VERSIÓN EN ESPAÑOL

UNAM CERT

OUCH! | Julio 2015

Boletín mensual de seguridad para usuarios de computadoras

OUCH!

En esta edición...

Social media

Resumen

Los sitios de medios sociales como Facebook, Twitter, Instagram y LinkedIn son recursos increíbles que permiten conocer, interactuar y compartir con personas de todo el mundo. Sin embargo, todo poder conlleva un riesgo, no sólo para ti sino para tu familia, amigos y empleados. En este boletín te explicamos los peligros y cómo utilizar estos sitios de forma segura.

Editor Invitado

Tanya Baccam es consultora de seguridad de gran experiencia. Ha sido autora del SANS e instructora durante más de una década, incluyendo los cursos de SEC502, SEC542, SEC401, MGT414, AUD507 y muchos más. Puedes seguirla en Twitter como **@tbaccam**.

Privacidad

Una preocupación común en las redes sociales es proteger tu información personal. Los peligros potenciales incluyen:

- **Impacto en tu futuro**: Algunas organizaciones buscan sitios de medios sociales/redes sociales como parte de la verificación de antecedentes. Las fotos o mensajes incriminatorios o vergonzosos, sin importar la edad, podrían impedir que fueras contratado o promovido. Además, muchas universidades realizan controles similares para el ingreso de nuevos estudiantes. Las opciones de privacidad no pueden protegerte si estas organizaciones te piden dar “Me gusta”, unirte a sus páginas o publicar algo que puede ser archivado en múltiples sitios.
- **Ataques en tu contra**: Los atacantes cibernéticos pueden analizar tus publicaciones y utilizarlas para obtener acceso a tu información o a la de tu organización. Por ejemplo, pueden utilizar información que compartes y adivinar las respuestas a tus “preguntas secretas” para restablecer tu contraseña en línea, crear ataques de correo electrónico llamados spearfishing o llamar a alguien de tu organización pretendiendo ser tú. Además estos ataques pueden extenderse al mundo físico, tales como identificar en dónde trabajas o vives.
- **Dañar accidentalmente a tus empleados**: Criminales o competidores pueden usar cualquier tipo de información sensible que publicas acerca de tu organización en contra de los empleados. Tus mensajes pueden dañar potencialmente la reputación de tu organización. Asegúrate de revisar las políticas antes de publicar cualquier cosa acerca de tu trabajo, algunas publicaciones de tus redes sociales pueden ser monitoreadas.

La mejor protección es limitar lo que publicas. Sí, las opciones de privacidad pueden protegerte, no obstante, pueden ser confusas y cambiar con frecuencia sin tu consentimiento. Lo que tienes como privado puede convertirse rápidamente a público por diversas razones. La privacidad de tus mensajes es tan segura como las personas a quienes se los compartes,

Social media

cuanto más compartas con amigos o contactos, más probable es que la información se haga pública. Debes asumir que todo lo que publicas puede o no ser público y permanecer en Internet.

Por último, ten en cuenta lo que tus amigos publican sobre ti. Si no estás cómodo con alguna publicación pídeles que la retiren. Si se niegan o te ignoran, contacta al sitio y pídeles que eliminen el contenido sobre ti. Al mismo tiempo, se respetuoso con lo que publicas de otros.



Las redes sociales son divertidas y poderosas pero debes tener cuidado de lo que compartes y con quién.

Seguridad

Además de los problemas de privacidad, aquí hay algunos pasos que te ayudarán a proteger tus cuentas de redes sociales y actividades en línea.

- **Inicio de sesión**: Protege cada una de tus cuentas con una contraseña fuerte y única, no la compartas con nadie más. Muchos sitios de medios sociales admiten autenticación fuerte como la verificación en dos pasos, activa siempre estos métodos de autenticación donde sea posible. Finalmente, no utilices tus cuentas de redes sociales para iniciar sesión en otros sitios, si son atacados entonces todas tus cuentas estarán vulnerables.
- **Configuración de privacidad**: Si haces uso de la configuración de privacidad, asegúrate de revisarla y probarla regularmente. Las redes sociales suelen cambiar la configuración de privacidad y es fácil cometer un error. Muchas de las aplicaciones y servicios permiten añadir tu ubicación al contenido que publicas (esto es llamado geotagging). Comprueba regularmente estos ajustes si deseas mantener tu localización física privada.
- **Cifrado**: Los sitios de redes sociales utilizan el cifrado llamado HTTPS para proteger sus conexiones en línea hacia el sitio. Algunos sitios como Twitter y Google+ habilitan esto por defecto, mientras que otros requieren que habilites HTTPS manualmente. Comprueba la configuración de tu cuenta de redes sociales y activa HTTPS como la conexión pre e stablecida siempre que sea posible.
- **Correo electrónico**: Desconfía de los correos electrónicos que dicen provenir de sitios de medios sociales, éstos pueden ser ataques de falsificación enviados por cibercriminales. La forma más segura de responder a este tipo de mensajes es ingresar directamente a la página web de tu red social (tal vez desde un marcador guardado) y después leer y responder a los mensajes o notificaciones desde la página web.
- **Enlaces maliciosos/Estafas**: Ten cuidado de los enlaces sospechosos o posibles estafas publicadas en los sitios sociales. Los chicos malos usan las redes sociales para difundir sus propios ataques. Que un amigo tuyo publique un mensaje no significa que éste proviene realmente de él, su cuenta puedo haber sido comprometida.

Social media

Si un miembro de la familia o amigo ha publicado un mensaje extraño que no se puede verificar (como que le han robado y necesita que le envíen dinero), llámalos a su teléfono móvil o utiliza cualquier otro medio para confirmar que el mensaje es realmente de ellos.

- **Aplicaciones móviles**: La mayoría de los sitios de medios sociales proporcionan aplicaciones móviles para acceder a sus cuentas en línea, asegúrate de descargarlas desde un sitio de confianza y que tu teléfono inteligente esté protegido con una contraseña segura. Si tu dispositivo móvil se pierde y no está bloqueado, cualquiera puede acceder a tus redes sociales y publicar en tu nombre.

Las redes sociales son una forma maravillosa de comunicarse y estar en contacto con el mundo. Si sigues estos consejos podrás disfrutar de una experiencia en línea mucho más segura. Para obtener más información sobre el uso de redes sociales de forma segura o reportar actividades no autorizadas, consulta la página de seguridad de tu red social.

Conoce más

Suscríbete al boletín mensual de conciencia sobre seguridad OUCH!, consulta los archivos OUCH! y aprende más acerca de las soluciones de seguridad SANS visitando: http://www.securingthehuman.org

Versión en español

UNAM-CERT, Equipo de Respuesta a Incidentes de Seguridad de la Información en México reconocido ante FIRST, es una referencia en la materia en este país.
Sitio web: http://www.seguridad.unam.mx
Síguelo en Twitter @unamcert

Recursos

Frases de acceso:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201504_sp.pdf
Verificación en dos pasos:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201308_sp.pdf
Uso seguro de aplicaciones móviles:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201501_sp.pdf
Educar a los niños en ciberseguridad:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201506_sp.pdf
Seguridad de Facebook:	https://www.facebook.com/safety

Consejo editorial: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Traducción al español por: Abril García y Diego Valverde