



Seguridad en las Redes Sociales

¿Cuales son las reglas de este juego?

Los sitios de redes sociales tales como Facebook, Orkut, Twitter, LinkedIn y YouTube, entre otros, brindan la posibilidad de la publicación propia de contenidos así como una enorme interacción entre usuarios por medio de blogs, RSS feeds, podcasts, y otras tecnologías

Estos sitios atraen a un gran número de visitantes, convirtiéndolos en extremadamente atractivos para atacantes.

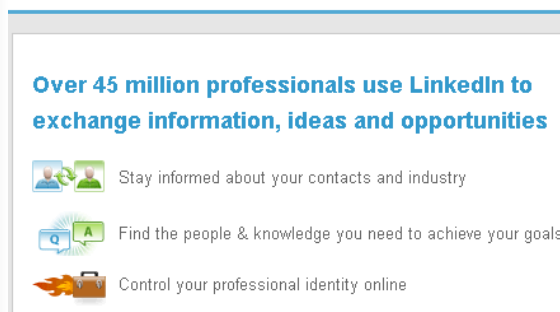
Sobre las redes sociales y sus portales

El día Martes 15 de Septiembre, Mark Zuckerberg, creador de Facebook, posteó en el blog¹ de esta aplicación:

"Al día de la fecha, Facebook es utilizado por 300 millones de personas alrededor del mundo. Es un gran número, sin embargo, a nuestros ojos, esto significa que recién estamos comenzando con nuestros objetivos de conectar a todos. [...]"

Es posible, a partir de este extracto, obtener una idea de la dimensión del alcance que pretenden tener estas aplicaciones en general.

LinkedIn[®]



Over 45 million professionals use LinkedIn to exchange information, ideas and opportunities

- Stay informed about your contacts and industry
- Find the people & knowledge you need to achieve your goals
- Control your professional identity online

Se puede apreciar claramente, además, desde la página de inicio de Orkut, por ejemplo, la misión y/o finalidad de este tipo de sitios:

- Conectar (con amigos)
- Descubrir (nuevos contactos)
- Compartir (fotos, videos, y todo tipo de datos)

En muchos casos, como Facebook y Orkut, los portales fueron creados con la misma idea base, lo que los lleva a competir entre ellos.

twitter

YouTube



Finalmente, citando al portal LinkedIn, se confirma que en la actualidad la cantidad de usuarios de las redes sociales alcanza fácilmente los millones, y cada una de estas redes comparte objetivos similares en ámbitos muy diversos.

En este caso, LinkedIn informa en su homepage que cuenta con más de 45 millones de profesionales registrados que se mantienen informados sobre la industria y sus contactos de negocios, así como también utilizan esta red para encontrar personas y adquirir conocimientos (siempre en el ambiente profesional/laboral).

Ahora sí, no quedan dudas de que este tipo de sitios está tendiendo a ser el "target" más atractivos para los "ladrones cibernéticos" y "hackers malintencionados" que pretenden, y logran, encontrar otras finalidades a las redes sociales, distintas de las que hasta aquí se han enumerado.

orkut^{beta}

Connect with friends and family using scraps and instant messaging
Discover new people through friends of friends and communities
Share your videos, pictures, and passions all in one place

¹ <http://blog.facebook.com/blog.php?post=13678227130>

Viviendo en la casa de vidrio

Los datos que pueden obtenerse simplemente accediendo al perfil de un usuario de estas redes sociales, que en muchos casos son públicos por defecto, van desde su fecha de nacimiento hasta el cargo que ocupa en la compañía para la que trabaja, pasando en el medio por infinidad de registros que, como se verá más adelante, tienen mucho valor en el proceso de "information gathering" previo a un ataque real.

Lo que asusta aun mucho más, es darse cuenta que con la capacidad de sumar y correlacionar todos estos ítems, el impacto de un ataque puede llegar incluso hasta el compromiso de varios sistemas de manera trivial (como por ejemplo, una cuenta de mail personal).

Se puede afirmar que la información publicada por los usuarios de estos sitios no sólo podría comprometer su privacidad, sino que también existe la posibilidad de que este riesgo traspase a los ambientes de negocios en los que se desenvuelven estos individuos. Hay que tener en cuenta que la actividad online de los empleados fuera del horario laboral también puede, sin parecerlo, crear todo tipo de problemas para el negocio (como la fuga de información, entre otros).

