No lleve consigo su DNI, a menos que sea necesario.
- Nunca escriba información sobre sus cuentas en la parte exterior de un sobre o de una postal.
- Corte sus tarjetas de crédito antiguas o vencidas. Cierre todas las cuentas bancarias o de tarjetas de crédito inactivas. Aunque usted no las utilice, estas cuentas aparecen en su informe crediticio y podrían ser utilizadas por ladrones.
- Escoja un PIN para la tarjeta que utiliza en el cajero automático que no sea su dirección, número de teléfono, segundo nombre, los últimos cuatro dígitos de su número de DNI, su fecha de nacimiento o cualquier otro tipo de información que pueda descubrir un ladrón.
- Memorice su PIN; no lo escriba en su tarjeta de cajero automático, ni lo ponga en un pedazo de papel en su billetera. Las estadísticas han demostrado que en muchos de los casos de fraude de tarjetas de cajero automático, los dueños de las tarjetas habían escrito su número de identificación personal en la tarjeta de cajero automático o en alguna hoja de papel que habían guardado en sus carteras o billeteras.
- Mantenga sus datos personales en un lugar seguro. Si usted emplea a alguien o está realizando arreglos de reparación en su casa, mantenga sus datos personales en un lugar escondido.
- Proporcione su número de DNI solamente cuando sea absolutamente necesario. Pregunte, siempre que sea posible, si puede utilizar algún otro número de identificación.
- No divulgue sus datos personales por teléfono, por correo o Internet, a menos que usted haya iniciado el contacto o que conozca la empresa con la cual está hablando.
- Compare los recibos de su cajero automático y los cheques cambiados con sus estados de cuenta bancarios para percatarse de cualquier transferencia o cargo no autorizado.
- Disminuya el número de solicitudes de tarjetas de crédito no solicitadas que recibe. Mientras menos solicitudes de tarjetas de crédito usted reciba, menos posibilidades tendrá de que le roben una. Póngase en contacto con la entidad bancaria para que su nombre sea eliminado del mailing.
- Pregúntele a su banco sobre su política de privacidad y las prácticas de uso de sus datos personales. Averigüe bajo qué circunstancias su banco podría proveer la información de su cuenta a terceros.
- Pida una copia de su informe crediticio por lo menos una vez al año para revisar si aparece alguna actividad fraudulenta o sospechosa. Esta información la puede solicitar de forma gratuita en periodos no inferiores a seis meses.
- No responda a los mensajes electrónicos o de aparición automática (pop up messages) mediante los que le soliciten información personal o financiera ni haga click sobre los vínculos o enlaces incluidos en estos mensajes. No utilice la función copiar y pegar (cut and paste) para colocar el domicilio de un enlace en el navegador de Internet — los “pescadores de información” o phishers pueden lograr que los vínculos aparenten llevarlo a un sitio Web pero en realidad lo conectan a uno diferente.

- Si está preocupado sobre la seguridad de su cuenta, comuníquese con la empresa utilizando un número de teléfono que le conste como genuino o abra una nueva sesión de navegación en Internet y escriba usted mismo el domicilio Web correcto de la compañía.
- Use programas antivirus y firewall y manténgalos actualizados.
- No envíe información personal ni financiera por correo electrónico.
- Revise los estados de cuenta de sus tarjetas de crédito y cuentas bancarias tan pronto como las reciba para verificar si le han imputado cargos que usted no ha autorizado.
- Tenga cuidado al abrir archivos electrónicos adjuntados o al descargar archivos de emails recibidos, independientemente de la identidad del remitente.

Si bien usted no puede controlar completamente la posibilidad de ser damnificado por el robo de identidad, sí es posible minimizar su riesgo siguiendo algunos pasos. Si un ladrón de identidad está abriendo cuentas a su nombre, muy probablemente estas cuentas aparezcan en su informe crediticio. Usted tiene la posibilidad de detectar en forma temprana un incidente si solicita periódicamente una copia gratuita de su informe crediticio en cualquiera de las empresas que brindan este tipo de servicio.
El derecho de acceso a que se refiere este artículo sólo puede ser ejercido en forma gratuita a intervalos no inferiores a seis meses (Art 14, Ley 25.326 de Protección de Datos Personales).

