Técnica de protección para credenciales de autenticación en redes sociales y correo electrónico ante ataques phishing

Protection Technique for Authentication Credentials on Social Networks and Email from Phishing Attacks

Paola Andrea Noreña Cardona[1], Sergio Calderón Restrepo[2]

Institución Universitaria Tecnológico de Antioquia, Facultad de Ingeniería, Medellín, Colombia

Recibido: 20/04/2018 • Aprobado: 19/05/2018

Resumen

Una credencial de autenticación es una orden que autoriza el acceso a una red social, correo electrónico u otros sitios web que requieren información personal de un usuario registrado. El phishing (suplantación de identidad) es un ataque fraudulento desde sitios web engañosos a credenciales de autenticación. Algunos autores plantean enfoques basados en la detección y prevención de estos ataques phishing en redes sociales y correos electrónicos. Sin embargo, las cifras de estos ataques se continúan incrementando, debido a que los usuarios siguen incurriendo en errores como la falta de conocimiento, el descuido visual y la falta de atención, que facilitan estos ataques. En este artículo se realiza un análisis de los riesgos y causas de ataques phishing a credenciales de autenticación en redes sociales y correos electrónicos. Además, se propone una técnica de protección para estas credenciales, mediante procedimientos de fácil recordación. Los procedimientos de la técnica se realizan para prevenir los riesgos a partir del conocimiento, atención y cuidado visual del usuario. Así también, se aplica la técnica a algunos usuarios.

Palabras clave: seguridad de la información, sistema de software, ingeniería de software, servicios de redes sociales, correo electrónico.

Abstract

An authentication credential is an order that authorizes access to a social network, email, and other websites that require personal information from a registered user. Phishing is a based on detection and prevention of these phishing attacks, on attack from false websites to authentication credential. Some authors propose approaches such as lack social networks and emails. However, the number of these attacks continues to increase, because users continue to incur errors as lack of knowledge, visual carelessness and lack of inattention, which facilitate

[1] panorena@tdea.edu.co, [2] Sergio.Calderon@tulpep.com

these attacks. In this paper, we analyze risks and causes of phishing attacks to authentication credentials on social networks and emails. Also, we propose a protection technique for such credentials, using easy-to-remember procedures. These procedures are carried out to prevent risks from knowledge, attention and visual care of the user. As well, we apply the technique to some users.

Key words: *electronic mail, information security, social engineering, social networks services, software engineering, software system.*

1. Introducción

Una credencial de autenticación es una orden que consta de un identificador de usuario y contraseña. Este identificador puede además ser un certificado digital acompañado de una autenticación que autoriza el ingreso de una cuenta virtual a través de información personal en la red. Estas credenciales pueden utilizar dispositivos biométricos o series de preguntas que el usuario debe responder (Khonji, Iraqi & Jones, 2013). Las credenciales de autenticación se utilizan para validar la información de cuentas de usuario en sitios web como redes sociales y correos electrónicos (Marforio, et al., 2015).

Phishing es el acrónimo en inglés de *Password Harvesting Fishing* o cosechar y pescar contraseñas. Este acrónimo se traduce como suplantación de identidad, aunque se utiliza el término original. El *phishing* se usa con el propósito de recolectar ilegalmente información personal de credenciales de autenticación (nombres de usuarios y contraseñas) (Hong, 2012). A partir de estas credenciales los atacantes pueden acceder a información confidencial como perfiles en redes sociales, información de correo electrónico, información empresarial e información financiera como números de tarjeta de crédito, identificación bancaria, etc. (Microsoft, s.f.). El *Anti-Phishing Work Group* (APWG) define el *phishing* como un ataque fraudulento que usa ingeniería social, es decir, en la que el atacante (*phisher*) utiliza sitios web engañosos, mediante información sensitiva que permita el hurto de las credenciales de autenticación y demás información personal, para luego monetizar tal información (NCSA, 2013).

Para contrarrestar los ataques *phishing*, algunos autores presentan enfoques basados en software (Salem, Hossain & Kamala, 2010; Zhang, Hong & Cranor, 2007). También, otros autores proponen trabajos para detectar phishing a partir del uso de minería de datos (Nikulchev & Pluzhnik, 2014). Algunos autores plantean enfoques a partir de la detección de un ataque específico (Sheeram et al., 2010; Kontaxis et al., 2011; Mishra & Gaurav, 2012; Reddy, Radha & Jindal, 2011). Los anteriores enfoques se centran en detectar ataques *phishing* de forma general a partir de los sistemas (Sastoque & Botero, 2015), pero no preparan a los usuarios ante estos ataques y sólo algunos trabajan en redes sociales y correos electrónicos. Por otro lado, algunos autores intentan incluir en sus enfoques a los usuarios en estrategias de prevención de riesgos (Khonji, Iraqi & Jones, 2013; Atighetchi & Pal, 2009; Scott, Ghinea & Arachchilage, 2014). Sin embargo, no incluyen elementos para redes sociales y correos electrónicos.

