REVISTA DIGITAL

RIISDS | Revista Interdisciplinaria De Ingeniería Sustentable Y Desarrollo Social

ISSN 2448–8003

Las redes sociales y la suplantación de identidad, Caso de estudio.

Social networks and identity theft, case study

Edgar Guillermo Medellín Orta [1], Lluvia Eréndira Ponce Martínez [1]

1 Instituto Tecnológico Superior de Tantoyuca, Veracruz , México
2

Recibido: 2018-11-06

Aceptado: 2018-12-03

Autor corresponsal: Edgar Guillermo Medellín Orta *edgar_medellin@hotmail.com*

DOI: 10.63728/riisds.v4i1.274

Resumen

Los delitos informáticos y las redes sociales están muy relacionados prácticamente desde su aparición en el ámbito global. El hecho de exponer información personal, familiar, profesional y laboral a prácticamente cualquier persona, deja abierta la oportunidad para que gente mal intencionada pueda hacer uso indebido de dicha información y como consecuencia, traer consigo una afectación al propietario de la misma. Esto ocurre ya que no existe, por parte de los usuarios, una cultura del cuidado de la información en Internet que sea lo suficientemente eficiente para evitar ser víctimas de algún tipo de delito informático. La presente investigación muestra la relación entre el uso de las redes sociales, en particular Facebook, y la identificación de algunos delitos informáticos que se han cometido usando estos medios, caso del delito de suplantación de identidad o phishing y sus consecuencias. Basados en experiencias de personas que se han visto involucradas en situaciones de este tipo, en particular casos comentados con estudiantes de la carrera de Ingeniería en Sistemas Computacionales, donde expresan algunos elementos de acciones que han identificado como delitos de suplantación de identidad. Finalmente se dan algunas recomendaciones para evitar en un futuro ser víctimas de algún delito informático y lograr con esto un uso más responsable de la información que se publica en Internet, en particular en las redes sociales.

Palabras clave: Información, Redes sociales, Delitos Informáticos, victimas, recomendaciones.

Abstract

Computer crimes and social networks are closely related practically since their appearance in the global arena. The fact of exposing personal, family, professional and employment information to practically any person, leaves open the opportunity for malicious people to make improper use of such information and as a consequence, bring with it an affectation to the owner of it. This happens because there is no, on the part of users, a culture of information care on the Internet that is efficient enough to avoid being victims of some type of computer crime. The present investigation shows the relationship between the use of social networks, in particular Facebook, and the identification of some cybercrimes that have been committed using these media, in the case of the crime of identity theft or phishing and its consequences. Based on experiences of people who have been involved in situations of this type, in particular cases discussed with students of the Computer Systems Engineering career, where they express some elements of actions that have been identified as crimes of identity theft. Finally, some recommendations are given to avoid being victims of a cybercrime in the future and to achieve a more responsible use of the information published on the Internet, particularly on social networks.

Keywords: Information, social networks, computer crimes, victims, recommendations.

Introducción

La forma de vida actual, de acuerdo con (Castañón Ortega, 2012) ha evolucionado a grandes pasos debido al desarrollo de nuevas tecnologías y la forma de comunicación moderna que existe. Los dispositivos electrónicos tales como teléfonos celulares smartphone, tablets y computadoras son parte importante de estos avances y permiten al usuario almacenar información, compartirla y estar

comunicados en cualquier momento y lugar siempre que se tenga un acceso a redes de datos o a Internet.

Sin embargo, de acuerdo con (Ojeda Pérez, Rincón Rodríguez, Arias Flores, & Daza Martínez, 2010) cada vez más los dispositivos de procesamiento y almacenamiento de información son vulnerables a ser víctimas de algún tipo de ataque cibernético, dejando expuestos muchos datos de valor incalculable. Aunado al auge que tiene el internet en usuarios cada vez más jóvenes pero a la vez más experimentados.

(Islas Carmona, 2015) publica un estudio donde se indica que la mayor cantidad de usuarios de internet en México está ente los 12 y 17 años de edad (23.6%) además de que otro segmento importante de usuarios oscila entre los 18 y 24 años (20.9%) teniendo en el rango de 12 a 24 años de edad, un total del 44.5% de usuarios de Internet en México

Actualmente la población tiene acceso a Internet, ya sea en sus hogares, escuelas o lugares de trabajo; y por ende acceso a las redes sociales. De acuerdo con (Martínez, Candelaria, Lozano, Zúñiga, Pelaez, & Michel, 2007) los sitios de redes sociales sirven para compartir con personas conocidas gran cantidad de información, sin embargo, la misma apertura que brindan estas tecnologías también tiene como consecuencia un mayor grado de responsabilidad que muchas veces los usuarios no toman muy en serio, trayendo como consecuencia diferentes problemáticas.

