Boletín mensual de consejos de seguridad para usuarios de computadoras

OUCH!

EN ESTA EDICIÓN



# Seguridad en redes sociales

## EDITOR INVITADO

Lenny Zeltser es el editor invitado para esta edición de OUCH! Lenny se dedica a salvaguardar las operaciones de TI de los clientes de Radiant Systems y enseña cómo combatir al malware en el SANS Institute. Sigue a Lenny en Twitter como @lennyzeltser y escribe en su blog de seguridad blog.zeltser.com.

## RESUMEN

Este mes revisaremos redes sociales como Facebook, Twitter, Google+ y LinkedIn. Sitios como estos son poderosas herramientas que te permiten conocer, interactuar y compartir con personas alrededor del mundo. Sin embargo, todas estas capacidades vienen acompañadas de riesgos considerables, no sólo para ti, sino también para tu empresa, familiares y amigos. En este boletín discutiremos cuáles son esos riesgos y cómo utilizar estos sitios de forma segura.

## PRIVACIDAD

Una preocupación frecuente acerca de los sitios de redes sociales es tu privacidad, ya que existe el riesgo de que tú mismo u otros compartan demasiada información sobre ti. Los peligros de compartir demasiado incluyen:

• **Daño a tu carrera:** Publicar información embarazosa puede dañar tu futuro. Muchas organizaciones, como parte de la revisión de antecedentes de un nuevo empleado, consultan en las redes sociales todo lo que haya sido publicado sobre él. Cualquier publicación embarazosa o incriminatoria, sin importar lo antigua que sea, podría evitar que obtengas ese nuevo empleo. Además, muchas universidades realizan revisiones similares para estudiantes de nuevo ingreso.

• **Ataques en tu contra:** Delincuentes cibernéticos pueden recolectar tu información y utilizarla para atacarte. Por ejemplo, podrían adivinar las respuestas a “preguntas secretas” que los sitios web utilizan para restablecer tu contraseña o quizás solicitar una tarjeta de crédito utilizando estos datos.

• **Ataques contra tu empresa:** Cuando los criminales buscan información empresarial o preparan un ataque contra tu empresa, pueden obtenerla a través de lo que compartes en redes sociales. Por otra parte, tu actividad en línea puede, involuntariamente, reflejar una mala imagen de tu empresa. Asegúrate de consultar las políticas sobre redes sociales de tu empresa para guiarte sobre cómo se espera que protejas sus datos y reputación.

La forma más efectiva de protegerte de estos peligros es ser cuidadoso con la información que publicas sobre ti. Ten en cuenta que los datos que compartes ahora podrían ser

# Seguridad en redes sociales

utilizados en tu contra después. También, restringe las opciones de privacidad de tu perfil de red social para limitar quién puede ver la información personal que compartes. Recuerda que tus datos pueden filtrarse inadvertidamente por el sitio web o por tus amigos, así que lo mejor es asumir que cualquier información que coloques puede hacerse del conocimiento público en cualquier momento. También, sé cuidadoso con lo que otros publican sobre ti. Si tienes amigos publicando información, fotografías u otros datos que no deseas que se hagan públicos, pídeles que los borren.

## SEGURIDAD

Además de ser una fuente peligrosa de fugas de información, los sitios de redes sociales pueden ser usados como plataforma para atacar tu computadora o realizar estafas. Aquí, te ofrecemos algunos consejos para protegerte:

• ***Inicio de sesión****:* Protege tu cuenta de redes sociales con una contraseña fuerte (revisa la edición de OUCH! de mayo 2011). No compartas esta contraseña con nadie ni la utilices para otros sitios. Adicionalmente, algunas redes sociales como Facebook o Google+ tienen características para una autenticación más robusta, por ejemplo los códigos de un sólo uso cuando se ingresa desde una computadora pública o al utilizar tu teléfono como parte del proceso de inicio de sesión. Habilita estas características si están disponibles.

• ***Cifrado****:* Muchos sitios como Facebook, Google+ y Twitter te permiten obligar el uso cifrado (llamado HTTPS) de todas las comunicaciones con el sitio web. Siempre que te sea posible, habilita esta opción.

• ***Correo electrónico****:* Sé precavido cuando des clic sobre los enlaces en correos electrónicos que afirmen ser de la


***Las redes sociales son herramientas poderosas y divertidas, pero ten cuidado con lo que publicas y en quién confías.***

red social. En su lugar, accede al sitio usando un marcador y verifica cada mensaje o notificación directamente.

• ***Enlaces****:* Sé cuidadoso al dar clic en enlaces publicados en los muros de personas o páginas públicas. Virus y gusanos se propagan fácilmente en ellos. Si un enlace te parece extraño, sospechoso o demasiado bueno para ser cierto, no des clic…, no importa que el enlace esté en el muro de tu mejor amigo. La cuenta de tu amigo pudo haber sido secuestrada o infectada, y estar distribuyendo software malicioso.

# Seguridad en redes sociales

• ***Estafas****:* Los criminales se aprovechan de la naturaleza abierta de las redes sociales para defraudar a las personas. En ocasiones, las estafas utilizan como anzuelo una oferta de empleo o dinero, que sea demasiado bueno para ser verdad. Otra estafa común es usar cuentas secuestradas para contactar a los amigos de la víctima pidiéndoles ayuda, diciendo que la persona fue robada en un país extranjero y necesita dinero. Desconfía si un amigo o un desconocido te pide dinero o te hace una oferta que sea sorprendentemente buena en alguna red social.

• ***Aplicaciones****:* Algunas redes sociales te permiten agregar o instalar aplicaciones de terceros, como juegos. Ten en cuenta que estas aplicaciones tienen un bajo o nulo control de calidad y que pueden tener acceso total a tu cuenta y a los datos que compartes. Las aplicaciones maliciosas pueden utilizar este acceso para interactuar con tus amigos en tu nombre, robar y hacer un mal uso de tu información personal. Procura sólo instalar aplicaciones de confianza de sitios reconocidos, y mantenerlas actualizadas una vez que las instales. Cuando ya no utilices alguna aplicación, bórrala.

Las redes sociales  son herramientas poderosas y divertidas que permiten comunicarte con todo el mundo. Si sigues los consejos indicados aquí, podrás disfrutar de una experiencia mucho más segura en línea.

## RECURSOS

Algunos de los enlaces mostrados abajo han sido reducidos para mejorar la legibilidad a través del servicio TinyURL. A fin de mitigar problemas de seguridad, OUCH! siempre utiliza la característica de vista previa de TinyURL (preview), la cual muestra el enlace destino, solicitando permiso antes de abrirlo.

OnGuard Online: http://preview.tinyurl.com/6ml3fx

Microsoft: http://preview.tinyurl.com/3sh2xkd

UNAM-CERT: http://preview.tinyurl.com/3r3fpwa

Facebook: http://preview.tinyurl.com/y2htc7b

Twitter: http://preview.tinyurl.com/43n9joy

## 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 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, Carmen Ruyle Hardy*
*Versión en español a cargo de UNAM-CERT: Angie Aguilar, Miguel Mendoza, Galvy Cruz, Mauricio Andrade, Rubén Aquino*