risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Revista Ibérica de Sistemas y Tecnologías de Información

Recebido/Submission: 24/03/2016
Aceitação/Acceptance: 27/04/2016

Después de presionar el botón enviar, se pierde el control sobre la información personal y la privacidad: un caso de estudio en México

Francisco R. Cortes Martinez[1], Angel D. Herrera Candelaria[1], Manuel A. Ramírez Lozano[2], Alma R. Rodríguez Zúñiga[2, 4], Rafael Martínez Peláez[2], Jorge R. Parra Michel[3]

al114359@alumnos.uacj.mx, al114847@alumnos.uacj.mx, mrl598021@udelasalle.mx, alma_rz@fisica.ugto.mx, rmartinezp@delasalle.edu.mx, jrparra@delasalle.edu.mx

[1] División Multidisciplinaria de Ciudad Universitaria, Universidad Autónoma de Ciudad Juárez, C. José de Jesús Macías Delgado, Ciudad Juárez, Chihuahua, México

[2] Facultad de Tecnologías de Información, Universidad de la Salle Bajío, Av. Universidad 602, 37150, León, Guanajuato, México.

[3] Escuela de Ingenierías, Universidad de la Salle Bajío, Av. Universidad 602, 37150, León, Guanajuato, México.

[4] División de Ciencias e Ingenierías, Universidad de Guanajuato, Lomas del Bosque 103, 37150, León, Guanajuato, México.

DOI: 10.17013/risti.21.115–128

Resumen: Desde el inicio de los servicios electrónicos, los usuarios de Internet han enviado su información personal y financiera a diferentes servidores web, perdiendo el control sobre su información. Años más tarde, con la popularización de los sitios de redes sociales, la información personal de los usuarios se encuentra disponible y fluye rápidamente entre miembros de la comunidad, exponiendo su privacidad. Por lo tanto, varios investigadores han estudiado la percepción de los usuarios acerca de la privacidad y seguridad en Internet, mundos virtuales y sitios de redes sociales desde. En este sentido, la primera contribución del presente trabajo es la exposición de problemas de privacidad y seguridad existentes en el proceso de registro. Además, se describen los problemas que pueden ocasionar la falta de seguridad y privacidad en sitios de redes sociales. Finalmente, se presentan los resultados de una encuesta sobre privacidad y seguridad de usuarios mexicanos, coincidiendo con trabajos previos.

Palabras-clave: autenticación; ciber-crimen; fraude; robo de identidad; privacidad

After click the submit button, control over personal information and privacy is lost: a case study in Mexico

Abstract: Since the beginning of electronic services, Internet users have disclosure their personal and financial information to different web servers, losing control over their information. Years later, with the popularization of social networking sites, users' personal information is available and flows quickly among community

members, exposing their privacy. Therefore, several researchers have studied the perception of users about privacy and security in the Internet, virtual worlds, and social networking sites since. In this sense, the first contribution of the present work is the exposition of problems of privacy and security existing in the process of registration. In addition, it describes the problems that can cause the lack of security and privacy on social networking sites. Finally, the results of a survey on privacy and security of Mexican users, coinciding with previous work, are presented.

Keywords: authentication; cyber-crime; fraud; identity theft; privacy

1. Introducción

Hoy en día, Internet es cada vez más importante en nuestra vida cotidiana. Esto significa que, necesitamos conexión a Internet para realizar muchas actividades, como comunicarnos con familiares y amigos, leer noticias, buscar información, comprar y más. Al mismo tiempo, desarrolladores, investigadores y estudiantes crean nuevas aplicaciones, servicios y soluciones donde el canal de comunicación es a través de Internet. Por ejemplo, los sitios de redes sociales, e-cloud e Internet de las cosas (IoT) representan la tendencia en la tecnología, que puede utilizarse en diferentes escenarios. Otro ejemplo de la relevancia de Internet es el concepto de Big Data donde se recoge y analiza el comportamiento de los usuarios de Internet para descubrir información. Como resultado, cada día aumenta el número de usuarios de Internet en todo el mundo, haciendo de Internet parte de nuestras vidas estemos de acuerdo o no.

En muchos de los servicios electrónicos y aplicaciones web, los usuarios de Internet necesitan llenar un formulario de registro web. Un formulario de registro web se utiliza para solicitar información personal, como dirección, edad, nombre, género, entre otros, a cada usuario de Internet (Schrammel, Köffel, & Tscheligi, 2009). La información se envía a través de la Internet desde la computadora del usuario al servidor. A continuación, la información personal se almacena en una base de datos y el sistema crea una nueva cuenta. Después de eso, cada usuario de Internet puede acceder al sistema usando su cuenta. Este proceso se ha utilizado desde el inicio de Internet. De acuerdo con Luke Wroblewski (Wroblewski, 2008) un formulario de registro web es:

"Registration forms are the gatekeepers to community membership",

"Data input forms allow user to contribute or share information", and

"Web forms are often the last and most important mile in a long journey."