Estas problemáticas se traducen en delitos cometidos por personas que buscan dañar física, moral o económicamente a otras. Cuando se habla de usar las TIC´s para cometer algún delito, se generan los delitos informáticos, que de acuerdo con (Temperini, 2015) son aquellas conductas típicas anti jurídicas y culpables donde usan a las computadoras como instrumento o fin, y a su vez (Hernández Díaz, 2009) menciona que es toda acción que provoca un perjuicio a personas o entidades en donde intervienen dispositivos usados en actividades informáticas.

Según (UNAM, CERT, 2011), uno de los problemas que se ha incrementado en los últimos años con el uso de internet y el comercio electrónico es el robo de identidad. De acuerdo con (UNAM, CERT, 2011) el robo de identidad se produce cuando una persona adquiere, posee o utiliza información de una persona física o jurídica de manera no autorizada, con la intención de efectuar o vincularlo con algún fraude u otro delito. Como menciona (Cassou Ruíz, 2009) el robo de identidad ha elevado las estadísticas de la Comisión Federal de Comercio de los EEUU donde ha habido un incremento en el robo de cuentas bancarias y tarjetas de crédito.

Según (Mendoza Enríquez, 2018) la información personal cuenta con un valor económico que pudiera compararse con activos intangibles. Y esto da a pensar en qué tan segura es la información que le proporcionamos a algunas dependencias tales como oficinas de gobierno, hospitales y escuelas. (Becerril López, 2010)

El delito de robo de identidad o suplantación de identidad se ha incrementado día con día, según un estudio publicado por la CONDUSEF, el Banco de México menciona que nuestro país ocupa el octavo lugar a nivel mundial en este delito (CONDUSEF, Edgar Amigón).

Un estudio publicado por (HOCELOT FINANCIAL TECHNOLOGIES, S.L., 2017) menciona que en el fraude de identidad en las redes sociales, más del 15% de los perfiles son falsos. De acuerdo con

(Borbón Sanabria, 2012) dentro de la información obtenida en las redes sociales, la que más se utiliza son: estados de ánimo, lugares visitados, fotografías, intereses, familiares, relaciones, entre otros.

Se han presentado muchos casos a nivel mundial sobre la suplantación de identidad y la violación a la privacidad de la información de los usuarios de las redes sociales, de acuerdo al portal (Deutsche Welle, 2018) la red social Facebook hizo público que descubrió un ataque masivo el veinticinco de septiembre del dos mil dieciocho y que este ataque permitió a los criminales apoderarse de información que podría haber sido usada por terceros.

El objetivo de la presente investigación es analizar el delito de suplantación de identidad en redes sociales desde un punto de vista académico identificando elementos que permitan conocer las estrategias y elementos que se necesitan para realizarlo. Se utilizarán los conocimientos adquiridos, como parte de las actividades de la materia de Seguridad en Tecnologías de la Información y Comunicación (TIC´s) que se cursa en séptimo semestre del plan de estudios de la carrera de Ingeniería en Sistemas Computacionales (ISC), programa educativo que se imparte en el Instituto Tecnológico Superior de Tantoyuca (ITSTa), tomando como antecedentes los saberes previos sobre estos temas y relacionándolos con experiencias propias y de terceros.

Materiales y métodos

Caso de estudio ITSTa

En el ITSTa se han presentado casos de delitos donde se han visto involucrados los estudiantes en situaciones que comprometen su integridad tanto física como moral. Dentro de los mas concurrentes se encuentran aquellos que involucran las diferentes tecnologías de comunicación tales como los Smartphone, Internet, redes sociales, entre otros.

En algunos de estos casos se ha tenido que acudir a autoridades del plantel para efectos de tomar decisiones respecto a las acciones a implementar, ya sea para dar con los responsables del delito cometido, y en otras ocasiones para aplicar la sanción correspondiente.

Sin embargo, a pesar de que existe un reglamento que rige a los estudiantes, este no siempre contempla todos los aspectos necesarios para poderlo aplicar. Aunado a que dicho reglamento fue elaborado hace mas de 20 años, época en la cual aún no se tenían las tecnologías que abundan hoy en día, en particular los Smartphone.

