VERSIÓN EN ESPAÑOL
UNAM CERT

OUCH! | Marzo 2013

Boletín mensual de consejos de seguridad para usuarios de computadoras

OUCH!

EN ESTA EDICIÓN

Redes sociales de manera segura

EDITOR INVITADO

Ted Demopoulos es el editor invitado para esta publicación. Es un consultor de seguridad con mucha experiencia y ha impartido cursos en el SANS desde hace una década, incluyendo SEC401/501 y MGT414/512. Conoce más acerca de Ted en http://demop.com

RESUMEN

Los sitios de redes sociales como Facebook, Twitter, Google+, Pinterest y Linkedin son poderosas, te permiten conocer, interactuar y compartir cosas con personas alrededor del mundo. Sin embargo, todas estas características implican riesgos; no solo para ti, también para tu familia, amigos y empleados. En este boletín se discutirán esos riesgos además de cómo usar estos sitios de una manera más segura.

PRIVACIDAD

Una inquietud común en las redes sociales es la protección de la privacidad de información personal y la información sensible de otros. Los riesgos potenciales incluyen:

- Impacto en tu futuro: Muchas organizaciones buscan sitios de redes sociales como parte del proceso de investigación de antecedentes. Publicaciones embarazosas o incriminatorias, no importa la fecha, pueden provocar que no te contraten o asciendan. Muchas universidades realizan investigaciones similares en la solicitud de nuevos estudiantes. Las opciones de privacidad podrían no protegerte, ya que una organización puede pedirte dar “me gusta” o unirte a sus sitios antes de continuar con el proceso de aplicación.

- Ataques en tu contra: Cibercriminales pueden obtener tu información personal y utilizarla para realizar ataques en tu contra. Por ejemplo, pueden usar tu información para adivinar las respuestas de tus “preguntas secretas” y cambiar tus contraseñas, crear ataques dirigidos de correo llamados *spear phishing* o solicitar tarjetas de crédito usando tu nombre. Además, estos ataques pueden aterrizarse en el mundo físico, ya que pueden identificar dónde trabajas o vives.

- Ocasionar daños a tu empresa: criminales o competidores pueden usar cualquier información sensible publicada por ti acerca de tu organización en contra de la misma. Tus publicaciones podrían causar un daño potencial a la organización. Asegúrate de conocer las políticas de tu organización antes de publicar cualquier cosa sobre tu empresa.

La mejor defensa es limitar la información que publicas. Es cierto que las opciones de privacidad pueden brindarte un

Redes sociales de manera segura

poco de protección; sin embargo, ten en mente que suelen ser confusas y pueden cambiar frecuentemente sin tu conocimiento. Lo que pensabas que era privado podría convertirse en algo público por una gran variedad de razones que llegan a ser desconocidas. La privacidad de tu información es tan segura como lo son las personas con las que la compartes, es decir, mientras más información privada compartas con amigos o contactos, más información se convertirá en pública. La mejor manera para proteger tu privacidad es seguir esta regla: si no quieres que tu madre o tu jefe vea lo que publicas, entonces no deberías publicarlo.

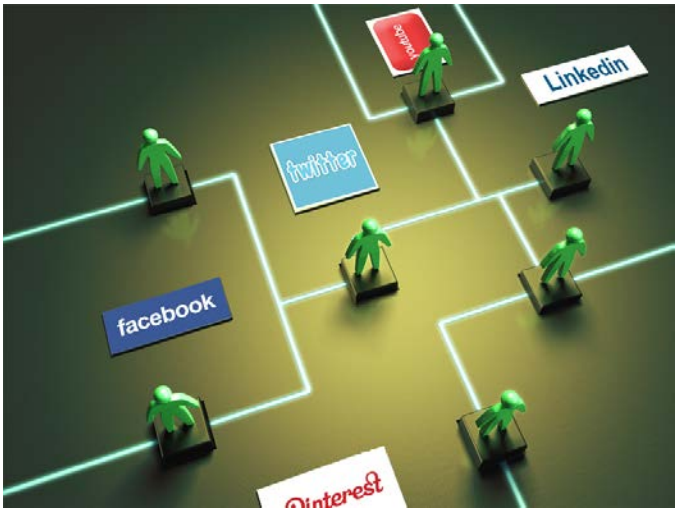
También debes estar consciente de qué información publican tus amigos. Esto podría convertirse en un daño si ellos publican información privada o embarazosa que te involucre. Asegúrate que tus amigos entiendan qué pueden y qué no pueden publicar acerca de ti. Si ellos publican algo con lo que no estás cómodo, déjales saber para que lo quiten. Al mismo tiempo, se respetuoso con las publicaciones que haces sobre otros.