Esto significa que, los usuarios de Internet comparten información con *n* empresas cuando hacen clic en el botón enviar para crear una cuenta. El problema con el proceso es que, los usuarios de Internet revelan información bajo presión (Joinson, Buchanan, & Paine Schofield, 2010). Esta acción tiene repercusión en cuestiones de privacidad y seguridad porque la información personal es utilizada y recogida por terceros (Schrammel, Köffel, & Tscheligi, 2009).

Por otro lado, los jóvenes usuarios de Internet han integrado los sitios de redes sociales (SRS) en su vida cotidiana. Según (Boyd & Ellison, 2007) un sitio de red social es:

> *"a web-based service that allow individual to 1) construct a public or semi-public profile within a bounded system, 2) articulate a list of other users with whom they share a connection, and 3) view and traverse their list of connections and those made by others within the system."*

En este escenario, los usuarios de SRS comparten sus sentimientos, ubicación, opiniones, imágenes y momentos especiales con otros (Boyd & Ellison, 2007) y (Ellison, Steinfield, & Lampe, 2007). Por otra parte, el servicio web almacena hábitos y preferencias de cada usuario en una base de datos, durante cierto tiempo, para ofrecer servicios y promociones basadas en sus preferencias (Facebook, 11). Como resultado, podemos conocer mucha información acerca de una persona sin reunirse en el mundo real.

Como consecuencia del uso del formulario de registro web y de sitios de redes sociales, el crimen organizado y los delincuentes pueden obtener varia información sobre personas vulnerables o desprotegidas. Por ejemplo, cuando hacemos clic en el botón enviar, sin revisar el certificado digital o verificar la legitimidad del sitio web, nuestra información personal o financiera podría ser robada. Esta acción es posible porque muchas personas no conocen la relevancia de la seguridad, en concreto el certificado digital. Además, la gente comparte información a través de sitios de redes sociales, dejando por un lado su privacidad.

Específicamente, la contribución de este artículo es doble. En primer lugar, explicamos las cuestiones de seguridad del formulario de registro web, que se centra principalmente en sus vulnerabilidades y su repercusión en la vida real de los usuarios. En segundo lugar, recopilamos datos para permitir una investigación empírica sobre la delgada línea entre lo privado y público en los SRS y como cada día nos volvemos más vulnerables. Este artículo expone los inconvenientes de seguridad y privacidad del formulario de registro web y los problemas de seguridad y privacidad en los sitios de redes sociales con el fin de encontrar nuevos y más seguros mecanismos para prevenir o reducir los ataques.

La estructura del artículo es la siguiente. En la sección 2, se describe el proceso de registro utilizando un formulario web, se da una breve definición y descripción de los SRS, y se explican brevemente trabajos relacionados sobre el estudio de la privacidad y seguridad en Internet, mundo virtual y SRS. La metodología e hipótesis son descritas en la sección 3. Los resultados del estudio de privacidad y seguridad en el proceso de registro y en SRS son presentados en la sección 4. En la sección 5, se dan las conclusiones y trabajo futuro de la investigación.

2. Conceptos y Trabajos Relacionados

En esta sección, se presenta el contexto del estudio en el proceso de registro utilizando el formulario de registro web y en sitios de redes sociales para describir el planteamiento del problema que se encuentra en estudio. Además, se describen los aportes realizados por diferentes investigadores para comprender la percepción de los usuarios sobre la privacidad y seguridad en Internet, mundos virtuales y SRS.

2.1. Proceso de registro utilizando el formulario web

Inicialmente, se describe el proceso general para crear una cuenta basada en el uso del formulario de registro web. Cabe mencionar que, el procedimiento es clave para el éxito de cualquier sitio web. La Figura 1 muestra el proceso entre el usuario de Internet y los servidores web para crear una cuenta.