- Sepa con quién está tratando. Cualquiera puede poner un comercio en Internet bajo cualquier nombre falso. Confirme el domicilio real y el número de teléfono del vendedor que opera en línea para utilizarlos en la eventualidad de que surgieran preguntas o problemas. Si no hay una manera de identificar al responsable (teléfono, email, CUIT, CUIL), no brinde ningún tipo de información. Si recibe un mensaje de correo electrónico o un pop-up mientras que está navegando en Internet, mediante el cual le solicitan información financiera, no responda al mensaje ni haga click sobre el enlace incluido en éste. Las compañías que operan legítimamente no solicitan este tipo de información por correo electrónico.
- Sepa exactamente qué es lo que está comprando. Lea atentamente la descripción del producto ofrecida por el vendedor, especialmente la letra chica. Los artículos de marcas renombradas que son ofrecidos a precios “demasiado buenos para ser reales” podrían ser falsificados.
- Averigüe cuánto le costará. Consulte los sitios Web que ofrecen comparaciones de precios y compare productos similares. Calcule y sume los gastos de envío y despacho — considerando sus necesidades y presupuesto — al costo total de su orden de compra. Bajo ninguna circunstancia envíe dinero en efectivo.
- Pague con tarjeta de crédito. Si usted paga con tarjeta de crédito su transacción estará protegida por el contrato que haya suscripto con su banco emisor o empresa emisora. Algunas compañías ofrecen una garantía de compras en línea que le asegura que no será responsable de pagar ningún cargo no autorizado efectuado a través de Internet, asimismo algunas tarjetas puede ofrecer una garantía adicional y beneficios de protección de devolución y/o compras.
- Verifique los términos del trato, tales como las políticas de reintegro y fechas de entrega. ¿Si estuviera insatisfecho con la compra, puede devolver el artículo y obtener un reintegro total de su dinero? Si devuelve un artículo, averigüe quién pagará los gastos de envío y despacho o los cargos de reposición de inventario y también pregunte cuándo recibirá su orden de compra.
- Conserve toda la documentación. Imprima y guarde los registros de sus transacciones electrónicas, incluyendo la descripción y precio del producto, el recibo de la compra por Internet y las copias de todos los emails que le envíe al vendedor o que reciba de éste. Revise los estados

de cuenta de su tarjeta de crédito tan pronto como los reciba y esté atento a los cargos no autorizados.

- No envíe su información financiera por e-mail. El correo electrónico no es un método seguro para transmitir ese tipo de información, como por ejemplo los datos de su tarjeta de crédito, cuenta corriente bancaria o número de DNI. Si usted inicia la transacción y quiere suministrar su información financiera a través del sitio Web de una empresa, busque indicadores que le demuestren la seguridad del sitio, como por ejemplo el ícono del candado en la barra de estado del navegador o un domicilio Web o URL que comience con "https:" (la letra "s" corresponde a "seguro").

Cómo corregir el problema

Al descubrir el robo de identidad, lo más importante es tomar medidas inmediatamente. Recuerde mantener un registro de todas sus llamadas telefónicas y otros tipos de correspondencia con compañías, en relación al fraude de identidad.

Realice la denuncia en la comisaria del lugar en el cual haya ocurrido el robo de identidad.

Siempre guarde la denuncia. Es posible que su banco, su tarjeta de crédito u otra compañía pida constancia del delito.

Si usted sospecha que su correo está siendo desviado a otra dirección, hable con su oficina de correos local para averiguar si alguien ha llenado un formulario de cambio de dirección en su nombre sin su autorización.

Llame a las compañías que emitieron sus tarjetas de crédito inmediatamente para verificar la condición de sus cuentas, si sus facturas no llegan a tiempo. Si fuera necesario, cierre todas sus cuentas. Mantenga los números de sus cuentas, las fechas de vencimiento y los números de teléfono de cada uno de los emisores de las tarjetas en un lugar seguro y separado de todas sus tarjetas de crédito, para que pueda reportar una pérdida rápidamente.

Comuníquese con su banco inmediatamente si su tarjeta de cajero automático ha sido robada o si se han efectuado transferencias o retiros no autorizados en una o varias de sus cuentas. Avísele a su banco si le han robado o no aparecen sus cheques. Cuando abra una nueva cuenta bancaria, pida que se tenga que utilizar una contraseña antes de que se puedan hacer cambios o preguntas sobre las cuentas y evite utilizar un número de identificación personal que un ladrón pueda descubrir, tal como su fecha de nacimiento o los últimos cuatro dígitos de su seguro social.

