COLEGIO DE ESPECIALISTAS EN DERECHO DIGITAL, CIBERSEGURIDAD Y CIBERCRIMINOLOGIA A.C

Marzo|4|2024

Por
Dr. Daniel Alberto Garza de la Vega[1]

Estadística aplicada a la suplantación de Identidad a través de medios electrónicos. Caso Redes Sociales.

Uno de los tópicos que han ido en aumento en la última década, es la suplantación de identidad a través de medios electrónicos. Según la Business Insider el 22% de los usuarios de internet en México fueron víctimas de alguna vulneración de seguridad en 2022 (Cueto, 2023).

Otra estadística alarmante es que el 22.1% de los internautas en México han sido víctimas de alguna vulneración de seguridad en los últimos 12 meses, según un estudio de la Asociación de Internet MX. Entre las principales vulnerabilidades que sufrieron los internautas mexicanos están el fraude y pérdida financiera, la suplantación de identidad y el robo de información. En cuanto a ciberataques, 20.2% de los internautas mexicanos dijo haber sido víctima de phishing, mientras que 8.1% de ransomware.

Otras estadísticas importantes a considerar el por qué de la alza de lo mencionado en supra líneas, es que, el número de usuarios en México con acceso a internet llegó a 88.6 millones durante el 2021, lo que equivale a 75.6 % de la población de seis años o más. El tiempo promedio de uso de internet al día en México durante el 2021 fue de 4.8 horas por persona. Los principales usos de internet fueron para comunicarse, buscar información y acceder a redes sociales (Cueto, 2022).

Con respecto a las actividades típicas y antijurídicas realizadas por medios electrónicos tenemos que las principales vulnerabilidades que sufrieron los internautas mexicanos están el fraude y pérdida financiera (46.5%), seguidas por la suplantación de identidad (27.3%) y el robo de información (22.2%). Todo esto lo debemos también a la cultura de la doble autenticación[2] y la higiene digital en el uso de contraseñas a

---

[1] Abogado especialista con más de 15 años de experiencia en Derecho Digital y Ciberseguridad. Ha realizado litigios estratégicos en materia de delitos informáticos, asesor jurídico en materia de Protección de Datos y Firma Electrónica Avanzada. Es especialista en Derecho Fiscal y Tecnologías emergentes otorgando asesoría empresarial en los tópicos de Facturación y Contabilidad Electrónica; el uso de Bigdata en materia fiscal; el uso de Tecnologías de Blockchain en materia fiscal; Fiscalización de las Criptomonedas; Derechos del Contribuyente a la Transparencia Algorítmica entre otros tópicos selectos. Es Doctor en Derecho con acentuación en MASC; Master en Derecho Fiscal y Licenciado en Derecho por la FacDyC-UANL; así como, Doctor en Derechos Humanos por la Universidad de Estudios Multinacionales. Cuenta con el reconocimiento del Sistema Nacional de Investigadores del CONAHCYT Nivel I. Es Investigador del CITEJyC-UANL. Es profesor en la Maestría en Derecho Fiscal y Finanzas Públicas de la FacDyC-UANL en la materia de Digitalización Tributaria. Tiene el reconocimiento del Ilustre y Nacional Colegio de Abogados de México y del Colegio de Abogados de Nuevo León como Presidente de la Comisión de Derecho Digital y Ciberseguridad. Actualmente funge como Presidente Rector del Colegio de Especialistas en Derecho Digital, Ciberseguridad y Cibercriminología.

[2] Esta función se conoce por varios nombres: doble autenticación, autenticación de dos factores, doble factor de autenticación o también autenticación en dos pasos. Sin importar cómo la conozcas, esta es una medida de seguridad que ofrecen prácticamente todas las plataformas y apps de servicios online.

través de medios electrónicos.

Un reciente estudio de Google revela que el solo hecho de asociar a tu cuenta de Google un número de teléfono para recuperar el acceso mediante el envío de un código a través de SMS[3], puede bloquear el 100% de los bots automáticos, el 99% de los ataques de phishing masivos, y el 76% de los ataques dirigidos. Realizado de manera conjunta con investigadores de la Universidad de Nueva York y de la Universidad de California, en San Diego, durante un año se recolectaron datos enfocados principalmente en ataques de gran escala y en ataques dirigidos. El objetivo de la investigación era demostrar qué tan efectivas son las prácticas de higiene cibernética básicas para prevenir el secuestro de cuentas de los usuarios por los cibercriminales (Harán, 2019).