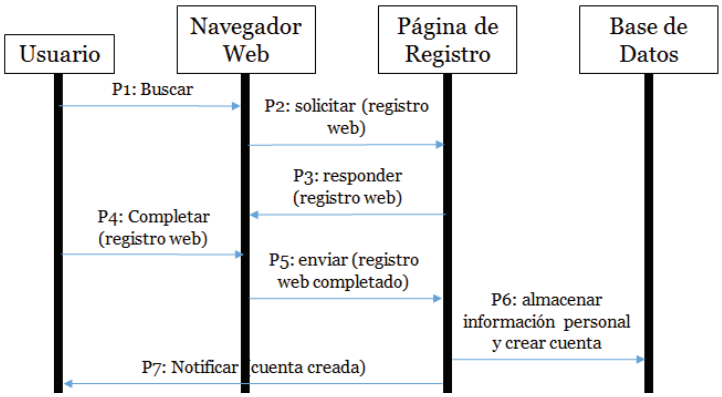

Figura 1 – Creando una cuenta de usuario utilizando el formulario de registro web

A partir de la Figura 1, se pueden explicar los siguientes pasos:

Paso 1: Los usuarios de Internet que desean ser miembros de una comunidad o utilizar un servicio electrónico deben crear una cuenta, en la mayoría de los casos de manera obligatoria. Por lo tanto, los usuarios acceden al sitio web donde se desean registrar a través de su navegador web.

Paso 2: Los usuarios de Internet deben solicitar el formulario de registro web para completar los datos personales solicitados.

Paso 3: El formulario de registro web, en la mayoría de los casos, solicita al usuario: nombre, edad, género, correo electrónico, y contraseña. Sin embargo, en sitios de comercio electrónico y sitios de redes sociales, se solicita: dirección, código postal, ciudad actual, escolaridad, entre otra información.

Paso 4: El usuario de Internet debe completar el formulario de registro web con la información solicitada.

Paso 5: El formulario de registro web es enviado al servidor web. Para permitir enviar el formulario web, se debe haber completado correctamente cada campo obligatorio.

Paso 6: La información recibida es almacenada en una base de datos y se crea la cuenta de usuario.

Paso 7: Se notifica al usuario sobre la creación de la cuenta.

2.2. Sitios de redes sociales

En la actualidad, los sitios de redes sociales (SRS) permiten mantener contacto con familiares y amigos; así como, compartir ideas, expresar opiniones y difundir fotos entre los miembros de la comunidad (Boyd & Ellison, 2007). En consecuencia, los SRS se han convertido, en poco tiempo, en un medio de difusión tan importante que (Ellison, Steinfield, & Lampe, 2007), 1) se utilizan para movilizar a grupos de personas en pro de

una causa común, 2) se emplean como parte del arsenal político en campañas electorales, y 3) se emplean como medio de diversión.

Lo anterior es posible gracias a las siguientes dos características (Tong & Der, 2008): rápida difusión y el comentario mantiene interés en el tiempo. Por lo tanto, un comentario, idea, opinión, o foto puede compartirse y llegar a ser visto por miles de usuarios en poco tiempo, convirtiéndose en *trending topic*. En cuanto a mantener el interés en el tiempo, la noticia puede mantener su popularidad entre diferente grupo de usuarios y retomar su interés cuando sea necesario debido a que no desaparece o no se borra por completo.

A pesar que, los SRS ofrecen una manera entretenida de comunicación entre diferentes usuarios, nada es perfecto. Existe el lado obscuro de los SRS que tiene que ver con la información proporcionada por cada usuario durante el proceso de creación de su perfil y durante su uso diario. Sin darse cuenta, cada usuario de los SRS comparte información personal que incluye desde su nombre, edad, lugar de nacimiento hasta su lugar favorito para cenar o su nivel socio-económico que puede ocasionar serios problemas al usuario.

Debido a la naturaleza de los SRS, los usuarios comparten, de manera consciente o inconsciente, información personal y privada en un medio de difusión masivo. Por ejemplo, varios usuarios comparten su estado de ánimo permitiendo que otros usuarios lo conozcan o se suele compartir la foto de la fiesta del viernes, invadiendo indirectamente la privacidad de un tercero.

Es a partir de esa situación que se han realizado diferentes estudios sobre la privacidad en sitios de redes sociales (Ellison, Steinfield, & Lampe, 2007), (Leitch & Warren, 2009), (Gross, 2005), (Schrammel, Köffel, & Tscheligi, 2009), (Li, Zhang, & Lu, 2016). Cabe mencionar que, la privacidad es uno de los temas que más ha preocupado a los usuarios de Internet desde sus inicios (Kermek & Bubas, 2000).

2.3. Estudios sobre la privacidad y seguridad en Internet, mundos virtuales y SRS

Al principio, los usuarios de Internet encontraron desventajas en Internet basado en los riesgos de seguridad y privacidad en línea (Kermek & Bubas, 2000). Esta percepción se fundó en los ataques cibernéticos a empresas, daños causados por virus, y ausencia de ley (Kermek & Bubas, 2000). Desde entonces, varios investigadores han estudiado la percepción que tienen los usuarios de Internet de la privacidad y la seguridad en tres escenarios: comercio electrónico, mundos virtuales, y sitios de redes sociales (Kermek & Bubas, 2000), (Stockton & Cunningham, 2014) y (Liebermann & Stashevsky, 2002).

