SUPLANTACIÓN DE IDENTIDAD Y SU USO EN REDES SOCIALES

Liliana Leticia Limón Vidal

Egresada de la licenciatura en derecho de la Universidad Juárez Autónoma de Tabasco.

Articulo Recibido: 19 de abril 2016. Aceptado: 25 de mayo 2016.

RESUMEN. El hecho de que las redes sociales o sitios web nos pidan nuestros datos personales con la finalidad de brindar transparencia en sus resultados de búsqueda, implica que los mismos puedan ser usados por otras personas haciéndose pasar por nosotros. En inglés, estas acciones en las que se presenta la suplantación de identidad en páginas de internet y redes sociales han sido identificadas con el nombre de "phishing". Por ello, la importancia de conocer esta figura, la legislación existente, los perjuicios sociales que conlleva su realización, así como medidas importantes que todo usuario de redes sociales debe tomar en cuenta.

Palabras Clave: Phishing, Identidad, Fraude, Redes Sociales.

INTRODUCCIÓN.

En algún momento de nuestra vida conocimos a alguien que nos preguntó algo parecido a ¿usas Facebook/Twitter/MySpace/Instagram?, ¿me agregas a tu red social?, ¡compré esta blusa en Mercado Libre más barata que en el Supermercado! o bien, al conocer que estas existen, las utilizamos como medio de venta de productos o comunicación, para contactarnos y compartir contenido, noticias, promociones, eventos o acontecimientos que consideramos importantes con nuestros familiares, amigos, conocidos, o incluso clientes.

Sin embargo, hay que destacar que nadie está exento de sufrir momentos desagradables si no hacemos uso correcto de los datos que ponemos en estas redes sociales o sitios de internet. Si bien es cierto que en sitios de compra como Mercado Libre o E Bay, existen condiciones de venta para los productos y el manejo de las tarjetas de crédito cuya función es proteger las transacciones, la realidad es que en las redes sociales nadie

nos garantiza la protección de nuestros datos o un límite de publicación de los mismos.

Como consecuencia, podemos aceptar como amigo/seguidor a un desconocido cuyas intenciones sean desde las más inocentes, como buscar una amistad, unirse a una causa social que defendemos, compartir gustos musicales o deportivos, hasta otras tales como conocer el lugar en el que vivimos, utilizar nuestras publicaciones como suyas, investigar a nuestros familiares, establecer relaciones "amorosas", inclusive robar nuestras fotos.

Mientras la "relación" sea cordial y de respeto, no habrá mayor problema, pero, ¿qué sucede si dicho amigo/seguidor está utilizando su red social para hacerse pasar por mí? ¿qué pasa si se recomienda como un buen vendedor y resulta ser un estafador que utiliza mis datos para su conveniencia y me perjudica? ¿y si pienso que estoy hablando con mi amiga de la infancia y resulta ser que es otra persona que para llegar a mí, utilizó sus fotos y nombre?.

DESARROLLO.

Según la CONDUSEF, la identidad está constituida por datos personales tales como nombre, domicilio, teléfono, números de tarjetas y cuentas bancarias o de seguridad social, huellas dactilares, contraseñas y fotografías. Define al Robo de identidad como la obtención, uso o transferencia de datos personales de alguien más con la intención de asumir su identidad y realizar compras, obtener créditos, documentos o cualquier otro beneficio financiero.

El INAI tiene una útil Guía de Robo de Identidad en la que define a éste último como la apropiación de la identidad de una persona para hacerse pasar por ella, asumirla frente a terceros públicos o privados, a fin de obtener ciertos recursos o beneficios a su nombre.

Para Microsoft, la suplantación de identidad, también llamada *phishing* , es una forma de engañar a los usuarios para que revelen información, comúnmente mediante la llegada de un correo electrónico que aparentemente proviene de una fuente de confianza como un banco o un comerciante en línea, y cuyo fin es

direccionar al usuario a un sitio web que les solicita sus datos personales, que posteriormente son usados para el robo de identidad. Se refiere a datos financieros.

Al hablar de este tema, fácilmente podemos asociarlo con las actividades financieras de los afectados, sin embargo quienes se dedican a esto, no sólo afectan operaciones de crédito o bancarias. La afectación puede ser una grave consecuencia que repercuta en la reputación del individuo o su situación psicológica, y es aquí la aparición del término *grooming,* puesto que las esferas de afectación pueden llegar a magnitudes de índole sexual. El Grooming consiste en acciones realizadas por un adulto para entablar una relación amistosa o afectiva con un menor de edad con el fin de persuadirlo para obtener su confianza y así abusar de él sexualmente.

Existe la figura denominada *smishing*, parecida al phishing pero con la particularidad de llevarse a cabo mediante el uso de teléfonos celulares. Funciona por medio del envío de mensajes de texto simulando procedencia de distintas instituciones o identidades, quienes les solicitan la actualización de sus datos o la participación en promociones inexistentes.

El llamado *pharming* consiste en una técnica más complicada, puesto que se usan softwares maliciosos cuya función es conservar el nombre de la dirección original del sitio al que deseamos ingresar, pero al entrar redirecciona a otra y sin darnos cuenta ingresamos nuestros datos personales en una página apócrifa.