Las cifras de ataques *phishing* a correo electrónico y redes sociales sigue en incremento (Prandini & Maggiore, 2013), ya que en general estos ataques afectan a usuarios vulnerables, que pueden ser comunes o de empresa. Pues, estos incurren en errores como falta de conocimiento de los ataques, descuido visual y la falta de atención a los indicadores de seguridad para reconocer un sitio falso, debido a su semejanza respecto al legítimo (Garera, et al., 2007). Estos errores siguen permitiendo estos ataques, que se traducen en un negocio para los atacantes, ya que monetizan la información hurtada obteniendo grandes sumas de dinero (NCSA, 2013).

De acuerdo a lo anterior, es necesario aumentar la protección en las credenciales de autenticación de redes sociales y correo electrónico. Por lo tanto, en este artículo se pretende analizar algunos riesgos y causas que ocasionan los ataques de *phishing*. A partir de ellos se propone una técnica que le permita al usuario conocer algunos procedimientos de fácil recordación que eviten el hurto de su información desde las credenciales de autenticación. Estos procedimientos ayudan a prevenir los riesgos de los usuarios desde aspectos como el conocimiento de estos ataques y la atención y cuidado que deben tener ante ellos.

Este artículo está organizado de la siguiente manera: En la sección 2 se incluye la metodología de investigación utilizada; en la sección 3 se presenta el marco conceptual; en la sección 4 se exponen los trabajos previos; en la sección 5 se define el problema; en la sección 6 se propone la solución. En la sección 7 se discuten los resultados. Finalmente se indican las conclusiones y el trabajo futuro.

2. Metodología

La investigación desarrollada para este artículo utilizó la metodología de *transferencia tecnológica* (Joode, 2012) que consiste en observar una necesidad en la industria y desarrollar la solución desde la academia. Las fases de esta metodología son planteamiento del problema (que se desarrolla a partir de la revisión de literatura y la necesidad), propuesta de solución y aplicación (a partir de la percepción de algunos usuarios).

3. Marco conceptual

3.1 Credenciales de autenticación

Una credencial es la combinación de una identidad y un autenticador en una orden que certifica y autoriza el ingreso de una cuenta virtual a través de datos personales en la red. Esta *identidad* se suele demostrar mediante un nombre de usuario de una cuenta, en compañía de un autenticador que comprueba la identidad solicitando información que la valide. Un *autenticador* puede tener varias formas, según el protocolo y el método de autenticación. Las credenciales de autenticación generalmente hurtadas son el usuario y la contraseña (Marforio et al., 2015).

Existen credenciales de autentificación para diferentes sitios en la red; cuando un usuario o servicio quiere acceder a un recurso de correo electrónico o red social, debe proporcionar información que demuestre su *identidad* (Marforio et al., 2015).

3.2 Phishing

El acrónimo *phishing* se define como un fraude informático (Samper & Bolaño, 2015) o un ataque fraudulento de ingeniería social y puede ser entendido observando una típica actividad de pesca (*fishing*), en donde un pescador ofrece un anzuelo a los pescados y espera a que ellos caigan en la trampa (Asanka et al., 2012). En el mundo cibernético, los *pescadores* siguen la misma estrategia; la diferencia en este caso, es que el anzuelo se convierte en sitio web falso con información sensitiva en la interfaz gráfica que demanda la información personal de las credenciales de autenticación del usuario que accede. Algunos usuarios caen en este anzuelo creyendo que estos sitios web son legítimos y responden a la información en las credenciales de autenticación (Purkait, 2012), en la *Fig. 1* se puede observar un ejemplo de la similitud en interfaz gráfica de un sitio falso de la red social Facebook.

Además de la interfaz gráfica, los ataques *phishing* intentan convencer a las personas para abrir un sitio falso desde espacios web gratuitos en internet y dominios personalizados (Asanka et al., 2012). Un ejemplo de estos dominios se suele presentar en la red social de *Facebook.com*, donde los atacantes obtienen nombres similares como: *Facebok.com*, o *Facebook-login.com*, en donde solo cambian algunos caracteres con similitud visual.

3.2.1 Fases del phishing

1. Visualización por las víctimas potenciales que reciben el ataque; 2. Ingreso de información por la víctima desde un sitio web, algunos incluyen la instalación

de un malware (software malicioso). 3. Monetización de la información hurtada (Purkait, 2012).