Datos presentados por Microsoft en la última edición de la conferencia RCA revelaron que el 99.9% de las cuentas comprometidas que los investigadores monitorean cada mes no utilizan doble factor de autenticación. La segunda estrategia más utilizada por los atacantes para comprometer cuentas es conocida como password replay y consiste en el uso de contraseñas que fueron filtradas en una brecha para luego utilizarlas en servicios de Microsoft, partiendo de la base de lo que decíamos anteriormente: los usuarios suelen reutilizar la misma combinación de usuario y contraseña en distintos servicios. Por otra parte, Walker dijo que el 99% de los ataques de password spraying y el 97% de los ataques de password replay apuntan a protocolos de autenticación heredados, como SMTP, IMAP y POP. Esto se explica en el hecho de que los protocolos de autenticación heredados no soportan el doble factor de autenticación. En este sentido, aquellas compañías que dejan habilitados estos protocolos de autenticación heredados para sus sistemas en la nube y para sus redes están expuestos a ataques y deberían deshabilitarlos lo antes posible (Harán, 2020).

Por otro lado, viéndolo desde la arista social, las familias en México también desconocen varias medidas de seguridad para navegar en internet. El estudio también presentó los riesgos presentes para menores de edad mientras navegan por internet. A su vez, reveló que la población internauta infantil del país está creciendo aceleradamente, y que actualmente más de 50% de los menores de edad cuenta con más de tres dispositivos conectados a internet. Pese a esta mayor conectividad, 47.3% de los padres de familia no usa un sistema de control parental; 4.8% dice no implementar estas herramientas por desconocimiento de cómo funcionan. A su vez, el principal problema de los padres de familia es el establecimiento de límites para el uso de los dispositivos (tres de cada 10 no establecen restricciones para usar internet).

En otro estudio estadístico, las empresas mexicanas se sienten más preparadas para enfrentar ciberataques. En cuanto al sector empresarial, el estudio revela que 63.5% de las empresas en México se sienten «extremadamente o razonablemente preparadas" para hacer frente a ciberataques; sin embargo, los incidentes de ciberseguridad crecieron, siendo el phishing la mayor amenaza para las empresas. Sin embargo, las empresas mexicanas han respondido mejor a otro de los ciberataques más comunes: el ransomware. De acuerdo con el estudio, en los últimos 18 meses 81.6% de las organizaciones detectaron y detuvieron/contuvieron exitosamente ataques de este tipo (Cueto, 2023).

Ahora bien, desde el aspecto estadísticos es alarmante la protección de la doble autenticación como ya se mencionó y la higiene digital para evitar la Suplantación de Identidad a través de medios electrónicos. Desde la concepción del uso del Facebook tenemos que hacer las primeras cuestiones para resolver si está suplantada la identidad o no.

¿*Qué es un perfil falso?* Es el perfil de una persona que no es quien dice ser. Puede ser que la persona

[3] El 99,9% de las cuentas vulneradas no utilizan doble factor de autenticación.

invente una identidad o use la identidad de otra persona. Estas cuentas pueden incluir las cuentas de personas, mascotas, celebridades u organizaciones falsas o inventadas.

¿Qué tengo que tener en cuenta para identificar un perfil falso? En general usa una sola imagen de perfil. Las fotos que publica no son de su autoría: pueden ser de un banco de imágenes o usurpadas de otro sitio. La cuenta tiene poca interacción. Sus contactos parecen falsos. Realiza pocos posteos y actualizaciones. No participa constantemente en grupos. Tiene muy poca información personal. Es una cuenta que pudo haber sido creada recientemente.

¿Qué hago en caso de ser acosado? Hacer capturas de pantalla. No bloquees a los perfiles falsos ya que esto puede impedir la investigación. Realiza la denuncia en la fiscalía más cercana a tu domicilio. Puedes acudir al Centro de Orientación y Denuncia donde puedes pedir asesoramiento o hacer tu denuncia (MJA, 2024).

