Published on *Revista .Seguridad* (https://revista.seguridad.unam.mx)

REDES SOCIALES, ENTRE LA INGENIERÍA SOCIAL Y LOS RIESGOS A LA PRIVACIDAD

Jeffrey Steve Borbón Sanabria

ataque

numero-12

En nuestro día a día, cada vez es más común el uso de las redes sociales. Hoy, ya no resulta extraño escuchar términos como Facebook, Twitter, e incluso Linkedin y FourSquare. La penetración de las redes de datos a partir del uso de dispositivos móviles, como teléfonos celulares, smarthphones, tablets, entre otros medios, ha facilitado el uso de este tipo de aplicaciones, portales y herramientas, transformándolas en parte de la vida diaria.

Sin embargo, como dice el adagio popular "no todo lo que brilla es oro", ya que en meses recientes, este tipo de aplicaciones y portales han enfrentado una gran cantidad de críticas por el manejo que tienen con la privacidad de la información publicada por sus usuarios, los controles de seguridad dentro de las aplicaciones y servicios prestados, así como con el manejo de la información una vez que el usuario ha cerrado su cuenta, o ha dejado de usar por un largo tiempo la herramienta.

Para ejemplificar este punto, se puede mencionar la situación acontecida con la red social Facebook y el buscador Google, el cual sin autorización comenzó desde hace unos días a indexar [1] (buscar y mostrar en sus resultados de búsqueda) los comentarios de muro que los usuarios realizan.

De la privacidad

Diseñadas para seducir, y provocar que compartamos grandes cantidades de información personal, las

redes sociales se han transformado en parteaguas de la privacidad en línea. Comúnmente, los usuarios son acusados de estar desinformados de los problemas relacionados, dejando el debate abierto.

Es cierto, actualmente no existe un marco de trabajo ni instancias regulatorias que guíen por completo lo que debemos o no publicar. La necesidad de tener certidumbre sobre la propiedad de lo que publicamos, es una de las tareas pendientes de las redes sociales.

Los riesgos a la privacidad parecen estar por todas partes; por ejemplo, al intervenir una comunicación, el robo de identidad, el phishing, fuga de información, entre otras. Esta consideración hace necesario que los usuarios estemos cada vez más conscientes de los cambios que los desarrolladores de estas tecnologías implementan, para así aprovecharlos, y no estar expuestos.

De no hacerlo, corremos el peligro que estos cambios dejen abierta la oportunidad de hurgar en la privacidad. En primera instancia, es importante comentar que, en la mayoría de los casos, son los propios usuarios quienes revelan deliberadamente información privada a través de estas tecnologías, el correo electrónico y foros públicos.

La privacidad se vuelve un tópico clave. Los usuarios experimentan una confrontación entre el uso y los riesgos, de ser titular de una red social. Algunos son lo suficientemente audaces para percibir los cambios realizados en redes sociales; pero otros no.

A estos últimos quisiera dedicar el siguiente contenido, la reflexión de que la vida privada de cada una de las personas debe representar una noción central que haga comprender las encrucijadas a las que nos podemos enfrentar al ser asiduos a estas tecnologías.

Hasta hace algunos años, los usuarios aún veíamos con cierta lejanía el uso de las redes sociales; hoy, las usamos con naturalidad para tener comunicación “cercana” con amigos, familiares, conocidos y, aunque peligroso, con desconocidos también.

Pero, ¿qué hay con la información que publico, comparto y avalo? En primera instancia, hay que reconocer y ser conscientes de que todo lo que "pongamos en línea", tenderá e alguna u otra forma, a hacerse del dominio público, y es esta parte de sensibilidad la que más debemos de desarrollar para mantener bajo control la integridad de nuestra privacidad.

La privacidad no debe asumirse como algo acabado, ni tampoco caer en el supuesto de que siempre estará en riesgo. El sentido común y una postura responsable acerca de lo que publicamos, serán de gran ayuda.

¿Qué debemos entender por privacidad?

La privacidad es un conjunto de prácticas que dividen las cosas públicas y privadas. En este sentido, partamos del punto de vista en que la privacidad y la confidencialidad forman parte imperativa de la actividad computacional. Así, los problemas que los circundan sistemáticamente se vuelven un conflicto

para la seguridad de la información, en muchos de los casos van más allá de las ciencias de la computación.