Las opciones multimedia que brindan estos portales permiten traspasar todas las barreras para lograr que la combinación de fotos, videos y datos se combinen exponiendo 100% la vida de un sujeto al público alrededor del mundo a través de Internet. Además, es realmente un punto a destacar que las personas publican detalles de sus vidas, amores, trabajos y hobbies que nunca pensarían en contarle a un extraño en una reunión de bar, por ejemplo. Esta actitud es consecuencia de la falsa sensación de anonimato que presta la Web, debido a la falta de contacto físico

▼ Basic Information

Sex: Show my sex in my profile

Birth day: Show my full birthday in my profile.

Hometown:

Home Neighborhood:

Family Members:
[Add another family member](#)

Relationship Status:

Interested in: Men Women

Looking for: Friendship Dating A Relationship Networking

Political Views:

Religious Views:

► Personal Information

► Contact Information

▼ Education and Work

College/University:

Concentration:

Second Concentration:

Third Concentration:
[Add Another Concentration](#)

Degree:
[Remove School](#)

[Add Another School](#)

High School:

[Remove High School](#)

[Add Another High School](#)

Employer:

Position:

Description:

City/Town:

Time Period: I currently work here.
 to present.

entre sus actores y del hecho que es accedida desde la comodidad y

Las actividades de un usuario peculiar, vectores de ataques

Quienes alguna vez dieron de alta una cuenta de mail, por ejemplo, recordarán que en uno de los pocos pasos que esta acción requiere hay que configurar una contraseña para el acceso a la misma y además, como medida de seguridad, una "respuesta secreta" a una "pregunta pública".

Entre las opciones de preguntas que proveen para configurar por defecto varios de los servicios de Webmail más conocidos (Gmail, Hotmail, Yahoo, entre otros) se encuentran las siguientes (extraídas de los sitios mencionados):

- Número de teléfono primario
- Nombre de la profesora preferida
- Nombre del mejor amigo de la infancia
- Nombre de la primer mascota
- Nombre del personaje favorito

Un usuario perspicaz fácilmente puede inferir que la mayor parte de las personas que utilizan las redes sociales publican allí muchas de estas "respuestas secretas". Se mencionó también que la pregunta tiene carácter de pública ya que cualquier persona puede llegar a la instancia en la que se muestra la misma siguiendo sencillos pasos al declarar que la contraseña de acceso de una cuenta determinada ha sido olvidada.

Se ha dado a conocer al público recientemente que la cuenta de correo Web de una funcionaria pública en USA había sido comprometida de esta forma.

Otros están aprovechando los datos contenidos en estos portales para poder realizar un "tunning" sobre los spams y publicidades que se envían por correo electrónico. Lo que es peor aún, hay quienes se encargan de lograr que los mails de phishing sean muchísimo

privacidad de nuestros hogares.

más convincentes a partir de la información recolectada.

Entre los otros vectores de ataque que se están explotando se encuentran los ya conocidos XSS² (Cross Site Scripting), donde se aprovechan vulnerabilidades en las aplicaciones Web de las redes sociales para poder inyectar código malicioso que finalmente se ejecute en las máquinas cliente.

Otro tipo de ataque que sigue la misma línea es XSRF³ (Cross Site Request Forgery), en el cual un comando o acción maliciosa es ejecutado mientras la víctima se encuentra logueada en la aplicación Web.

Muchos de los ataques en la actualidad, y más aún en lo que respecta a las redes sociales, nada tienen que ver con un exploit. La tendencia muestra que se trata de persuadir al usuario a realizar una acción sobre la que un atacante tenga control, como por ejemplo, hacer click sobre un link determinado.

Incidentes de seguridad que han visto la luz pública

De esta última forma, a finales del año 2007 los usuarios de Orkut en Brasil ya eran sujetos de un ataque en el que un Worm intentaba robar detalles de cuentas bancarias. El programa malicioso, que también intentaba tomar control de la computadora comprometida, se propagaba mediante falsos links ubicados en las páginas personales de los usuarios de este portal.

En el mes de Agosto de este año, se hizo de público conocimiento que la red social Twitter había estado bajo ataques que llevaron a la aplicación a

² [http://www.owasp.org/Index.php/Cross-site_Scripting_\(XSS\)](http://www.owasp.org/Index.php/Cross-site_Scripting_(XSS))

³ [http://www.owasp.org/Index.php/Cross-Site_Request_Forgery_\(CSRF\)](http://www.owasp.org/Index.php/Cross-Site_Request_Forgery_(CSRF))

recibir mayor cantidad de tráfico del que estaba preparado para soportar, estando al borde de un DoS.