Debido al uso masivo de estos dispositivos, es más fácil realizar acciones que pudieran incurrir en un tipo de delito, y basados en la definición de delitos informáticos previamente mostrada y analizada, estamos ante la situación de que cualquier estudiante puede cometer o ser víctima, voluntaria o involuntariamente, de algún tipo de delito informático.

Actualmente el ITSTa cuenta con nueve carreras profesionales, pero solo en el plan de estudios de Ingeniería en Sistemas Computacionales se contempla una materia que toca temas acordes a los delitos informáticos y los elementos principales tanto para prevenirlos así como para sancionarlos.

Por tal motivo, para la presente investigación se tomaron en cuenta a los estudiantes del curso de Seguridad en TIC´s que se imparte en la carrea de ISC del ITSTa, en este caso son cuarenta y siete alumnos inscritos al séptimo semestre en el periodo Agosto-Diciembre del dos mil dieciocho.

A estos estudiantes se les aplicó una encuesta enfocada a identificar sus conocimientos sobre el tema de delitos informáticos pero buscando principalmente las respuestas que lleven hacia el delito de suplantación de identidad, ya que es el objeto de estudio.

Para tal efecto se usó la siguiente encuesta conformada por cinco preguntas que a continuación se muestran.

1.- ¿Conoces el término delito informático?
a) Si b) No

2.- ¿Sabes qué son los delitos informáticos?
a) Si b) No

3.- ¿De cuál de los siguientes delitos informáticos has sido víctima?
a) Suplantación de identidad
b) Hacking de correo
c) Clonación de tarjetas
d) Ingeniería social
e) Otros

4.- De los delitos mencionados anteriormente, ¿Cuál consideras de mayor peligro para un usuario de redes sociales?

5.- En base a tus conocimientos, ¿Qué fin tiene cometer algún delito informático?
a) Ingeniería social
b) Difamación
c) Fraude
d) Cyberacoso
e) CyberBulling

Solo se contemplaron cinco preguntas en la encuesta debido a que la totalidad de los estudiantes encuestados ya tenía conocimiento sobre el tema de delitos informáticos, en ese sentido, no hubo necesidad de profundizar en una explicación para definir dicho tema, esto debido a que a lo largo de su carrera han tenido que realizar algunas actividades referentes a este tema.

Resultados y discusión

Identificación de delitos.

Cuando se habla de los delitos que se cometen teniendo como instrumento de acción algún dispositivo electrónico con acceso a una red de datos, se tienen que englobar algunos factores tales como la seguridad de la información, así como las características que debe tener dicha información para que pueda ser considerada como confiable.

Sin embargo, esta seguridad se puede ver comprometida cuando no se tiene el cuidado necesario y se da acceso a ella para que esté al alcance de cualquier persona, caso específico de lo que se publica en redes sociales.

Ante esta situación, de los cuarenta y siete alumnos encuestados, en la pregunta ¿De cuál de los siguientes delitos informáticos has sido víctima?, al analizar los resultados, se obtuvieron los datos mostrados en la tabla 1, siendo los ahí mencionados aquellos que más se han identificado por parte de los usuarios afectados.

Tabla 1.
Delitos Informáticos

Delitos	Casos identificados
Suplantación de identidad	12
Hacking de correo	15
Clonación de tarjetas	3
Ingeniería social	7
Otros	10
Total alumnos	47

Fuente: Los autores.
Elaboración: propia.

Aunque existe gran cantidad de información sobre los diferentes tipos de delitos informáticos existentes, mucha gente desconoce de ellos y de cómo saber si han sido víctimas, ya que se tiene la falsa creencia de que al ser un usuario normal no estamos expuestos a ser blanco de los delitos en mención.

Al hacer un sondeo más específico del uso de las redes sociales en los estudiantes encuestados, se identificaron algunos sucesos en los cuales se han presentado situaciones que indican que se cometió un delito informático. Esta información se obtuvo de la pregunta número cinco de la encuesta aplicada.

Uno de los casos más recurrentes que se encontraron en el uso de las redes sociales es la suplantación de identidad.