La cancelación de sus tarjetas de crédito puede impedir el uso de sus cuentas existentes por parte de los impostores, pero no los impide de poder abrir nuevas cuentas a nombre suyo. Para evitar que esto suceda, si existe la posibilidad de que sus tarjetas hayan sido indebidamente utilizadas por alguien no autorizado, comuníquese con el departamento de fraudes de cada una de las principales agencias de información crediticia y pídales que pongan una marca de aviso en su expediente, como perteneciente a una posible víctima de fraude. Este aviso también informará a los acreedores que deben llamarlo(a) a usted para obtener su permiso antes de aprobar nuevas tarjetas de crédito o préstamos a nombre suyo. Después de llamar a cada una de las tres agencias de información crediticia (incluidas en la lista de recursos de este informe), usted debería darles seguimiento por escrito. Mantenga copias de dichas notificaciones escritas.

Pídale una copia de sus informes crediticios a las agencias de información crediticia. Usted tiene derecho a recibir una copia gratis de su informe crediticio si le negaron algún préstamo recientemente o si su informe está incorrecto debido a fraude. Revise su informe cuidadosamente, para asegurarse de que no haya ningún cargo no autorizado en sus cuentas existentes y que nadie haya abierto cuentas fraudulentas o tomado préstamos a nombre suyo. En unos meses, vuelva a

pedir copias de sus informes crediticios para verificar que la información incorrecta haya sido eliminada y que no haya ocurrido más actividad fraudulenta.

Tips

Comuníquese con las principales empresas de informes de riesgo crediticio si usted descubre o sospecha que ha sido víctima de robo de identidad. Usted tiene derecho a recibir una copia gratis de su informe crediticio a intervalos no inferiores a seis meses (Art 14, Ley 25.326 de Protección de Datos Personales). http://www.ceic.org.ar/spanish/info_inst_6.html

Recursos: Federal Trade Comission
http://www.ftc.gov/bcp/edu/microsites/idtheft/en-espanol/index.html
Alerta en Linea
http://alertaenlinea.gov/articulos/s0005-robo-de-identidad
Privacy Rights Clearinghouse
https://www.privacyrights.org/spanish/pi17a.htm

Robo de identidad en internet

Facebook

Si alguien crea una cuenta para hacerse pasar por ti, puedes acceder al perfil del impostor y hacer clic en "*Denunciar/bloquear a esta persona*", marca la casilla "*Denunciar a esta persona*" y selecciona la opción "*Perfil falso*" añadiendo que se están haciendo pasar por ti e incluyendo la dirección de tu perfil para contrastar la información. Más información aquí.
Si lo que crees es que te han robado la cuenta, y están publicando cosas en tu muro, o enviando mensajes o correos no deseados, Facebook recomienda seguir ciertos pasos que se pueden consultar aquí.
Si resulta que han robado la cuenta de un amigo y lo quieres denunciar, ésta información te será útil.
En cuanto a la Seguridad en Facebook les recomendamos visitar las siguientes páginas que Facebook pone a tu disposición entre otras: *"Información para padres"*,*"Información para adolescentes"* e *"Información general sobre seguridad"*.

Twitter

¿Cómo informo de una usurpación de identidad?

Completando este formulario (en Inglés)
La información básica que tienes que incluir para informar de este robo de identidad es el nombre del usuario o URL del perfil de la persona que te esté suplantando, tus datos personales y nombre de usuario en Twitter si lo tuvieras.

Tuenti

En el caso de que alguien haya accedido a tu cuenta haciéndose pasar por ti en Tuenti, lo primero es cambiar tu contraseña en: *"Mi cuenta">"Preferencias">"Preferencias de mi cuenta">"Cambiar contraseña"*. En caso de que no puedas acceder a tu perfil Tuenti te ofrece un formulario para denunciarlo. También podrás denunciar el caso de que alguien se haya creado una cuenta haciéndose pasar por ti. Más información aquí

Hotmail / Live

Si crees que te han robado la contraseña lo primero es intentar recuperarla reseteándola. En éste post nos indican información relevante sobre cómo recuperar la contraseña de una cuenta de correo MSN y como ponerse en contacto con el personal de Microsoft. Es recomendable leer la Ayuda de Windows Live ID y Administración de cuentas

Gmail
Si crees que han accedido a tu cuenta sin autorización, Google te hará responder a un formulario para tratar de ayudarte a resolver el problema.

Linkedin
En el Centro de Ayuda de LindkedIn podrás encontrar información en caso de que hayan accedido a tu cuenta, como restablecer la contraseña o ponerte en contacto con ellos

Importante
Si crees que has sido testigo o víctima de un delito informático, puedes denunciar los hechos para que sean investigados por la División Delitos en Tecnología y Análisis Criminal (Cavia 3350, Piso 1, Ciudad Autónoma de Buenos Aires) Tel: (011) 4370-5899
Email **analisis_criminal@policiafederal.gov.ar**
Con información de GVA.es

Fuente: identidadrobada.com