A primera vista, estos problemas no tendrían tanta incidencia con un tema tan delicado como las consecuencias de ataques de ingeniería social, o tal vez un poco más peligroso como puede ser el tema de secuestro, extorsión e incluso "matoneo" o "bullying" a niños y jóvenes.

Entendiendo la ingeniería social

Una verdad absoluta, en términos de seguridad de la información, es decir que el eslabón más débil de la cadena es el usuario, el ser humano. Esto se traduce en que resulta más sencillo atacar a una persona y obtener información o una acción de ésta, que lograr vulnerar un sistema de información que se encuentra asegurado, blindado y protegido ante posibles atacantes. Esto nos lleva a la definición de la ingeniería social:

"Arte o ciencia de manipular a las personas para que realicen acciones que pueden ser o no del interés del objetivo", Chris Hadnagy [2]

"Acto de manipular personas y desarrollar acciones o divulgar información", [3]

En pocas palabras se puede hablar de la ingeniería social como una especie de hacking humano.

Ahora bien, así como en el hacking se deben realizar tareas de obtención de información (Information Gathering) de un posible objetivo, de igual forma la obtención de información es la base de los ataques de ingeniería social, con la diferencia que normalmente el objetivo del ataque será una persona, un humano y para ello es necesario cavar en todos los medios posibles que contengan posible información del blanco, es aquí donde aparece Internet y las redes sociales.

Desde la perspectiva de un ingeniero social, cualquier información acerca de la persona que se tiene como objetivo, puede aportar a formar un perfil o esquema de gustos, lugares que frecuenta, actividades que realiza, lugar y actividades del trabajo, entre otros datos. Es por ello que sin lugar a dudas, las redes sociales pueden proveer mucha información que puede ser de utilidad. A continuación, vamos a observar en una corta tabla que abarca algunos datos que se pueden llegar a obtener a través de estos sistemas de información:

Red Social/Plataforma	Información obtenida	Utilidad

Facebook/G+/Hi5/Badoo/...	• Estados de ánimo • Lugares visitados • Fotografías • Intereses • Familiares • Relaciones • Etc.	Estas redes proveen mucha información en general de la persona y sus contactos.
Twitter/Tuenti/BBM/...	• Estados de ánimo • Lugares visitados • Fotografías • Intereses	Establecer un listado de actividades, perfil psicológico, lugares visitados, información consultada y gustos de la persona.
MySpace/Grooveshark/LastFM/...	• Música escuchada • Gustos musicales	Establecer un perfil de preferencias y gustos musicales
Linkedin/...	• Estado laboral • Conocimientos • Asignación Salarial • Estudios en proceso	Identificar perfil laboral de la persona, trabajo actual, pasados, estudios, conocimientos, intereses de trabajo, etc.
Foursquare/...	• Lugares visitados • Gustos gastronómicos	Permite geoposicionar a las personas e identificar qué lugares suelen frecuentar o posibles movilizaciones a través de viajes.

Flickr/Picasa/...	• Lugares visitados • Gustos particulares • Entorno en que se desarrolla el individuo	Establecer un listado de actividades, perfil psicológico, lugares visitados y gustos de la persona.

Ahora bien, sabiendo que información se suele tener publicada por estos sistemas y teniendo en cuenta que esta información puede ser indexada en motores de búsqueda con o sin autorización expresa del usuario, es necesario validar que tanto se está compartiendo, para ello veamos cómo protegerse**.**

Entonces... ¿Cómo puedo protegerme?

El panorama que se puede percibir a través de noticias como estás (Navegación segura en Facebook [4] y Cookie espía en Facebook [5]) genera preocupación acerca de los alcances que pueden tener para nuestras vidas el compartir tanta información. Aquí quiero acuñar una frase muy empleada a nivel de seguridad: "Si está en internet, ya es público".