Ahora otra pregunta que sale a relucir es *¿cómo se hacen los ciberdelincuentes con el control de nuestros perfiles?* Existen diferentes formas de suplantación de identidad en redes sociales: Robo de cuenta: cuando los ciberdelincuentes se hacen con las credenciales (usuario y contraseña) del perfil de la empresa. Mediante técnicas de phishing: envían un correo electrónico haciéndose pasar por la red social en cuestión. En el mensaje, se insta al usuario a acceder a un enlace fraudulento, alegando que su contraseña ha sido comprometida o que existe una nueva actualización. Una vez que el usuario introduce sus datos, estos quedan en manos de los ciberdelincuentes, cambiándolos para que el usuario legítimo no pueda volver a acceder Mediante ataque de fuerza bruta: acceden a las credenciales del perfil probando combinaciones de las contraseñas más comunes, pudiendo llegar a dar con la de la cuenta, si no es lo suficientemente segura.

Suplantación: En este caso, los ciberdelincuentes no acceden directamente al perfil personal o de la empresa, sino que crean uno muy similar con el que se hacen pasar por la cuenta original. Suelen aprovechar variaciones mínimas en el nombre del perfil, objeto de la suplantación para hacer creer a las víctimas que se trata del original. Se crean falsas noticias del entorno: Se propagan principalmente a través de las redes sociales, tienen como objetivo principal la difamación. Suelen tener titulares llamativos que incitan a pinchar en la noticia (clickbait), para obtener un mayor número de visitas. Una falsa noticia sobre una persona o una empresa, podría conllevar un gran impacto reputacional en esta. Estafas: Mientras se navega por las redes sociales, es muy común cruzarse con estafas que pueden pasar casi desapercibidas. Ya sea en forma de publicidad, comentario, mensaje privado, etc. Los ciberdelincuentes aprovechan este medio a través de descuentos increíbles, sorteos de marcas conocidas, URL maliciosas ocultas, etc (INCIBE, 2023).

¿Es un delito suplantar la identidad de alguien en Internet? ¿Se puede crear un perfil en nombre de otra persona sin tener consecuencias legales?

Para comenzar y contestar esta última pregunta, comenzaremos por aplicar el artículo 14 constitucional[4] tercer párrafo que reza:

> *Artículo 14. A ninguna ley se dará efecto retroactivo en perjuicio de persona alguna.*
>
> *En los juicios del orden criminal queda prohibido imponer, por simple analogía, y aún por mayoría de razón, pena alguna que no esté decretada por una ley exactamente aplicable al delito de que se trata.*

[4] Constitución publicada en el Diario Oficial de la Federación el 5 de febrero de 1917 TEXTO VIGENTE Última reforma publicada DOF 24-01-2024

Este principio de legalidad emanado de nuestro máximo ordenamiento jurídico menciona el principio general del derecho *Nullum Poena Sine Lege* estableciendo los rigores legislativos y jurídicos del principio de tipificación de la conducta traducida en acción u omisión que sancionan las leyes penales denominado como tipo penal. Por fortuna en el Código Penal del Estado de Nuevo León en su numeral 444[5] tipifica la conducta denominada Suplantación de Identidad[6], activo menesteroso del presente estudio y reza como sigue:

> *Artículo 444. Comete El Delito De Suplantación De Identidad Quien Se Atribuya Por Cualquier Medio La Identidad De Otra Persona U Otorgue Su Consentimiento Para Llevar A Cabo La Suplantación De Su Identidad, Produciendo Con Ello Un Daño Moral O Patrimonial A La Persona*

Una de las acciones principales que debe realizar la persona afectada es lo siguiente: Revisar la política de privacidad y las condiciones del servicio al que se está accediendo. De esta forma conocerás qué uso hace la red social de tus datos, como los tratarán, almacenarán, si son compartidos con terceros, etc. Deberás recordar que las redes sociales cuentan con secciones que trabajan para evitar suplantaciones y tomar las medidas necesarias para resolver una suplantación en el menor tiempo posible.

Para esto, si aún te encuentras en la posibilidad de poder resolver esto directamente con las aplicaciones, será un verdadero aliciente, aún así comparto las ligas de cada una de las redes sociales más populares para su vía de denuncia.

Facebook[7], X[8], Google+[9], Linkedin[10], Snapchat[11], Instagram[12], Badoo[13], Flickr[14], Pinterest[15]

Si tras denunciar los hechos el problema no se soluciona, puedes interponer una denuncia ante Centro de Orientación y Denuncia más cercano a tu localidad, solicita asesoría. Necesitarás facilitar alguna evidencia de cómo realmente estás siendo víctima de una suplantación. Para ello, guarda por ejemplo alguna captura de pantalla del perfil falso. Deberás en un futuro otorgarle validez oficial a esas probanzas digitales para que tus pruebas tengan una validez legal a la hora de un posible juicio.

