Risk & Business Consulting.
Internal Audit.

Administración de Riesgos

Riesgos y consejos de seguridad al utilizar Twitter.

La forma como Twitter ha cambiado la manera de comunicarnos, los riesgos y consejos de seguridad al utilizarlo son abordados en esta nueva entrega de Punto de Vista.

En este punto de vista

El poder de 140 caracteres.

Twitter, con menos de seis años de existir, es globalmente, el noveno sitio más popular en Internet, según la compañía de investigación Alexa (datos al 23-Abril-2012). Si eso le asombra, permítanos informarle que Twitter genera más de 340 millones de *tweets* diarios y tiene poco más de 145 millones de usuarios activos.

Algunos medios de comunicación han resaltado el papel crítico que jugó Twitter en las protestas en Túnez en 2010-2011 y en la revolución en Egipto en 2011. También este microblogging ha servido como medio efectivo de comunicación ante emergencias, por ejemplo, en el terremoto de california de 2008 y canalizando el poder informativo y solidario, luego del gran desastre natural de Haití, de 2010. De igual forma ha sido, al parecer, un medio donde famosos informan a sus *fans* sobre sus gustos, pensamientos y orientación sexual.

Indistintamente de su impacto social o el uso que le queramos dar, ya sea a nivel personal o como herramienta de mercadeo corporativa, al igual que cualquier otra tecnología, los usuarios de Twitter no son inmunes a riesgos al utilizarlo.

Riesgos y privacidad en Twitter.

Los usuarios de Twitter (personas y compañías) deben tener presente que sus credenciales de acceso e identidad pueden ser comprometidas. Twitter no ha estado exento a ser víctima de técnicas de *hacking* para el uso indebido. Las cuentas de famosos, sin su conocimiento y consentimiento han sido utilizadas para no precisamente fines filantrópicos. Estos eventos han envuelto a Twitter, Inc. en varios procesos legales alrededor del mundo. La FTC (Federal Trade Comission) en los Estados Unidos en Junio de 2010, sentenció a Twitter, Inc. a realizar acciones urgentes para mejorar la privacidad de la información de sus usuarios. La buena noticia es que Twitter, Inc. ha mejorado y sigue mejorando la seguridad y privacidad de sus usuarios.

Aunque probablemente su cuenta personal o la de su compañía no tenga el número de seguidores de la cantante Lady Gaga (número uno con más de 23 millones en abril 2012), nos permitimos recomendar algunos consejos y buenas prácticas para que su experiencia en Twitter sea satisfactoria y no sufra un robo de identidad.

Los consejos que abajo describimos, aplican para la cuenta personal y diríamos, con mayor relevancia si es la cuenta de su compañía para mercadear sus productos-servicios o estar más cerca de sus clientes.

Consejos y buenas prácticas al utilizar Twitter.

1. **Solicita restablecer tu contraseña si sientes que tu cuenta ha sido "*hackeda*" o comprometida.**

   Visita la página https://support.twitter.com/forms y selecciona la opción "cuenta hackeada", allí se te guiará sobre cómo resolver el problema.

2. **Utiliza una contraseña fuerte y única.**

   Seguramente usted ha escuchado varias veces este consejo. Pues lo escuchará una vez más. Asegúrese de que su contraseña sea una frase (Twitter lo permite) y no una palabra. Cámbiela con alguna frecuencia sobre todo si la cuenta es utilizada para fines corporativos. No la comparta y evite que la misma sea la que utilice para acceder otros servicios en Internet, como por ejemplo, banca en línea.

3. **Utiliza www.twitter.com a través de HTTPS.**

   Cuando acceda Twitter hágalo en su navegador desde https://www.twitter.com Hacerlo de esta forma permite que sus credenciales de acceso (usuario y contraseña) viajen en forma encriptada y más segura entre su computador y los servidores de Twitter. Para esto, vaya al menú de configuración de su cuenta en Twitter y marca la casilla "Usar Siempre HTTPS".