Afortunadamente, es posible cambiar esta situación a partir de un cambio en la cultura del uso de estos medios de comunicación, a continuación se presenta un listado de consejos para aplicar y protegernos de posibles ataques de ingeniería social usados para delinquir y afectar nuestra integridad y la de nuestras familias:

- Establezca los controles de privacidad a través de redes sociales permitiendo el acceso a información sólo a amigos y/o familiares.
- No publique información personal tal como dirección de residencia, teléfonos, lugares de trabajo, ocultando así información que puede ser empleada para establecer contacto y así realizar ataques o engaños contra usted y familiares o amigos cercanos.
- Evite realizar publicación de lugares que frecuenta o asiste.
- Evite publicar cambios de estado sentimental o problemas de este tipo, la información de este tipo puede ser empleada para establecer contacto ofreciendo ayuda o consejo y así ganar la confianza de la posible víctima.
- Evite seguir enlaces o notificaciones vía correo electrónico o mensajes de texto respecto a información personal o del perfil en redes sociales, puede ser un engaño para secuestrar las cuentas de usuario y la información en las redes almacenada.
- Dentro de las redes sociales evite dar clic a cualquier enlace, pueden enviarlo a sitios o descargar aplicaciones con código malicioso que pueden obtener información acerca de usted y quienes usen el equipo.

En los siguientes recursos podrá encontrar algunas guías o tutoriales que ilustran como aplicar estos controles o cambios en la seguridad de la información para sus cuentas de usuario en redes sociales:

- Configurando privacidad en Facebook [6]
- Configurando privacidad en Twitter [7]
- Configurando privacidad en Linkedin [8]
- Configurando privacidad en FourSquare [9]

Para finalizar unas frases que valen la pena analizar para ver como estamos en cuanto al aseguramiento de la información que publicamos en la red:

- Cuando viaja, usted no publica en la puerta de su hogar un aviso que dice: "No molestar, estoy de viaje"; sin embargo, en las redes sociales sí publica información, fotografías y nociones de que se encuentra en otro lugar de viaje, lo que equivaldría a lo mismo. Esta noticia [10] ilustra lo aquí mencionado anteriormente.
- Cuando se enfrenta a problemas sentimentales o familiares, no sale a la calle portando un cartel que diga: "Tengo problemas familiares"; sin embargo, sí los hace públicos por redes sociales.

Revisado lo anterior, es momento de hacernos una pregunta ¿Qué tanto estoy publicando y qué tipo de información publico en la red?

Como usuarios debemos estar mejor informados sobre todo lo relacionado a redes sociales, articular de manera efectiva la configuración de privacidad, dejando lo que necesitamos, y eliminando lo que no.

Información complementaria:

- "Guía de seguridad en redes sociales" - http://www.eset-la.com/pdf/documento_redes_sociales_baja.pdf
- "Solo dos de nueve redes sociales protegen por defecto el perfil del usuario" - http://www.abc.es/20110930/medios-redes/abci-redes-sociales-privacidad-201109301611.html
- "Seguridad y redes sociales, la perspectiva del usuario" - http://blog.segu-info.com.ar/2011/09/seguridad-y-redes-sociales-la.html#axzz1ceX77KTO

Referencias

- [1] Google Indexes Facebook Comments on Website – Digital Inspiration - http://www.labnol.org/internet/google-indexes-facebook-comments/20295/
- [2] Social Engineering: The Art of Human Hacking – Chris Hadnagy - Wiley; 1 edition (December 21, 2010)
- [3] Social Engineering: http://eljeffto.com/wp-content/uploads/2012/12/paper_stalkerphone_jeffrey_borbon.pdf

- [4] Opción frustrada de navegación segura en Facebook – Subdirección de seguridad de la información Unam (México) - http://www.seguridad.unam.mx/noticias/?noti=4337
- [5] Regresa cookie espía de Facebook - Subdirección de seguridad de la información Unam (México) - http://www.seguridad.unam.mx/noticias/?noti=4903
- [6] Guía de seguridad en Facebook – Inteco (España) http://www.inteco.es/file/nVpd_oWQO0blBIiD4wnTxQ
- [7] Guía de seguridad en Twitter – Inteco (España) http://www.inteco.es/file/0GJXYRVkJXnLSDCfeJCkbA
- [8] Guía de seguridad en Twitter – Inteco (España) http://www.inteco.es/file/nVpd_oWQO0ZRK6a0e7iZKg
- [9] Slides sobre seguridad en FourSquare – Alicantevor http://www.slideshare.net/Alicantevor/accin-24-seguridad-en-foursquare
- [10] Delincuentes usan Facebook y Twitter para captar víctimas - http://www.seguridad.unam.mx/noticias/?noti=4881