La raíz del problema se encontraba en que una cuenta de este portal estaba siendo usada como una parte de un servidor improvisado de actualizaciones para computadoras que pertenecen a una Botnet⁴. Más precisamente, se utilizaba como canal de comando y control para las computadoras afectadas.

Desde esta cuenta se posteaban "tweets" que contenían solo una línea de texto que, para el ojo de un usuario común, parecía indescifrable. Sin embargo, llevando este string a un decodificador de base64, el resultado apuntaba a enlaces donde las computadoras infectadas podían recibir las actualizaciones del malware instalado en ellas.

Los Bots que hacían uso de esta cuenta de Twitter se conectaban mediante RSS, técnica que les permitía recibir cada "tweet" en tiempo real sin la necesidad de tener una cuenta asociada en la aplicación.

No sólo hallazgos de seguridad que implican Worms y Malware se han visto publicados recientemente. A comienzos de este año, la introducción de una nueva política en los "términos de uso" de la aplicación Facebook hizo que casi 200 millones de usuarios pasaran a dejar una copia de todos sus mensajes, acciones y actualizaciones online aun cuando dejaran de usar el sitio o sus cuentas fueran borradas o desactivadas. Esta política generó un gran debate, y un día después que Mark Zuckerberg defendiera en persona esta postura, Facebook se vio revertido a sus anteriores "términos de uso y servicio".

Cuando los "términos del servicio" (o los "términos de uso") declaran tener, en ciertos establecimientos, derechos totales sobre la información del usuario

(o el contenido, en este caso) durante y aun después de que haya dejado de usar el servicio, es el momento en que se generan las preocupaciones por la privacidad. Más específicamente, surge la necesidad de preguntarse: ¿qué es lo que harán con todos mis datos?

¿Cuáles son las reglas de este juego? ¿Existe el "Fair Play"?

Mientras la popularidad de las redes sociales sigue en crecimiento, así también aumentan los riesgos de pertenecer a alguna de ellas. Como vimos, hackers, spammers, desarrolladores de virus y Worms, ladrones de identidades y otros tipos de criminales están detrás de todo este tráfico.

A continuación se listan varios tips a tener en cuenta al entrar en el boom de las redes sociales:

- **Limitar la información personal que se postea** - No publicar información que nos convierta en vulnerables, tal como direcciones o datos sobre compromisos de agenda o rutinas. En el caso en que las conexiones (amigos o contactos) publiquen información acerca de uno, hay que asegurarse que todos los datos combinados no sean mayor a la cantidad de información que estamos dispuestos a compartir con un extraño. También aplica para el caso inverso, cuando publicamos información de nuestras conexiones.
- **Recordar siempre que Internet es un recurso PÚBLICO** - Publicar sólo información con la que uno se sienta cómodo hacer pública. Esto incluye datos y fotos en el perfil, blogs y otros foros. También, es necesario tener presente que una vez que se ha realizado un post, no hay vuelta atrás o forma alguna de revertirlo. Aun cuando la

⁴ <http://en.wikipedia.org/wiki/Botnet>

información sea borrada de un sitio, versiones cacheadas o guardadas puede aun existir. (US-CERT provee una guía online sobre publicación de información online⁵)