Quien ha visto en la televisión el controversial programa del canal MTV “Catfish” sabrá que la trama consiste en un individuo que se “enamora” de otra persona por medio de internet. Comienzan aceptando/enviando una solicitud de amistad, después continúan hablando, se cuentan sus problemas, preocupaciones, alegrías y logros, hasta que la belleza física y emocional se vuelve tan afín, que el vínculo sentimental termina siendo tan fuerte que se enamoran.

Así, con el tiempo estas personas que casi siempre están separadas por kilómetros y kilómetros de distancia, desean conocerse en persona, y acuerdan una cita. Pero el

día de la cita no se ven, y surgen increíbles pretextos.

En estas historias de amor, la mayoría de las veces al por fin verse con la persona amada, resulta ser físicamente diferente: no es quien creían que era. “María” se enamoró de “Juan el de ojos verdes, moreno y alto, con un tatuaje en el brazo”, y al verse por primera vez cara a cara, “Juan” resulta ser “Sofía”.

Si bien este tipo de situaciones son desagradables y el daño moral o emocional es grave, pocas veces se considera como un delito puesto que, como menciona el abogado Luis Madrigal Pereyra, el robo de identidad puede ser de dos maneras: como el delito en sí, o como el camino para cometer otro delito, es decir, usar la identidad de una persona y solicitar un crédito que obviamente no pagará, para así cometer el delito de fraude.

El Congreso de Jalisco publicó en su sitio oficial, un boletín en el que se daba a conocer la aprobación de reformas al Código Penal con las que se tipificaba el delito de Suplantación de Identidad a quien usando medios electrónicos o internet, se atribuya datos de alguna persona, generándole un daño moral o a su patrimonio al obtener un lucro indebido, el cual será sancionado de tres a ocho años de prisión y multa de mil a dos mil salarios mínimos. Así mismo, la pena puede agravarse si quien cometa el delito, se vale de parecido físico, similitud de voz, homonimia, licenciatura, ingeniería o cualquier grado académico dentro del rubro de la informática, computación o telemática.

En España existe la Oficina de Seguridad del Internauta (OSI) quien proporciona información para evitar y resolver aquellos problemas existentes al navegar por internet y funge como formadora en materia de ciberseguridad, concientizando a los usuarios de su responsabilidad para minimizar la incidencia y gravedad experimentadas por los usuarios.

A continuación se presentan una lista de medidas precautorias para que el lector de este artículo se mantenga informado, comparta con sus conocidos y amigos, y ponga en práctica las acciones que pueden

dificultar la exposición indebida de su identidad:

- Al abrir una cuenta personal en una computadora que sea de uso público, recuerda elegir la opción "NO" si el navegador te indica mediante una ventana emergente el recordar tu contraseña, así como cerrar la sesión correctamente una vez que hayas terminado de utilizarla.

- Utiliza contraseñas que impliquen números y letras, evitando usar datos que cualquier persona puede adivinar, tales como fechas de cumpleaños o aniversarios, así como cambiarlas con regularidad.

- Configura tus redes sociales para ocultar el contenido con personas que no formen parte de tu perfil, piensa antes de publicar cualquier tipo de información personal, no aceptes solicitudes de amistad sin previa verificación de que el perfil que aceptas es de un conocido de manera preferentemente personal.

- No tires estados de cuenta o documentos personales a la basura sin haberlos destruido con anterioridad.

- Protege el sitio donde se deposita tu correspondencia para que no pueda ser extraída de tu domicilio.

- No abras archivos adjuntos de correos electrónicos cuando provengan de un remitente desconocido para ti.

- Instala antivirus o aplicaciones de seguridad, activa contraseñas de acceso o patrones de bloqueo para acceder a tus dispositivos electrónicos.

- Mantén apagado el *Wi Fi* o *Bluetooth* cuando no lo estés utilizando.

- No publiques o compartas fotos de documentos personales.

- No guardes en tus dispositivos móviles notas de texto que contengan contraseñas o claves de acceso personal.

LITERATURA CITADA.

Referencias Citadas desde páginas Web

Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (CONDUSEF). (2015). *Robo de identidad, un delito en aumento.* Obtenido de http:// www.condusef.gob.mx/Revista/index.php/usuario-inteligente/consejos-de-seguridad/563-robo-de-identidad

Fecha de consulta el 10 de Marzo del 2016

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI). *Guía para prevenir robo de identidad.* (Enero de 2016). Obtenido de http://inicio.inai.org.mx/nuevo/Guia%20Robo%20Identidad.pdf

Fecha de consulta el 28 de Marzo de 2016

Instituto Nacional de Ciberseguridad (INCIBE). (2016). *Oficina de Seguridad del Internauta.* Obtenido de http://www.osi.es/es/quienes-somos.html

Fecha de consulta el 13 de Abril del 2016

Monastersky, D.,Salimbeni, M. (2012). *Introducción al Robo de identidad.* Obtenido de https://dl.dropboxusercontent.com/u/24286331/Robo_de_identidad.pdf

Fecha de consulta el 13 de Abril del 2016

¿Qué es la suplantación de identidad (phishing)? (2016). Obtenido de http://windows.microsoft.com/es-mx/windows-vista/what-is-phishing

Fecha de consulta el 18 de Marzo del 2016

Robo o Suplantación de Identidad, Delito que crece exponencialmente. (Agosto de 2013). Obtenido de http://www.misionpolitica.com/anteriores/columnas/tema-principal-de-la-semana/62938-robo-o-suplantacion-de-identidad-delito-que-crece-exponencialmente

Fecha de consulta el 15 de Abril de 2016