El primer estudio sobre la percepción de los usuarios acerca de la privacidad y seguridad fue elaborado por Kermek y Bubas (2000). Ellos investigaron el efecto de la privacidad y seguridad al comparar Internet con los medios de comunicación tradicionales, encontrando que Internet se consideraba más inseguro en comparación con la televisión y prensa.

Dos años más tarde, Liebermann y Stashevsky (2002) investigaron las barreras para adoptar el comercio electrónico, encontrando que utilizar tarjetas de crédito y compartir información personal eran percibidos como riesgoso. En este sentido, (Belanger, J.S.,

& Smith, 2002) identificaron que la privacidad y la seguridad son dos preocupaciones claves para los usuarios cuando quieren comprar algo en Internet.

Un año más tarde, (Wang, Wang, Lin, & Tang, 2003) explicaron la relación entre privacidad y seguridad como un efecto positivo en los usuarios de la banca electrónica. Más tarde, (Scott, 2004) estudió la percepción del riesgo de comercio electrónico demostrando que la privacidad y la seguridad todavía se perciben como un riesgo. Más recientemente, (Mekovec & Hutinski, 2012) llevaron a cabo una investigación sobre la percepción de usuarios de Internet acerca de la privacidad y la seguridad durante sus actividades en línea, concluyendo que son relevantes para la expansión del comercio electrónico. Recientemente, (Qi, Hao, & Xing, 2016) evaluaron la seguridad del comercio electrónico basado en el entorno de cómputo en la nube, corroborando que para el usuario el riesgo de mantener su privacidad es alto.

Con la aparición de los mundos virtuales, surgieron nuevos paradigmas en los campos de la psicología, antropología y ciencias de la computación. En este nuevo escenario, donde los usuarios de Internet tienen la opción de crear una segunda vida (Mennecke, y otros, 2008; Kimble et al., 2016), la privacidad y seguridad se perciben como alarmantes (Leitch & Warren, 2009). Además, los usuarios identificaron los siguientes riesgos: robo de identidad, fraudes y delitos virtuales (Schrammel, Köffel, & Tscheligi, 2009).

De esta manera, los sitios de redes sociales han abierto una nueva puerta para que investigadores puedan estudiar la relación entre las personas (Ellison, Steinfield, & Lampe, 2007) y su impacto en diferentes temas, tales como: amistad, privacidad, seguridad, y popularidad. En términos de privacidad, los estudios (Leitch & Warren, 2009) y (Gross, 2005) han evaluado la información revelada en sitios de redes sociales y problemas de seguridad. En (Gross, 2005), los autores demostraron que los usuarios comparten sus datos personales y no cambiaron las preferencias de privacidad por defecto.

Con el fin de identificar la información revelada por los usuarios en diferentes sitios de redes sociales, en (Schrammel, Köffel, & Tscheligi, 2009) se realizó un estudio sobre las variables demográficas y los contextos de uso y patrones, encontrando que los usuarios revelan su nombre real, fotografía, fecha de nacimiento y red de amigos a desconocidos; mientras que, su número de teléfono, dirección física, mensajería instantánea, y sitio web se divulga entre amigos.

En (Dwyer, Hiltz, & Passerini, 2007), los autores encontraron una correlación entre la percepción de los usuarios sobre la confianza en el SRS y la información revelada, obteniendo resultados similares que (Schrammel, Köffel, & Tscheligi, 2009). Más tarde, en (Sahinaslan & Kantürk, 2009), los autores encontraron que compartir información de contacto es más personal que compartir información personal. Más recientemente, en (Ögütcü, Testik, & Chouseinoglou, 2015), los autores encontraron que el comportamiento y hábitos de los usuarios deben ser protegidos, al igual que la información de contacto y personal.

3. Metodología

Es esta sección, se postulan las hipótesis de investigación. Además, se procede a explicar la metodología empleada para estudiar la seguridad y privacidad en: 1) proceso de registro utilizando el formulario web en diferentes sitios web en México y 2) sitios de redes sociales.

3.1. Planteamiento de hipótesis

En base al crecimiento de usuarios de Internet y al crecimiento de transacciones de comercio electrónico (AMIPCI, 2016) en México, se han planteado las siguientes hipótesis:

- H1: El 100% de los sitios web que almacenan algún dato personal tienen implementado un certificado digital en la página del formulario de registro web.
- H2: El 100% de los sitios web que almacenan algún dato personal tienen política de privacidad.
- H3: Ningún sitio web cuenta con una herramienta, técnica o procedimiento para verificar la identidad del usuario.