Por último, ya observamos que afortunadamente en la legislación local del Estado de Nuevo León en el numeral antes citado, regula la suplantación de identidad, independiente del medio, ahora bien, debemos entender el mecanismo de denuncia para los efectos de que el Ministerio Público realiza la indagatoria correspondiente y hacer poderla presentar como una posible comisión del delito y poder ejercer la acción penal en contra de quien resulte culpable. Si tú o un contacto tuyo ha sido víctima de una suplantación, denúnciala al Centro de Orientación y Denuncia y ellos asignaron tu carpeta de investigación al ministerio público especialista en en la materia.

---

[5] Título Vigésimo Sexto
(Adicionado con el Capítulo y Artículo que lo integran, P.O. 26 de Junio de 2013)
Delitos contra la Identidad Personal

[6] Capítulo Único
(Adicionado con Artículo que lo Integran, P.O. 26 De Junio De 2013)
Suplantación de Identidad
(Reformado, P.O. 27 de Octubre de 2023)

[7] https://es-es.facebook.com/help/181495968648557

[8] https://help.twitter.com/es/forms/safety-and-sensitive-content/abuse

[9] https://support.google.com/googlecurrents/answer/6320425?hl=es&visit_id=638451133952252690-4024477600&rd=1

[10] https://www.linkedin.com/help/linkedin/safety/report-a-problem

[11] https://help.snapchat.com/hc/es/requests/new

[12] https://es-es.facebook.com/help/instagram/547601325292351

[13] https://badoo.com/es/help/?section=89#es/help

[14] https://www.flickr.com/abuse

[15] https://help.pinterest.com/es/article/report-something-on-pinterest#Web

Esperamos que esta información breve te haya sido de utilidad. Si tienes alguna situación o conflicto suscitado por algún delito cibernético, contacta a los especialistas del Colegio de Especialistas en Derecho Digital, Ciberseguridad y Cibercriminología A.C. que cuentan con expertos en la materia, esperando poder resolver tus dudas o situaciones en particular.

Atentamente.

Dr. Daniel Alberto Garza de la Vega
Presidente Rector
Colegio de Especialistas en Derecho Digital, Ciberseguridad y Cibercriminología A.C.

Referencias.

Cueto, H. (2022, July 4). *México suma 88.6 millones usuarios de internet*. Business Insider México. Retrieved February 26, 2024, from https://businessinsider.mx/mexico-millones-usuarios-internet-mexicanos-endutih-inegi-2022_tecnologia/

Cueto, H. (2023, January 18). *22% de internautas en México sufrieron vulneración de seguridad en 2022*. Business Insider México. Retrieved February 26, 2024, from https://businessinsider.mx/22-por-ciento-usuarios-internet-mexico-fue-victimas-vulneracion-seguridad-2022_tecnologia/

Cueto, H. (2023, January 18). *22% de internautas en México sufrieron vulneración de seguridad en 2022*. Business Insider México. Retrieved March 3, 2024, from https://businessinsider.mx/22-por-ciento-usuarios-internet-mexico-fue-victimas-vulneracion-seguridad-2022_tecnologia/

Harán, J. M. (2019, May 21). *Doble factor de autenticación: la solución más efectiva para prevenir el secuestro de cuentas*. WeLiveSecurity. Retrieved March 3, 2024, from https://www.welivesecurity.com/la-es/2019/05/21/doble-factor-autenticacion-solucion-seguridad-mas-efectiva/

Harán, J. M. (2020, March 11). *El 99,9% de las cuentas vulneradas no utilizan doble factor de autenticación*. WeLiveSecurity. Retrieved March 3, 2024, from

https://www.welivesecurity.com/la-es/2020/03/11/mayoria-cuentas-vulneradas-no-utilizan-doble-factor-autenticacion/

INCIBE. (2023, April 4). *Suplantación y robo de identidad en las redes sociales, un riesgo para las empresas | Empresas*. INCIBE. Retrieved March 3, 2024, from https://www.incibe.es/empresas/blog/suplantacion-y-robo-identidad-las-redes-sociales-riesgo-las-empresas

MJA, M. d. J. (2024, Febrero 14). *¿Cómo me doy cuenta si un perfil es falso en Facebook?* Argentina.gob.ar. Retrieved March 3, 2024, from https://www.argentina.gob.ar/justicia/convosenlaweb/situaciones/como-detecto-un-perfil-falso