Al analizar la información obtenida sobre la suplantación de identidad, se identificaron varias finalidades dentro de las cuales destacan tres principales (ver tabla 2):

Ingeniería social: que por sí misma, algunos autores la consideran como delito, de acuerdo con (Kaspersky Labs, 2018) es un conjunto de técnicas que usan los cibercriminales para engañar a los usuarios para robar datos confidenciales e infectar sus computadoras.
Difamación o difamar: según (Real Academia Española, 2018) es desacreditar a alguien, ya sea de palabra o por escrito, publicando algo contra su buena opinión y fama.
Fraude: de acuerdo con (Real Academia Española, 2018) es la acción contraria a la verdad y a la rectitud, que perjudica a la persona contra quien se comete.

Tabla 2.
Suplantación de identidad

Finalidad	Casos
Ingeniería social	6
Difamación	4
Fraude	2

Fuente: Los autores.
Elaboración: propia.

Otros fines que también se involucran aunque en menor proporción son: cyberacoso, ya sea sexual o de otro tipo y cyberbullying.

Acciones que causan los delitos.

Una manera de salir adelante después de ser víctima de un delito, es buscar las causas que lo originaron para evitar caer de nuevo en esas situaciones, si bien en ocasiones esto requiere hacer uso de herramientas informáticas, tal es el caso de algún software especializado, muchas veces basta con recordar cómo se presentaron las situaciones que llevaron a la acción del delito.

En nuestro caso de estudio, se presentó la situación que muchos usuarios dejan abiertas sus sesiones de redes sociales en sus dispositivos, ya sea computadora o teléfono celular, dejando el camino abierto para que cualquier persona que tenga acceso a dichos dispositivos, también lo tenga al perfil de red social.

Esto ha generado una serie de consecuencias como las mencionadas anteriormente, y desafortunadamente los usuarios no se percatan del mal uso que se hace tanto del dispositivo como de la red social.

Sin embargo no es la única causa que origina esto, otro de los factores que se presentan es el uso de contraseñas fáciles de identificar, esto sucede porque muchos usuarios manejan la misma contraseña para diferentes dispositivos o sistemas, por ejemplo la contraseña para acceder a la computadora es la misma que ocupan para acceder a sus cuentas de correo electrónico o a sus redes sociales.

Esto trae como consecuencia que una persona malintencionada, al conocer estas contraseñas, fácilmente puede usarla en alguna de las otras plataformas, teniendo así acceso a ellas para poder hacer lo que quiera en perjuicio de la víctima.

Aunque actualmente los sitios web de correo electrónico y redes sociales ya exigen contraseñas más seguras en base a ciertos criterios establecidos por ellos mismos, si el usuario no los cumple o simplemente no guarda bien su contraseña, de nada sirven estas estrategias planteadas por dichos sitios web.

Una situación más que se logra identificar en el uso de redes sociales para ser víctimas de algún delito, es el agregar a contactos sin estar seguros de quien se trata realmente, las personas que se dedican al robo de identidad generalmente se hacen pasar por usuarios comunes de la red social, y mandan solicitudes de amistad a muchos usuarios, y más de alguno los acepta, y a partir de ahí empiezan a relacionarse con otros usuarios, haciendo cada vez más grande la lista de contactos los cuales se vuelven víctimas potenciales.

Esto le ocurre sobre todo a personas que empiezan a hacer uso de las redes sociales y buscan tener una lista grande de contactos, pero no tienen la debida precaución de corroborar o comprobar quien es el contacto que les mando la solicitud de amistad para poderlo agregar sin ningún problema.

Nuevamente, a pesar de que esto ya viene de tiempo atrás y existe demasiada información que habla sobre la prevención en este tipo de acciones, los usuarios siguen haciendo caso omiso y caen en las situaciones de riesgo.

Lo anteriormente expuesto no son todas las causas que pueden provocar ser víctimas de delitos en redes sociales, sin embargo son las más comunes. Otras circunstancias que se pueden presentar son: caer en publicidad engañosa, visualizar videos que pudieran ser falsos, acceder a enlaces de noticias falsas, entre otros.

Conclusiones

Una vez que se analizaron las causas y consecuencias de ser víctima de un delito informático, es necesario seguir las recomendaciones generales que sugieren los expertos en el tema, aunque hay algunas que no necesariamente son dichas por expertos, pero si por gente que ha sufrido algún tipo de ataque.

Una de las principales recomendaciones es hacer uso del sentido común, es decir, ser precavido en lo que se publica, cómo se publica, a quién se le comparte y a que sitios se accede.

No acceder a enlaces de videos que parecen interesantes o chuscos, ni a sitios que pidan enviar alguna información sensible por medio de un formulario web como son contraseñas o datos personales.