En base a la popularidad del SRS Facebook en México, se centró el estudio de seguridad y privacidad inicialmente en ese SRS (AMIPCI, 2012). Sin embargo, se tuvo que incluir otros SRS debido a su gran uso entre la población mexicana. Las hipótesis definidas son:

- H4: Los usuarios de SRS aceptan invitaciones de otros usuarios que no conocen en el mundo real.
- H5: Los usuarios de SRS publican información personal e información de contacto.
- H6: Los SRS no verifican la información personal utilizada para crear la cuenta.

3.2. Proceso de registro utilizando el formulario web: metodología

En la fase 1, se creó una lista que incluyen sitios web de varios sectores de la economía en México, que incluyen: fabricantes, sector público, servicios inmobiliarios, servicio de negocios, transporte, y turismo. En la creación de la lista no se considera el número de empleados, ingresos o tiempo de creación del sitio web. El número total de la lista es de 46 sitios web.

En la fase 2, se procedió a realizar la creación de una cuenta en cada uno de los sitios web con la intención de identificar:

- Uso de certificados digitales para autenticar al sitio y asegurar la comunicación de los datos a través de los protocolos SSL o TLS. Para corroborar la seguridad en la comunicación, se utilizó el analizador de protocolos de red “WireShark”.
- Publicación de la política de privacidad.
- Técnicas, herramientas o procedimientos para detectar información falsa.

En la fase 3, se consolidaron los datos obtenidos para su posterior análisis y definición de riesgos de privacidad y seguridad.

3.3. Sitios de redes sociales: metodología

En la fase 1, se diseñó una encuesta en línea (goo.gl/e3mD8P) para investigar el nivel de privacidad de cada persona en sus cuentas de SRS. La encuesta fue publicada en el muro de Facebook de cada uno de los miembros del proyecto y se difundió a través de correo electrónico. Se recibieron un total de 69 respuestas. En esta parte de la investigación, se buscó conocer la percepción de los usuarios acerca de la privacidad en sus cuentas, considerando si los usuarios aceptan como amigos a usuarios desconocidos y si los usuarios comparten fotos con familiares y amigos. En este sentido, se pregunta si su información es pública o privada.

La encuesta en línea consiste en 19 preguntas de opción múltiple. Los encuestados contestaron preguntas orientadas a conocer información relacionada con su cuenta de Facebook, que incluye: cantidad de tiempo con una cuenta (1 año, 2-4 años, más de 4 años), conocimiento sobre la política de datos personales, y edad. También se solicitó a los encuestados contestar preguntas orientadas hacia la privacidad de las cuentas, que incluye: cuenta es pública (sí, no, no sé), publicación de fotos con familiares y amigos (yo, con familiares, otro), si tienen entre la lista de amigos a personas desconocidas en el mundo real, y si el nombre utilizado en la cuenta es real o no.

En la fase 2, se creó una cuenta utilizando información falsa. La creación de la cuenta fue de manera manual para evitar el uso de bots.

En la fase 3, se procedió a llevar a cabo un ataque entre la comunidad de estudiantes de la Universidad Autónoma de Ciudad Juárez. El procedimiento fue de manera manual, que incluyó: crear un perfil, realizar publicaciones periódicas, ingresar a grupos, e invitar a amigos para crear la red social.

En la fase 4, se consolidaron los datos obtenidos para su posterior análisis y definición de riesgos de privacidad y seguridad.

4. Resultados

A partir de las hipótesis definidas y la metodología empleada, se presentan los datos obtenidos y se procede a realizar el análisis. Es importante mencionar que, la encuesta se aplicó entre el mes de diciembre 2015 y el mes de enero 2016, y los datos recopilados no contienen información personal de ninguna persona encuestada.

También se desea expresar que durante el ataque al SRS no se hizo mal uso de la información recopilada y que en ningún momento se buscó afectar la integridad, privacidad o seguridad de ninguna persona.

4.1. Proceso de registro utilizando el formulario web: resultados

La Tabla 1 resume los datos encontrados en nuestro estudio.

Clasificación	Certificados digitales		Detección de Información falsa		Aviso de privacidad		Total de sitios web
	Yes	No	Yes	No	Yes	No	
Fabricantes	2	-	-	2	2	-	2
Sector público	2	4	1	5	6	-	6
Servicios inmobiliarios	0	5	-	5	5	-	5
Negocios	14	6	-	20	20	-	20
Transporte	2	2	-	4	4	-	4
Turismo	9	-	-	9	9	-	9
	29	17	1	45	46	-	46

Tabla 1 – Estudio de seguridad y privacidad en el proceso de creación de una cuenta

A partir del estudio de seguridad, se identifica claramente que el uso de certificados digitales es implementado en un 63% de los sitios web. En estos casos, el certificado digital ofrece certeza al usuario sobre la legitimidad del sitio web y protege el canal de comunicación para transmitir la información personal. El otro 37% de los sitios web que no implementan un certificado digital pueden ser víctimas de *phishing* y no protegen la información transmitida de los usuarios.