SEGURIDAD

Además de los problemas de privacidad, las redes sociales pueden ser usadas por los cibercriminales para atacarte a ti o a tus dispositivos. Algunos pasos para protegerte son:

- Inicio de sesión: Protege tu cuenta de redes sociales con contraseñas seguras y no las compartas con nadie ni las reutilices en otros sitios. Algunas redes sociales soportan una autenticación segura, como la verificación de dos pasos. Activa el método de autenticación segura cuando sea posible.

- Cifrado: Muchos sitios de redes sociales permiten cifrar la comunicación usando el protocolo seguro https, lo que asegura tu conexión al sitio. Algunos sitios como Twitter y Google+ tienen estas características predeterminadas, mientras que otros sitios requieren que se habilite manualmente mediante las configuraciones de la cuenta. Utiliza https siempre que sea posible.



Los sitios de redes sociales son poderosos y divertidos, pero se cuidadoso en lo que publicas y en quien confías.

- Correo electrónico: Desconfía de correos que pretenden venir de sitios de redes sociales. Éstos pueden ser fácilmente falsificados por cibercriminales. La manera segura de responder a estos mensajes es acceder al sitio web directamente (tal vez desde un marcador) y checar cualquier mensaje o notificación en el sitio web.

- Enlaces maliciosos/fraude: Se precavido de ligas maliciosas, sospechosas o estafas potenciales publicadas en sitios de redes sociales. Los atacantes pueden publicar ligas maliciosas y, si tú accedes a

Redes sociales de manera segura

ellas, serás reenviado a sitios web que podrían infectar tu computadora. Además, no hay que confiar en un mensaje solo porque es enviado por un amigo, ya que no siempre significa que provenga de él. Su cuenta pudo haber sido comprometida. Si un miembro de la familia publica un mensaje que no puede ser verificado (como en aquellos que indican que fueron asaltados y que necesitan que les envíes dinero) trata de comunicarte con ellos por otros medios para confirmar el mensaje.

- Aplicaciones: Algunos sitios de redes sociales te permiten agregar o instalar aplicaciones de terceros, por ejemplo juegos. Ten en mente que existe un mínimo o nulo control de calidad o revisión de estas aplicaciones, podrían tener acceso a tu cuenta y a tu información privada. Solo instala aplicaciones que necesites, que sean bien conocidas o de sitios confiables y elimínalas cuando ya no las necesites.

Las redes sociales son una manera completa y divertida para comunicarte con el mundo. Si sigues las recomendaciones mencionadas en esta publicación, disfrutarás de una experiencia de seguridad en línea. Para más información de cómo usar redes sociales de manera segura o reportar una actividad no autorizada, asegúrate de revisar la seguridad de las páginas de los sitios que estás utilizando.

RECURSOS

Algunos de los enlaces mostrados a continuación se redujeron para mejorar la legibilidad a través del servicio TinyURL. Con el fin de mitigar problemas de seguridad, OUCH! siempre utiliza la característica de vista previa de TinyURL (preview), la cual muestra el enlace destino solicitando tu permiso antes de abrirlo.

5 consejos de seguridad para manejar tus redes sociales:
http://preview.tinyurl.com/baqlxvo

Seguridad en Facebook:
http://preview.tinyurl.com/3gcafus

Seguridad en Twitter
http://preview.tinyurl.com/lqpgj2

Robo de identidad:
http://preview.tinyurl.com/b2em85t

Términos de seguridad:
http://preview.tinyurl.com/bkcuk2s

MÁS INFORMACIÓN

Suscríbete al boletín mensual OUCH!, el boletín de consejos sobre seguridad. Accede a los archivos de OUCH! y aprende más acerca de las soluciones preventivas de seguridad que SANS tiene para ti.
Visítanos en http://www.securingthehuman.org

VERSIÓN EN ESPAÑOL

UNAM-CERT, Equipo de Respuesta a Incidentes de Seguridad en Cómputo en México reconocido ante FIRST es una referencia en seguridad de la información en este país.

Sitio web http://www.seguridad.unam.mx
Síguelo en Twitter @unamcert

Consejo Editorial: Bill Wyman, Walt Scrivens, Phil Hoffman, Lance Spitzner
Versión en español a cargo de UNAM-CERT: José Luis Sevilla, Fusto Pérez, Célica Martínez, Andrea Méndez, Gustavo Villafán