3.2.2 Tipos de phishing

Existen varios tipos de ataques *phishing* y en la mayoría de los casos el motivo principal del atacante es realizar un robo de identidad para beneficio económico a partir de la información de sus credenciales en redes sociales o correo electrónico; eventualmente, el atacante puede adentrarse en la vida social del individuo y realizar estafas utilizando *phishing* (Hong, 2012). En la Tabla 1 se presentan algunos ataques *phishing* en redes sociales y en correo electrónico.

Tabla 1
Ataques de phishing en redes sociales y correo electrónico

Ataques phishing	¿En qué consiste?
Enlace con software malicioso	Técnica en la que el atacante envía un enlace a una página web. Se pide descargar y abrir un archivo adjunto al usuario haciéndolo pasar por algo importante como información de entidad bancaria. Una vez abierto el archivo, el software malicioso empieza a funcionar y en muchos casos, a enviar información confidencial a través de internet.
Mensajería instantánea	El usuario recibe mensajes que lo llevan a un sitio fraudulento para que posteriormente ingrese la información.
Correo / Spam	Se envía el mismo correo electrónico a millones de usuarios, requiriendo llenar información confidencial en detalle. Esta información es la que se utiliza para actividades ilegales. La mayoría de los mensajes tienen notas urgentes que piden al usuario ingresar credenciales para actualizar información, cambiar detalles o verificar la cuenta.
Pass-the-Hash (PtH)	El atacante captura las credenciales de inicio de sesión en un computador y entonces las utiliza para autenticarse en otros equipos a través de la red. El ataque se roba el hash de la contraseña en vez del texto plano.
Keystroke logger	Aplicación maliciosa que captura las credenciales mientras son escritas por el usuario y se envían al atacante.

Fuente: Jungles et al., 2012; Phishing.org, 2011

4. Trabajos previos

El software "cantina" se desarrolla para la detección de sitios web de *phishing* (Zhang, Hong & Cranor, 2007) y el sistema experto para detectar *phishing* en sitios web basado en sus características (Sheeram et al., 2010). Ambos trabajos presentan detección de ataques *phishing* mediante el uso de sistemas. Sin embargo, lo hacen para diferentes enlaces *phishing*. El uso de algoritmos de minería de datos (Nikulchev & Pluzhnik, 2014) y metodología *phishing* con teoría del caos (Dadkhah, Lyashenko & Jazi, 2015), son enfoques propuestos para la detección automática de *phishing* a partir de la minería de datos, pero se basan en enlaces *phishing* de información general. Detección de clonación del perfil en una red social (Kontaxis et al., 2011), detección de ataques de *phishing* basado en la categorización de enlaces (Atighetchi & Pal, 2009),

contenido basado en *anti-phishing* (Mishra & Gaurav, 2012) y detección de páginas *phishing* basada en relaciones asociadas (Reddy, Radha & Jindal, 2011) son trabajos que se centran en la detección de un tipo de ataque. Sin embargo, sólo algunos se emplean en redes sociales y correos electrónicos.

Los anteriores enfoques se centran en detectar ataques *phishing* de forma general a partir de los sistemas (Sastoque & Botero, 2015), y sólo algunos ayudan en la detección de *phishing* en redes sociales y correos electrónicos.

Campaña *anti-phishing* (Khonji, Iraqi & Jones, 2013), juego educativo *anti-phishing* con elementos de conocimiento para preparar a los estudiantes en la identificación de enlaces *phishing* (Scott, Ghinea & Arachchilage, 2014); y un marco de trabajo para que usuarios identifiquen características en enlaces *phishing* (Garera et al., 2007) son trabajos de autores que presentan estrategias de prevención de riesgos ante ataques *phishing* para los usuarios. Sin embargo, estos enfoques no incluyen elementos de prevención para redes sociales y correos electrónicos.

5. Problema

A pesar que se está trabajando en la mitigación de los ataques *phishing* mediante diferentes sistemas, la cifra de ataques *phishing* a correos electrónicos y redes sociales continúa aumentando. Según los informes y estudios realizados por el Registro de Direcciones de Internet para Latinoamérica y el Caribe (LACNIC), dado su impacto económico, los ataques de *phishing* a correos electrónicos y redes sociales han aumentado en Brasil, Argentina, Colombia, México y Chile en un 20% más de lo que han crecido a nivel global (Prandini & Maggiore, 2013; Salem, Hossain & Kamala, 2010). La información personal de los usuarios (números de teléfonos personales, lugares de residencia, sitios que frecuentan, información familiar y fotos privadas) en redes sociales como Facebook, Twitter y LinkedIn es generalmente de interés para los atacantes. De igual modo la información confidencial que se envía por el correo electrónico, personal o laboral, ya que el hurto de esta información puede ser monetizada (Enough-is-Enough, 2013).