La detección de información falsa es una necesidad cada vez más urgente para brindar mayor certeza sobre la información utilizada debido a que dicha información es utilizada para tomar decisiones. En este sentido, se encontró que solo un sitio web, del sector público, tiene implementado un procedimiento para verificar la información personal a través del uso de la tarjeta para votar expedida por el Instituto Nacional Electoral (INE).

Se ha encontrado que el aviso de privacidad se encuentra disponible en el 100% de los sitios web. La ley de privacidad de datos que está vigente en México se puede consultar en http://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf, y busca promover, fomentar y difundir una cultura de protección de datos personales entre dependencias gubernamentales, empresas privadas y sociedad en general.

Con esta información, se procede a responder las tres hipótesis definidas en el apartado 3.1.

En cuanto a la hipótesis 1, se ha encontrado que el 63% de la muestra utilizada tiene implementado un certificado digital y por lo tanto no se alcanza el 100%. El resultado es congruente con el estudio realizado por la Asociación Mexicana de Internet sobre protección de datos personales (AMIPCI, 2012), en dos aspectos: 1) se informa que el 32% de las empresas que almacenan algún dato personal desconocen las acciones a realizar y) se informa que el 53% de las empresas consideran que la protección de los datos representa gastos adicional.

En cuanto a la hipótesis 2, se ha encontrado que el 100% de los sitios web evaluados cuentan con una política de privacidad y está disponible para su consulta.

En cuanto a la hipótesis 3, se ha encontrado que el 2% de la muestra utilizada tiene implementado una técnica, herramienta o procedimiento para verificar la identidad del usuario y por lo tanto no se cumple el 100% de ausencia inicial. El sitio web de la ciudad de México (https://www.plataforma.cdmx.gob.mx/) solicita el número identificador OCR de la tarjeta para votar del INE, así como, la clave única de registro de población (CURP) que es expedida por el registro nacional de población e identificación personal (RENAPO) para crear una cuenta.

4.2. Proceso de registro utilizando el formulario web: problemas identificados

Como resultado de nuestro trabajo, encontramos los siguientes problemas:

Problema 1: durante el paso 3, muchos servidores web no utilizan protocolos de seguridad y certificados digitales para proteger la información de los usuarios. Esta acción representa un riesgo para la seguridad porque los intrusos pueden obtener dicha información.

Problema 2: durante el paso 4, el servidor web lleva a cabo la verificación en línea del formulario de registro web para asegurar que cada cuadro de texto esté completo. Sin embargo, el servidor web no verifica la legitimidad de la información del usuario.

Problema 3: cada nueva cuenta o nueva compra en línea representa que, los usuarios de Internet compartan su información personal y/o financiera con diferentes servidores web a través de Internet. Después de eso, los usuarios pierden el control sobre dicha información porque no gestionan el servidor web o la base de datos. Aunque, algunos países tienen leyes de privacidad muchos otros no.

Problema 4: en el caso de los sitios de redes sociales, los administradores del sistema no tienen información sobre los antecedentes criminales. Como resultado, los delincuentes pueden tener acceso a la información personal de muchos usuarios.

Problema 5: la información personal y financiera almacenada en una base de datos debe estar protegida por el proveedor del sistema. Sin embargo, ¿cómo podemos estar seguros de eso?.

Problema 6: el robo de identidad es un gran problema para los usuarios de Internet debido a las siguientes razones: dificultad para encontrar un perfil falso y el perfil falso puede afectar la reputación de la víctima.

Problema 7: cuando ocurre un crimen en Internet, la policía tiene problemas para rastrear la identidad real del criminal desde el perfil virtual usado para cometer el ataque.

Problema 8: en algunos casos, niños o jóvenes pueden tener acceso a material para adulto porque el sistema no puede verificar la edad real del usuario.

Como notas finales: 1) el formulario de registro web sigue siendo el mismo cuando otras aplicaciones han cambiado en los últimos años y 2) todos los días, muchos usuarios de Internet necesitan llenar un formulario de registro web para crear una nueva cuenta o para finalizar un compra en línea. Esta acción representa, para los usuarios de Internet, una tarea tediosa, que puede dar como resultado que los usuarios decidieran abandonar la acción.