- **Ser precavido con los extraños** – Internet facilita a las personas cambiar sus identidades y disfrazar sus motivos finales de contacto. Considerar limitar las personas a quienes se les permite contactarnos y ver nuestros datos publicados en las redes sociales. Si se interactúa con personas desconocidas, ser cauteloso acerca de la cantidad de información que se revela o si se acuerda encontrarse con esta persona.
 - **Ser escéptico** – No hay que creer todo lo que se lee online. Las personas podrían postear información falsa o engañosa sobre varios tópicos, incluyendo sus identidades. No necesariamente esto se hace con malas intenciones, podría ser sin intención, una exageración o incluso una broma. Aun así, tomar las precauciones apropiadas y verificar la autenticidad de cualquier información antes de realizar alguna acción.
 - **Evaluar las configuraciones** – Hacer provecho de las opciones de configuración de seguridad de los sitios. Estas, por defecto en algunos, permiten que cualquier persona acceda de forma completa a un perfil. Es posible personalizar la configuración para restringir el acceso sólo a ciertas personas. Sin embargo, existe el riesgo de que estos datos continúen expuestos, por lo tanto, como se ha dicho, no publicar información que no querremos que el público pueda
- ver. También, ser cuidadoso al momento de decidir a que aplicaciones se les permite acceder a nuestro perfil (en el caso de Facebook, por ejemplo) y verificar que datos puede leer.
- **Usar passwords fuertes** – Proteger cada cuenta con un password distinto, que sean difíciles de adivinar. Si la contraseña es comprometida, alguien más podría ser capaz de acceder a la cuenta y realizar una impersonalización, por ejemplo.
 - **Verificar las políticas de privacidad** – Algunos sitios podrían compartir datos tales como direcciones de correo o preferencias de los usuarios con otras compañías. Esto podría ocasionar un incremento del spam. También se recomienda leer las políticas del sitio con el fin de detectar otros expuestos con los que no estemos conformes, como por ejemplo, el envío de mails a nuestros amigos para que se unan a la red social en cuestión.
 - **Usar y mantener software antivirus** – Los antivirus reconocen la mayoría de los virus y protegen las computadoras contra estos. Es por esto que pueden detectar y remover un virus antes de que cause algún daño. Dado que los atacantes están continuamente desarrollando código malicioso que luego se convertirá en un virus o gusano, es importante mantener las definiciones del antivirus actualizadas.

¿ No apto para menores ?

Los niños son especialmente susceptibles a las amenazas que los sitios de redes sociales presentan. A pesar de que muchos de estos portales tienen restricciones de edad, los niños

⁵ <http://www.us-cert.gov/cas/tips/STO4-014.html>

pueden "falsificar" sus edades para unirse al sitio. Educándolos acerca de la seguridad en Internet, estando conscientes de sus hábitos online y guiándolos a sitios apropiados, los padres pueden asegurarse de que los niños también se conviertan en usuarios responsables y seguros.

En esta aventura que emprenden los niños, los padres deben ser sus guías por lo que deben conocer el camino para llegar a los sitios deseados. En primera instancia, es primordial establecer reglas para el uso de Internet y sus aplicaciones, así como también es recomendable mantener una lista de sitios permitidos o autorizados a los cuales los niños pueden acceder. Se deberá definir, también, un marco de tiempo/horarios en el que los niños estén permitidos realizar estas actividades.

Como tutores, se deberá enseñarles a proteger su privacidad, a no revelar información personal o de la familia, como el nombre de la escuela, el domicilio o fotografías familiares, y a no responder mensajes de desconocidos sin antes consultar acerca del contacto.

Es importante enseñar al niño que cuando aparezca algo en su pantalla que lo haga sentir incomodo de inmediato llame a sus padres (caso de Cyberbullying⁶, por ejemplo). Para darle mayor soporte a esta situación, es recomendable que la computadora se encuentre a la vista, en un pasillo transitado de la casa, por ejemplo, y estar alertas a sus reacciones y movimientos.

Tomando todos estos recaudos y precauciones, es posible motivar a los niños a interactuar de forma segura con otros pares por medio de las redes sociales especialmente creadas para este fin, las cuales, además, incentivan la creatividad y la cooperación. Uno de los sitios creados tomando estos fundamentos como base es Club

Penguin⁷, de Disney (el cual hace foco en las políticas de seguridad y privacidad). Un mundo donde todos los personajes son pingüinos, característica que no da lugar a diferencias que permitan la discriminación y resulta atractivo tanto para niños como para niñas.

Entonces, ¿debo vivir en una burbuja ?

Todos los puntos aquí analizados, críticas, desventajas y amenazas, no deben desanimar a los usuarios de Internet a registrarse en los sitios de redes sociales.

Por el contrario, las propuestas provistas por los portales aquí mencionados son más que interesantes. Y, lo que se intenta lograr es concientizar a los usuarios para que, finalmente, sean mucho más responsables con el uso de la red pública.

Se recomienda, entonces, ser discretos, escépticos, considerados, profesionales, cautelosos y además verificar las políticas de privacidad y seguridad de cada sitio.

Como conclusión, tal como se mostró en este artículo, así como no es necesario ser experto en informática para reencontrarse en estas redes con amigos del colegio primario tampoco lo es para hacerlo en forma segura.

Joaquín Paredes – CCSP
jparedes@cybsec.com

⁶ <http://en.wikipedia.org/wiki/Cyber-bullying>

⁷ <http://www.clubpenguin.com/>