No compartir claves bancarias o importantes por medio de mensajes de redes sociales, debido a que dicha información se queda almacenada en estos sitios.

Cuando se extravíen documentos personales o sean robados, se deben hacer el reporte correspondiente a las autoridades competentes para evitar que hagan mal uso de esos documentos, por ejemplo cancelar tarjetas bancarias o credencial de elector.

En particular, para evitar la suplantación de identidad en redes sociales, se recomiendan algunas acciones preventivas tales como: evitar dar datos importantes a personas que llaman realizando algún tipo de encuesta, cambia regularmente tus contraseñas de redes sociales, no mantengas abierta tu sesión de red social en dispositivos que compartas con otras personas o en equipos de lugares públicos.

De igual manera, no son todas las recomendaciones que se pudieran dar, pero sí de las más recomendables a seguir para poder tener un buen uso de las redes sociales.

Referencias bibliográficas

Becerril López, S. A. (2010). Acuerdos Internacionales para la privacidad de la información. *Punto Seguridad, Seguridad en TIC*, 5-7.

Borbón Sanabria, J. S. (2012). Redes sociales, entre la ingeniería social y los riesgos a la privacidad. *Seguridad, cultura de prevención para TI*, 32-36.

Cassou Ruíz, J. E. (2009). Delitos Informáticos en México. *Revista del Instituto de la Judicatura Federal*, 207-236.

Castañón Ortega, B. M. (06 de Noviembre de 2012). *Los avances tecnológicos y la cultura digital.* Recuperado el 20 de Octubre de 2018, de gestiopolis.com: https://www.gestiopolis.com/los-avances-tecnologicos-cultura-digital/

CONDUSEF, Edgar Amigón. (s.f.). *Primer Plano.* Recuperado el 10 de Septiembre de 2018, de proteja su dinero: https://www.condusef.gob.mx/Revista/PDF-s/2015/186/robo.pdf

Deutsche Welle. (28 de Septiembre de 2018). *Actualidad/Política. Deutsche Welle*. Recuperado el 15 de Octubre de 2018, de sitio web de DW Deutsche Welle: https://www.dw.com

Hernández Díaz, L. (2009). El delito Informático. *Eguzkilore*, 227-243.

HOCELOT FINANCIAL TECHNOLOGIES, S.L. (08 de Junio de 2017). *Sobre nosotros HOCELOT.* Recuperado el 19 de Septiembre de 2018, de Sitio web de HOCELOT FINANCIAL TECHNOLOGIES, S.L.: https://hocelot.com

Islas Carmona, O. (2015). Cífras sobre jóvenes y redes sociales en México. *Entretextos*, 1-16.

Kaspersky Labs. (2018). *Centro de recursos: Kaspersky Labs.* Recuperado el 10 de Noviembre de 2018, de sitio web de Kaspersky Labs: https://latam.kaspersky.com/resource-center/definitions/what-is-social-engineering

Martínez, F. R., Candelaria, A. H., Lozano, M. R., Zúñiga, A. R., Pelaez, R., & Michel, J. P. (2007). Después de presionar el botón enviar, se pierde el control sobre la información personal y la privacidad: un caso de estudio en México. *Revista Ibérica de Sistemas y Tecnologías de la Información*, 115-128.

Mendoza Enríquez, O. A. (2018). Marco jurídico de la protección de datos personales en las empresas de servicios establecidas en México: desafíos y cumplimiento. *IUS, 12(41)*, 267-291.

Ojeda Pérez, J. E., Rincón Rodríguez, F., Arias Flores, M. E., & Daza Martínez, L. A. (2010). Delitos Informáticos y entorno jurídico vigente en Colombia. *Cuadernos de contabilidad*, 41-66.

Real Academia Española. (2018). *dle.rae.es*. Recuperado el 10 de Noviembre de 2018, de sitio web de la Real Academia Española: https://dle.rae.es/srv/search?m=30&w=difamar

Temperini, M. G. (2015). Delitos Informáticos en Latinoamérica: Un estudio de derecho comparado. 1ra. parte. *Biblioteca digital del Departamento de Cooperación Jurídica*, 1-12.

UNAM, CERT. (06 de Junio de 2011). *Documentos de la CSI, UNAM-CERT.* Recuperado el 11 de Noviembre de 2018, de Sitio web de la UNAM-CERT: https://www.cert.org.mx/