4.3. Sitio de red social Facebook: resultados

Los participantes de la encuesta fueron $n=69$, encontrando que el 85.52% de los encuestados usaron su nombre real, y el 81.16% de los encuestados utilizaron su imagen en el perfil de Facebook. De esta manera, el 75.36% de los participantes comparten su ciudad natal, información de trabajo y pasatiempo. En este punto, nuestros resultados corroboran estudios previos y caracterizan el perfil del usuario mexicano.

Como nuevo resultado, se encontró que el 23.29% de los encuestados tienen como amigo a personas desconocidas en el mundo real. Además, el 88.41% de los encuestados desconocen si su cuenta es pública o no.

En cuanto a los resultados de la fase 2 y fase 3, se muestra en la Figura 2 que el ataque fue exitoso. En la Figura 2-a se observa el nombre, correo electrónico, fecha de nacimiento, y género utilizado para crear la cuenta, sin contratiempo. Como se ha demostrado en la Tabla 1, la mayoría de los SRS no tienen implementado una técnica, herramienta o procedimiento para verificar los datos utilizados en la creación de la cuenta.

La Figura 2-b muestra el resultado del perfil creado en el SRS. La información proporcionada tuvo como base la experiencia de los estudiantes que participaron en el proyecto con la intención de establecer credibilidad. Se buscó publicar mensajes diariamente por un periodo de un mes.

La Figura 2-c presenta el resultado de cierto número de solicitudes de amistad aceptadas. Las solicitudes fueron dirigidas a estudiantes de la universidad pero no se advirtió o solicito a conocidos su apoyo. En este sentido, se consiguió la aceptación de amistad en dos grupos.

Figura 2 – Ataque en el sitio de red social Facebook

Con esta información, se procede a responder las tres hipótesis definidas en el apartado 3.1. En cuanto a la hipótesis 4, se corrobora la hipótesis con un porcentaje del 23.29% de encuestados que confirmaron haber aceptado la invitación de amistad de al menos una persona. La información coincide con estudios de popularidad que indican sobre la importancia del número de amigos en los SRS. En cuanto a la hipótesis 5, se obtienen resultados similares a trabajos previos debido a que 75.36% de los encuestados afirmaron haber publicado información personal y de contacto. En cuanto a la hipótesis 6, se corrobora la hipótesis debido a que ningún SRS verifica la información personal utilizada para completar un perfil.

4.4.Sitio de red social Facebook: problemas identificados

Como resultado de nuestro trabajo, encontramos los siguientes problemas.

Problema 1: los sitios de redes sociales no tienen mecanismos de seguridad para verificar la información personal enviada por los usuarios. En consecuencia, el crimen organizado, criminales y usuarios malintencionados pueden crear cuentas falsas.

Problema 2: los usuarios no tienen una buena educación en términos de privacidad debido a que comparten mucha información personal en su muro, tales como: sentimientos, comentarios, chismes, fotografías, y más, sin preocuparse de quién o quiénes pueden verlo.

Problema 3: los usuarios no respetan la privacidad de los amigos cuando publican una fotografía. Esta acción afecta directamente a la privacidad de cada persona que aparece en la imagen.

Problema 4: la policía no puede rastrear fácilmente y rápidamente la información personal del atacante cuando aparece un problema de seguridad. Por ejemplo, en una investigación de *grooming*.

Problema 5: muchas cuentas se pueden crear usando la información personal de otra persona. El robo de identidad es un gran problema de seguridad en los sitios de redes sociales.

5. Conclusiones y Trabajo Futuro

En este trabajo, se ha evaluado las implicaciones de seguridad y privacidad en el uso de sitios de redes sociales, corroborando los resultados anteriores. Se ha demostrado que, los usuarios publican y comparten más información que en cualquier otro momento de la historia de la humanidad; sin considerar las consecuencias a su privacidad y seguridad. Es alarmante la cantidad de información que se puede obtener de una persona a través de su perfil de usuario y lo fácil que es tener acercamiento con la persona deseada (víctima).

Por otra parte, se ha demostrado que el formulario de registro web es el eslabón más débil en la cadena de seguridad porque la información no es verificada por ningún mecanismo. Debido a que día a día, los usuarios de Internet se ven forzados a compartir su información, se pierde el control de dicha información debido a que se delega o se comparte su administración con una empresa. El formulario de registro web es utilizado en el proceso de registro por todos los servicios web, lo que significa que el crimen organizado, usuarios criminales y malintencionados pueden crear cuentas falsas y realizas acciones delictivas, dificultando su conexión. Como resultado, el robo y suplantación de identidad son un gran problema para los usuarios de Internet y la policía.

En consecuencia al presente estudio, se encuentra en evaluación un procedimiento para medir el nivel de privacidad que tiene una persona en su cuenta de red social. La intención del procedimiento es indicar al usuario cuáles son los errores que se encuentra cometiendo que afectan su privacidad y seguridad.