4. **No contestes *email* sospechosos que pareciera provengan de Twiter.com**

   Twitter no envía *email* a sus usuarios solicitando su contraseña o pidiéndole que "baje" archivos adjuntos o le den "click" a un sitio en Internet. Estos *emails* pueden ser técnicas de phishing para robar tus credenciales de acceso a Twitter. Si recibes algún *email* de esta naturaleza envíalo a la cuenta spoof@twitter.com y luego borra ese correo de tu bandeja de entrada de *emails*.

5. **No abras “links” que recibas en tu cuenta de Twitter si lucen sospechosos.**

   Otra forma de robar tu identidad (credenciales de acceso) puede ser solicitándote abrir un “link” para ver alguna noticia o foto. Si dudas de la fuente, no lo abras.

6. **Si sientes que un usuario te acosa o envía *tweets* inapropiados, bloquea su cuenta.**

   Si no deseas recibir *tweets* fuera de lugar de un usuario en particular, bloquea su cuenta para no recibir sus *tweets*. Para tal efecto ingresa a tu cuenta, vas al perfil de la persona, haces “click” en el icono de la persona y seleccionas la opción bloquear. Los usuarios bloqueados no podrán: añadirte a sus listas; tener sus @menciones o @respuestas en la pestaña de tus @menciones; seguirte; ver tus fotos de perfil en su perfil ni en su cronología.

7. **Habilita la opción de cuenta protegida si sientes paranoia que desconocidos lean tus *tweets.***

   Por defecto las cuentas en Twitter son creadas como cuentas públicas. Si deseas que sólo personas que tú autorices, y no todos tus seguidores, lean tus tweets, habilita la opción de “cuenta protegida”. Para esto ve al menú de configuración y marca la casilla “Proteger mis Tweets”.

8. **Conectate a aplicaciones de terceros de forma segura.**

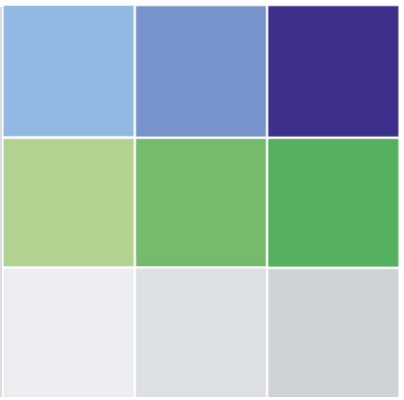
   Hay dos formas de asociar tu cuenta de Twitter a aplicaciones de terceros. La primera es mediante un protocolo seguro y transparente para el usuario denominado OAuth. La segunda es solicitándole al usuario de Twitter sus credenciales de acceso. Sea muy cuidadoso cuando una aplicación de un tercero solicita sus credenciales. Tenga presente que las mismas estarán en manos de un tercero de quien, quizás, usted no tenga mayores referencias.

9. **Hazte seguidor de las cuentas @spam y @safety.**

   Ambas cuentas te informan sobre amenzas en Twitter de las cuales debes estar alerta y, además, te brindan consejos de seguridad.

Independencia. Integridad. Conocimiento. Credibilidad.

RISCCO (www.riscco.com) es una compañía panameña, independiente y dedicada de manera exclusiva a la consultoría en riesgo tecnológico y auditoría interna, compuesta por profesionales con el conocimiento y credibilidad necesaria para traducir aspectos muy técnicos a un lenguaje simple y con sentido de negocio. Con tres años de iniciar operaciones, RISCCO cuenta en su cartera de clientes con compañías e Instituciones del Estado Panameño, líderes en su ramo.



info@riscco.com

Teléfono: +507 279-1410

Contactos

Antonio Ayala I.
t: 279-1410 Ext. 104
aayala@riscco.com

Benildo Vergara
t: 279-1410 Ext. 105
bvergara@riscco.com

Félix Olivares C.
t: 279-1410 Ext. 108
folivares@riscco.com