Los atacantes se aprovechan de la vulnerabilidad de los usuarios y a pesar que también se trabaja en enfoques de prevención para ellos, se siguen utilizando estrategias como la falta de conocimiento en aplicaciones, correos, páginas web; el descuido visual y la falta de atención frente a los indicadores de seguridad para reconocer un sitio fraudulento (APWG, 2013; Dhamija, Tygar & Hearst, 2006). Esto muestra la necesidad de conocer los riesgos y las causas de estos ataques y la forma en que los usuarios pueden prevenirlos (APWG, 2013).

6. Solución

6.1 Análisis de riesgos en credenciales de autenticación en redes sociales y correo electrónico ante ataques phishing

La Tabla 2 presenta los principales riesgos y causas en las credenciales de redes sociales y correo electrónico. Estos riesgos inciden por ataques *phishing*, y son los de más crecimiento a través de los últimos años (NCSA, 2010). Esta tabla da a conocer los ataques *phishing* comunes que se presentan en redes sociales y mensajería instantánea en correos electrónicos.

Tabla 2
Riesgos de credenciales en redes sociales y correo electrónico

Ataques phishing	Riesgos	Causas
Enlaces con software malicioso	Pueden llevar a sitios de phishing, infectar el equipo con malware y robar información personal.	Los enlaces suelen venir de un atacante utilizando el nombre de empresa conocida.
Mensajería instantánea	Mensajes que intentan hacer que el usuario actualice la contraseña, información personal o descargue algún adjunto malicioso.	Como en el caso de los enlaces maliciosos, aparentan venir de fuentes de confianza como amigos de la red social o marcas reconocidas que suelen generar previa confianza.
Correo / Spam	La cuenta de correo o mensajería de redes sociales podría verse comprometida, y desde ella enviar la misma propaganda a todos los contactos para que se siga propagando.	Estos correos suelen tener éxito debido a que utilizan información pornográfica o de interés general, como noticias actuales o falsas loterías.
Pass-the-Hash (PtH)	El atacante se apodera de las credenciales de inicio de sesión.	Mala administración en cuanto a privilegios locales del usuario, o del servicio web que se esté usando.
Keystroke Logger	El atacante obtiene toda la información que se ingresa por el teclado; esto incluye usuarios y contraseñas.	Aplicaciones maliciosas que se instalan en el equipo del usuario.

Fuente: Jungles et al., 2012; Phishing.org, 2011; APWG, 2013

6.2 Técnica de protección para credenciales en redes sociales y correo electrónico ante ataques phishing

Una técnica es un conjunto de procedimientos o normas que de forma ordenada cumplen unas pautas para llegar a un cierto fin. La técnica de protección tiene el propósito de prevenir estrategias que utilizan los atacantes (falta de conocimiento, descuido visual y falta de atención), utilizando procedimientos de fácil recordación que permitan conocer los sitios web, tener cuidado visual y atención mediante gráficos y normas que los usuarios pueden utilizar. En las empresas puede funcionar como un recurso adicional a los sistemas y en usuarios comunes como su principal apoyo para proteger sus credenciales de autenticación. La técnica congrega 4 fases que agrupan normas para prevenir los riesgos expuestos previamente ante ataques *phishing* a credenciales de autenticación de redes sociales y correo electrónicos como se observa en la *Fig.1.*

Fig. 1. Técnica de protección a credenciales de autenticación

6.2.1 Prevención al ingresar a la red social o al correo electrónico

La protección proactiva contra el *phishing* debe iniciar antes de ingresar al sitio web.

Evitar el acceso a enlaces de un tercero: es indispensable digitar siempre el sitio web legítimo en la barra de direcciones y no ingresar a enlaces que llegan mediante mensajería de redes sociales o correos electrónicos. De este modo, el ingreso a los sitios de internet a través de un enlace de un tercero se puede evitar, ya que el atacante aprovecha la confianza generada por la fuente a los usuarios y los direccionan a un sitio web falso, teniendo éxito en el ataque (Jakobsson, 2007). La *Fig.2.* presenta un ataque *phishing* que contiene un enlace con software malicioso haciendo clic sobre él, este tipo de ataque se debe evitar.

Fig. 2. Mensaje de confianza con sitio falso (Jakobsson, 2007).

Eludir el acceso desde gráficos: los logos, diseños, gráficos y textos de la página pueden dar acceso a ataques *phishing*, haciendo creer al usuario que el sitio es completamente legítimo al tener una apariencia similar en su interfaz gráfica, por tal razón se debe eludir el acceso desde gráficos. Ya que todos estos aspectos pueden ser duplicados por el atacante (Dhamija, Tygar & Hearst, 2006).