Referencias

AMIPCI. (2012). Estudio de protección de datos personales entre usuarios y empresas. Ciudad de México: Asociación Mexicana de Internet.

AMIPCI. (2016). Estudio comercio electrónico en México 2016. Ciudad de México: Asociación Mexicana de Internet.

Belanger, F., J.S., M., & Smith, W. (2002). Trustworthiness in electronic commerce: the role of privacy, security and site attributes. The Journal of Strategic Information Systems, 245–270.

Boyd, D., & Ellison, N. (2007). Social Network Sites: Definition, History, and Scholarship. Journal of Computer-Mediated Communication, 210–230.

Dwyer, C., Hiltz, S., & Passerini, K. (2007). Trust and Privacy Concern with Social Networking Sites: A Comparison of Facebook and MySpace. Proceedings of 13th Americas Conferences on Information Systems.

Ellison, N., Steinfield, C., & Lampe, C. (2007). The Benefits of Facebook "Friends: 'Social Capital and College Students' Use of Online Social Network Sites. Journal of Computer-Mediated Communication, 1143–1168.

Facebook. (2015 de 12 de 11). Policy. Obtenido de https://www.facebook.com/policy.php

Gross, R. A. (2005). Information Revelation and Privacy in Online Social Networks. Proceedings of the Workshop on Privacy in the Electronic Society (71-80). New York: ACM.

Joinson, A. R.-d., Buchanan, T., & Paine Schofield, C. (2010). Privacy, Trust, and Self-Disclosure Online. Human-Computer Interaction, 1–24.

Kermek, D., & Bubas, G. (2000). Being connected to the Internet: Issues of privacy and security. Journal of Information and Organizational Sciences, 55–67.

Kimble, C., de Vasconcelos, J. B., & Rocha, Á. (2016). Competence management in knowledge intensive organizations using consensual knowledge and ontologies. Information Systems Frontiers, 18(6), 1119–1130.

Leitch, S., & Warren, M. (2009). Security Issues Challenging Facebook. Proceedings of the 7th Australian Information Security Management Conference, (137–142).

Li, J., Zhang, H., & Lu, X. (2016). Research on Acceptance Effect of Ideological and Political Education among College Students Based on Network Media. Iberian Journal of Information Systems and Technologies, 111–120.

Liebermann, Y., & Stashevsky, S. (2002). Perceived risks as barriers to Internet and e-commerce usage. Qualitative Market Research: An International Journal, 291–300.

Mekovec, R., & Hutinski, Z. (2012). The role of perceived privacy and perceived security in online market. Proceedings of the 35th International Convention of Information Communication Technology, Electronics and Microelectronics (1549–1554). Opatija: IEEE.

Mennecke, B., McNeill, D., Ganis, M., Roche, E., Bray, D., Konsynski, B., Lester, J. (2008). Second Life and Other Virtual Worlds: A Roadmap for Research. Communications of the Association for Information Systems, 371–388.

Ögütcü, G., Testik, Ö. & Chouseinoglou, O. (2015). Analysis of personal information security behavior and awareness. Computers & Security, 83–93.

Qi, J., Hao, L., & Xing, J. (2016). The research on the security Evaluation of the Electronic Commerce based on the cloud computing environment. Iberian Journal of Information Systems and Technologies, 131–139.

Sahinaslan, E., & Kantürk, A. (2009). Information security awareness and awareness creation methods in organizations. Proceedings of the 11th Acaemic Information Conference, (597–602). Sanliurfa.

Schrammel, J., Köffel, C., & Tscheligi, M. (2009). How Much do You Tell? Information Disclosure Behaviour in Different Types of Online Communities. Proceedings of the fourth international conference on Communities and technologies (275–284). New York: ACM.

Scott, J. (2004). Measuring dimensions of perceived e-business risks. Information Systems and e-Business Management, 31–55.

Stockton, R., & Cunningham, S. (2014). An Investigation into User Perceptions of Privacy and Trust and their Real-World Practices. Proceedings of the Tenth International Network Conference (139–149). United Kingdom: Pymouth University.

Tong, S. T., & Der, B. V. (2008). Too Much of a Good Thing? The Relationship Between Number of Friends and Interpersonal Impressions on Facebook. Journal of Computer-Mediated Communication, 531–549.

Wang, Y., Wang, Y., Lin, H., & Tang, T. (2003). Determinants of user acceptance of Internet banking: an empirical study. International Journal of Service Industry Management, 501–519.

Wroblewski, L. (2008). Web Form Design: Filling in the Blanks. Rosenfeld Media.