La red social advirtió sobre intentos masivos de terceros por acceder a cuentas.

Twitter indicó que “estamos comprometidos a mantener a Twitter como una comunidad segura y abierta. Como parte de ese compromiso, en casos en los que creemos que una cuenta ha sido comprometida, reseteamos la contraseña y enviamos un correo electrónico al propietario de la cuenta indicando lo que ha ocurrido junto con información sobre cómo crear una nueva contraseña. Esta es una parte rutinaria de nuestros procesos para proteger a nuestros usuarios”. “En este caso, sin querer se resetearon las contraseñas de un mayor número de cuentas, más allá de aquellos que cree que se han sido comprometido. Nos disculpamos por cualquier inconveniente o confusión que esto pueda haber causado”, sentenció la red social. “Twitter cree que su cuenta puede haber sido comprometida por un sitio web no asociado. Hemos borrado su contraseña para prevenir el acceso no autorizado”. Si este jueves, al tratar de iniciar sesión en Twitter, le llegó este mensaje obligándolo a cambiar de contraseña, su cuenta no necesariamente estuvo en la mira de ‘hackers’. Lo primero es aclarar que el mensaje es auténtico y usted debe cambiar la contraseña con toda confianza, pues esa sería la respuesta de la red social a los intentos masivos de sistemas de ‘spam’ por apoderarse de cuentas para publicar en ellas sin autorización. Ahora, reconocidos blogs de tecnología como TechCrunch y Portaltic -también afectados- insisten en que recibir este mensaje al correo no implica necesariamente que el perfil haya sido atacado, sino que se trata de una medida preventiva en la mayoría de los casos. También se conoció que la alerta la han recibido, especialmente, las cuentas verificadas o con gran número de seguidores. Los usuarios de la red social han mostrado su descontento debido a que se utiliza un enlace para cambiar la contraseña, lo que alentaría a los ‘hackers’ a realizar ataques de ‘phishing’, un tipo de ingeniería social que intenta adquirir información confidencial mediante engaños. Este no es el primer intento de ataque a gran escala que ha sufrido Twitter. En junio pasado, el grupo informatico LulzSec dijo haber accedido a más de 8.000 usuarios mediante la aplicación TweetGif, que se usa para generar animaciones en el avatar o foto de perfil. Por cuenta del intento de ataque, recogimos algunos consejos de bloguerospara que no ponga en riesgo su contraseña de Twitter: -Compruebe que está en la página real de Twitter, para ello

asegúrese de que en la barra de direcciones aparezca https://twitter.com (con 's') . Los 'hackers' pueden imitar el diseño y las propiedades de los sitios con relativa facilidad. -No haga uso de sitios web que aseguran llenarlo de seguidores. Aunque de hecho cumplen su promesa, también es sabido que son capaces de apoderarse de su cuenta para enviar 'spam' y causar otros problemas. -En 'Configuración', revise las aplicaciones que tiene asociadas a su cuenta de Twitter. Muchas veces las extensiones malignas acceden sin permiso y otras las aprueba el usuario casi sin darse cuenta. -Cualquier sospecha de ataque, repórtela directamente al Centro de Ayuda de Twitter , donde resuelven toda clase de dudas.

FUENTE: Eltiempo