6.2.2 Verificación del dominio

Al ingresar a un sitio web el usuario debe cerciorarse teniendo atención y cuidado visual que el dominio (nombre del sitio web) corresponde al legítimo, por ejemplo: *www.facebook.com*, *www.outlook.com*. Es necesario validar en detalle el nombre del dominio, pues como se mencionó antes pueden ser modificados en algún carácter y recibir un ataque de *phishing* (NCSA, 2010), ya que los atacantes pueden cambiar algunas letras y hacer que el sitio tenga una semejanza al legítimo, Por ejemplo: *www.outlok.com* (sin doble 'o'). *www.myfacebook.com* (con 'my-') o simplemente se puede mostrar la dirección IP como se muestra en la *Fig. 3*. Los atacantes aprovechan cualquier descuido de los usuarios en la premura y agilidad de realizar diferentes procesos en el trabajo o en sus actividades que se realizan en modo multitarea (varias tareas al mismo tiempo).

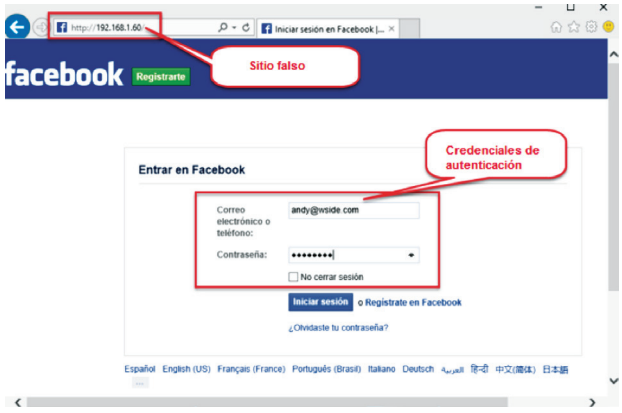

Fig. 3. Phishing en credenciales de autenticación de red social

6.2.3 Análisis de indicadores de seguridad

En el análisis de indicadores de seguridad es indispensable conocer cómo se pueden identificar, para ello se deben tener en cuenta tres aspectos fundamentales (Marforio et al., 2015).

Identificar indicador del dominio principal: los navegadores web más populares del mercado como Internet Explorer, Mozilla Firefox y Google Chrome, identifican el dominio principal del sitio web al cual se está ingresando, resaltando el dominio con negrilla como se puede observar en la *Fig. 4*. Por lo tanto, el sentido de observación y atención se debe agudizar para la verificación de este indicador y así, asegurar el ingreso al sitio web legítimo.

Fig. 4. Dominio principal resaltado en Internet Explorer

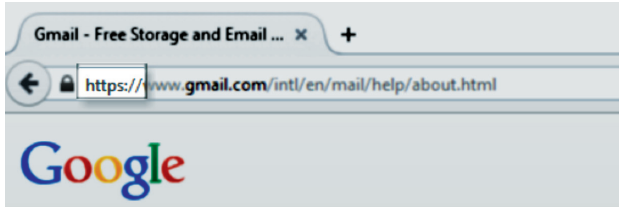

Fig. 5. Indicador Https en Gmail

Observar indicador de seguridad HTTPS: El indicador de seguridad HTTPS (siglas en inglés de Hypertext Transfer Protocol Secure, protocolo destinado a la transferencia segura de datos de Hipertexto), es un mecanismo común de seguridad adaptado para proteger la sesión, ya que la comunicación se transmite de forma cifrada (NCSA, 2010). La mayoría de redes sociales o páginas de correo electrónico lo usan como se puede observar en la *Fig. 5*., en la barra de direcciones siempre se antepone el HTTPS antes del dominio. Por ejemplo: ***https://****www.facebook.com*. La ausencia de este indicador representa un riesgo potencial de un ataque *phishing*, por lo que se requiere tanto el conocimiento de este indicador como la atención y cuidado visual para detectarlo.

Buscar indicador de certificado digital

Todos los sitios web deben tener un certificado o firma digital para que sean confiables; este certificado se representa a través de un candado en la parte derecha de la barra de direcciones. Si el sitio es falso, el certificado y reporte no corresponderá con el del sitio legítimo. En la *Fig. 6.* se muestra el candado en la barra de direcciones del navegador como un indicador de seguridad que se debe tener en cuenta para su acceso. Por lo tanto, se requiere conocerlo y buscarlo en la respectiva barra.

Fig. 6. Certificado digital en Mozilla e Internet Explorer

6.2.4 Prevención en la administración de credenciales al inicio de sesión

Generalmente un usuario asigna la misma clave para sus cuentas (correo, banco, red social, etc.) (NCSA, 2010) y pocas veces cambia la contraseña de sus cuentas en el transcurso del tiempo (NCSA, 2012; 2013). Agravando esto, el contenido de las contraseñas frecuentemente tiene combinaciones fáciles de tomar por los atacantes (Joode, 2012). De esta manera, es de vital importancia utilizar una contraseña segura que contenga combinaciones de letras mayúsculas, caracteres especiales y números, además debe ser diferente la de cada sitio de red social y de correos electrónicos, por ejemplo: Ert254*. Así, en caso de que el atacante logre hurtar una credencial de autenticación, no tendrá asegurado el acceso a las demás.

7. Resultados y discusión

La técnica de protección para credenciales de autenticación en redes sociales y correo electrónico se

aplica a algunos usuarios como auxiliares de gestión de datos y cajeros de supermercados, con el objetivo de tomar una muestra de 10 usuarios. Para obtener los resultados se utilizan do etapas la primera consiste en utilizar un sitio falso sin el previo conocimiento de la técnica y se realiza un cuestionario. Posteriormente se realiza la segunda etapa utilizando técnica y se realiza otro cuestionario. Estos fueron los resultados.

7.1 Etapa 1. Sin la técnica

¿Considera que el sitio era realmente el sitio de la red social?

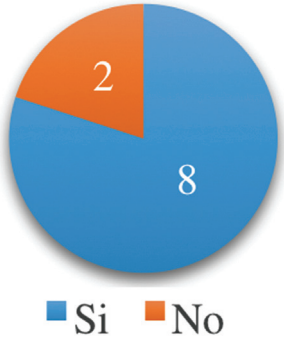

Fig. 7. Pregunta 1

La mayoría de usuarios no tuvo precaución al ingresar su información en las credenciales de la red social, consideran que se trataba del sitio legítimo, debido a que su apariencia era muy similar, Sólo 2 de los analistas de datos tuvieron precaución como se puede ver en la *Fig. 7.*

¿Qué tiene en cuenta a la hora de validar si un sitio es *legítimo?*

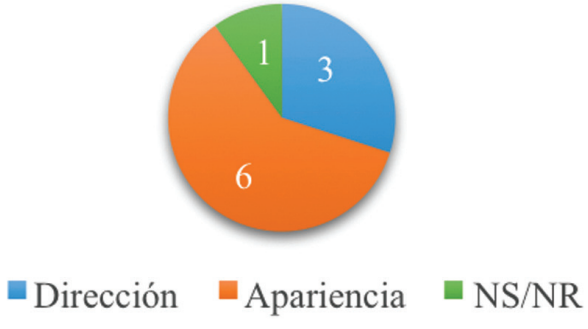

Fig. 8. Pregunta 2

A la hora de validar el sitio legítimo, la mayoría usuarios mencionan que intentan fijarse en la apariencia, es decir que le dan más importancia a la apariencia que al contenido de la dirección y 3 lo hacen desde la dirección.

¿Por qué cree que no inició sesión en el primer intento?

Fig. 9. Pregunta 3

Se obtuvo la percepción de los usuarios en la misma cantidad ya que algunos creen que se cayó el internet y otros no saben porque no se pudo acceder al sitio web.

¿Sabe que es phishing?, Si la respuesta es sí, indique con sus palabras que es.

Hubo la misma cantidad de usuarios que conocían el término y los que no lo conocían y en la respuesta abierta quienes conocían el término indicaron que era el hurto de las contraseñas, a pesar de saberlo incurrieron en el error de ingresar su información en las credenciales del sitio falso.

Fig. 10. Pregunta 4

7. http://www.radios.com.co/region/bogota/#w-radio-fm-99-9-bogota2 Etapa 2. Con la técnica

Se proporciona la técnica físicamente como guía para seguir los procedimientos.

¿Cree que esta técnica le ayuda *a recordar fácilmente la prevención ante phishing?*

Fig. 11. Pregunta 5

La mayoría de usuarios indica que al seguir los procedimientos de la técnica pueden evitar el *phishing* para sus credenciales en redes sociales y correos electrónicos, y les parece que es fácil su recordación por lo que muestra aceptación y en el cumplimiento de los ítems.

¿Considera que la técnica agrupa los procedimientos necesarios para proteger las credenciales?

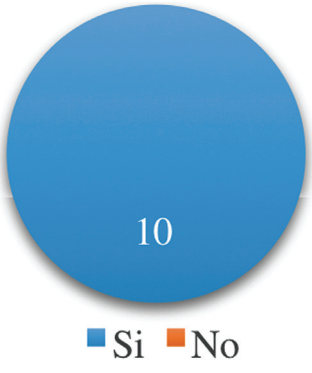

Fig. 12. Pregunta 6

Para los usuarios la técnica es apropiada junto con los procedimientos que agrupan para proteger las credenciales de redes sociales y correo electrónico ante los ataques *phishing*.

En esta aplicación de la técnica se puede analizar que la causa principal por la que los usuarios pierden fácilmente sus credenciales es efectivamente la falta de conocimiento sobre ataques *phishing*, el descuido visual y la falta de atención en el contenido o la fuente del enlace. De este modo los diferentes usuarios utilizaron la técnica y sus procedimientos y coincidieron en que es una práctica fácil que pueden seguir utilizando en su cotidianidad con un mayor conocimiento, cuidado y atención.

8. Conclusiones

Los ataques *phishing* en credenciales de redes sociales y correo electrónico, aprovechan la vulnerabilidad de los usuarios por la falta de conocimiento en estos ataques, descuido visual y falta de atención en los caracteres del dominio y la interfaz gráfica de los sitios falsos. El desconocimiento de estas estrategias, riesgos y causas es uno de los factores claves que utilizan para hurtar las credenciales. De acuerdo a esto, en este trabajo se realiza un compendio de los riesgos de algunos ataques *phishing* en credenciales de redes sociales y correo electrónico.

Adicionalmente, para evitar estos ataques se define una técnica que condensa una serie de procedimientos para lograr una protección, ante los ataques *phising* en las credenciales de autenticación de redes sociales y correos electrónicos, por parte del usuario como una herramienta de prevención. Así, puede ser incorporada como una práctica cotidiana para usuarios comunes. Para los usuarios de empresa puede apoyar en este proceso de prevención en adición a los sistemas utilizados anti-*phishing*.

Como trabajo futuro se pueden contemplar estrategias que integren tanto a los usuarios como a los sistemas para prevenir ataques phishing. También se pueden implementar estrategias interactivas que permitan capacitar a los usuarios ante ataques *phishing*.

Referencias

APWG, Anti-phishing Working Group. (2013). Phishing Activity Trends Reports. Recuperado de: http://docs.apwg.org/reports/apwg_trends_report_q1_2013.pdf

APWG, Antiphishing Working Group. (2012). Global Phishing Survey: Trends and Domain Name Use in 1H2012, *Tecnhical report*, An APWG industry advisory.

Asanka, N., Arachchilage, G., Love, S. & Scott, M. (2012). Designing a Mobile Game to Teach Conceptual Knowledge of Avoiding Phishing Attacks. *International Journal for e-Learning Security (IJeLS), 2*(1), 127-132.

Atighetchi, M. & Pal, P. (2009). Attribute-Based Prevention of Phishing Attacks. *2009 Eighth IEEE International Symposium on Network Computing and Applications*, (pp. 266-269). Cambridge, MA.

Dadkhah, M., Lyashenko, V. & Jazi, M. (2015). Methodology of the Chaos Theory in research of phishing attacks. *International Journal of Academic Research*, *7*(1). DOI: 10.7813/2075-4124.2015/7-1/A.26

Dhamija, R., Tygar, J. D. & Hearst, M. (2006). Why Phishing Works. *Proceeding, CHI '06 Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, (pp. 581-590). Boston, MA. Recuperado de: http://people.ischool.berkeley.edu/~tygar/papers/Phishing/why_phishing_works.pdf

Enough-is-Enough. (2013). Social Media Statistics. *Report document*, Recuperado de: http://www.internetsafety101.org/Socialmediastats.htm

Garera, S., Provos, N., Chew, M. & Rubin, A. D. A. (2007). Framework for detection and measurement of phishing attacks, *WORM '07 Proceedings of the 2007 ACM workshop on Recurring malcode*, (pp. 1-8). Alexandria, VA. Recuperado de: https://dl.acm.org/citation.cfm?id=1314391

Hong, J. (2012). The State of Phishing Attacks, *Communications of the ACM*", (8), 74-81.

Jakobsson, M. (2007). The human factor in phishing. *3rd TIPPI Workshop*, *Trustworthy Interfaces for Passwords and Personal Information*, (pp. 1-19). Standford. Recuperado de: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.68.8721&rep=rep1&type=pdf

Joode, D. d. (2012). Does password fatigue increase the risk on a phishing attack? Master Thesis, directed by M.V. Zaanen and J.J. Paijmans, Tilburg University, The Netherlands.

Khonji, M., Iraqi, Y. & Jones, A. (2013). Phishing Detection: A Literature Survey. *IEEE Communications Surveys & Tutorials*, *15*(4), 2091-2121.

Kontaxis, G., Polakis, I., Ioannidis, S. & Markatos, E. P. (2011). Detecting social network profile cloning. *2011 IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops),* (pp. 295-300). Seattle, WA. Recuperado de: https://ieeexplore.ieee.org/document/5766886

Marforio, C., Jayaram Masti, R., Soriente, C., Kostiainen, K. & Capkun, S. (2015). Personalized Security Indicators to Detect Application Phishing Attacks in Mobile Platforms. *Cryptography and Security,* pp. 1-15, Recuperado de: https://arxiv.org/pdf/1502.06824.pdf

Microsoft, (s.f.). Introducción técnica a las credenciales almacenadas y almacenadas en caché. Recuperado de: https://technet.microsoft.com/es-es/library/hh994565(v=ws.11).aspx

Mishra, M. & Gaurav, J. (2012). A Preventive Anti-Phishing Technique using Code word. *International Journal of Computer Science and Information Technologies*, *3*(3), 4248-4250.

NCSA, Norton and Zogby International. (2010). 2010 NCSA / Norton by Symantec Online Safety Study", *Technical Document*, vol.12.

NCSA, National Cyber Security Alliance and McAfee. (2012). 2012 NCSA / McAfee Online Safety Survey. *Technical Document*, vol. 11.

NCSA, National Cyber Security Alliance and McAfee and PayPal. (2013). 2013 National Online Safety Study. *Technical Document*, vol. 7.

Nikulchev, E., & Pluzhnik, E. (2014). Study of Chaos in the Traffic of Computer Networks. *International Journal of Advanced Computer Science and Applications*, *5*(9), 60-62.

Jungles, P., Simos, M., Margosis, A., Grimes, R. & Robinson, L. (2012). Techniques, Mitigating Pass-the-Hash (PtH) Attacks and Other Credential Theft. *Technical Document*, vol. 82.

Phishing.org. (2011). Phishing techniques. *Report document.* Recuperado de: http://www.phishing.org/phishing-techniques/.

Prandini, P. & Maggiore, M. L. (2013). Ciberdelito en América Latina y el Caribe, una visión desde la sociedad civil. *proyecto amparo*. Recuperado de: http://www.proyectoamparo.net/files/ciberdelito_lac_lacnic_amparo_estudios2013_completo_vfinal.pdf

Purkait, S. (2012). Factors that influence internet Phishing website. *The IUP Journal of Information Technology*, *7*(3), 7-38.

Reddy, V., Radha, V. & Jindal, M. (2011). Client Side protection from Phishing attack. *International Journal of Advanced Engineering Sciences and Technologies*, *3*(1), 39-45.

Salem, O., Hossain, A. & Kamala, M. (2010). Awareness Program and AI based Tool to Reduce Risk of Phishing Attacks. *2010 10th IEEE International Conference on Computer and Information Technology*, (pp. 1418-1423). Bradford. Recuperado de: https://ieeexplore.ieee.org/document/5577836

Samper, J. & Bolaño, M. R. (2015). Seguridad informática en el siglo xx: una perspectiva jurídica tecnológica enfocada hacia las organizaciones nacionales y mundiales. *Publicaciones e Investigación*, (9), 153-162.

Sastoque, D. & Botero, R. (2015). Técnicas de detección y control de phishing. *Cuaderno Activa,* (7), 75-81.

Scott, M. J., Ghinea, G. & Arachchilage, N. A. G. (2014). Assessing the Role of Conceptual Knowledge in an Anti-Phishing Educational Game. *2014 IEEE 14th International Conference on Advanced Learning Technologies*, (pp. 218-218). Athens. Recuperado de: https://ieeexplore.ieee.org/document/6901441

Sheeram, V., Suban, M., Shanthi, P. & Manjula, K. (2010). Anti-phishing detection of phishing attacks using genetic algorithm. *2010 International Conference on Communication Control and Computing Technologies*, (pp. 447-450). Ramanathapuram. Recuperado de: https://ieeexplore.ieee.org/document/5670593

Wohlin, C., Runeson, P., Höst, M., Ohlsson, M. C., Regnell, B. & Wesslén, A. (2012). *Experimentation in software engineering*. New York: Springer Science & Business Media.

Zhang, Y., Hong, J. I. & Cranor, L. F. (2007). Cantina: a content-based approach to detecting phishing web sites. *WWW '07 Proceedings of the 16th international conference on World Wide Web*, (pp. 639-648). Hanoi. Recuperado de: https://www.cs.cmu.edu/~jasonh/publications/www2007-cantina-final.pdf