Consejos para mantener protegida la cuenta de Twitter contra hackeos y estafas

Los cibercriminales utilizan diversos tipos de estrategias para poder acceder a cuentas de **redes sociales** y robar información personal que pueda significar algún tipo de ganancia económica para ellos. Así como pasa en muchas plataformas, los usuarios Twitter también son vulnerables a estos ataques.

En el caso de que las personas no tengan conocimiento sobre las modalidades de **engaños** y otros aspectos a tener en cuenta para mantener seguros sus datos, tienen más posibilidades de convertirse en víctimas de los delincuentes que buscan perjudicarlos.

Una forma en la que cibercriminales pueden vulnerar la **seguridad** de las cuentas de los usuarios es por medio de mensajes directos en los que se hacen pasar por miembros del equipo de **Twitter** y solicitan información sobre las credenciales de inicio de sesión, además de usar links sospechosos o archivos adjuntos que podrían estar infectados con malware de algún tipo.

Los cibercriminales pueden vulnerar la seguridad de las cuentas por medio de mensajes directos en los que se hacen pasar por miembros del equipo de Twitter. (ifep.com/Scyther)

Esta modalidad de engaño, llamada **phishing**, es una de las más comunes en internet y consiste en que los cibercriminales se hacen pasar por una empresa o personalidad que inspire confianza entre los usuarios para posteriormente solicitar **información** personal y que esta sea entregada de forma voluntaria por la víctima.

Cuidado con mensajes y links sospechosos

Para no ser una víctima de este tipo de engaño online, las personas tienen que considerar lo siguiente:

En principio, **Twitter** no pide contraseñas o datos de inicio de sesión a ninguno de sus clientes. Además, no envía mensajes directos (DM) a los usuarios, sino que realiza comunicaciones oficiales por medio de correos identificados con “@twitter.com” al final.

En caso de que una persona haya recibido un correo desde direcciones distintas y que aseguren ser de parte de la **red social**, el usuario debe eliminarlo de inmediato sin hacer clics o interactuar con su contenido de ninguna forma, incluidos sus archivos adjuntos y enlaces, pues existe la posibilidad de que puedan redirigir a **sitios web** inseguros o maliciosos.

Twitter no pide contraseñas o datos de inicio de sesión a ninguno de sus clientes. Tampoco envía mensajes directos (DM) a los usuarios, sino que realiza comunicaciones oficiales por medio de correos identificados. (Franziska Gabbert/dpa)

En caso de que se hayan recibido **mensajes directos** por Twitter que sean sospechosos:

– Se debe proceder a **reportarlo**.

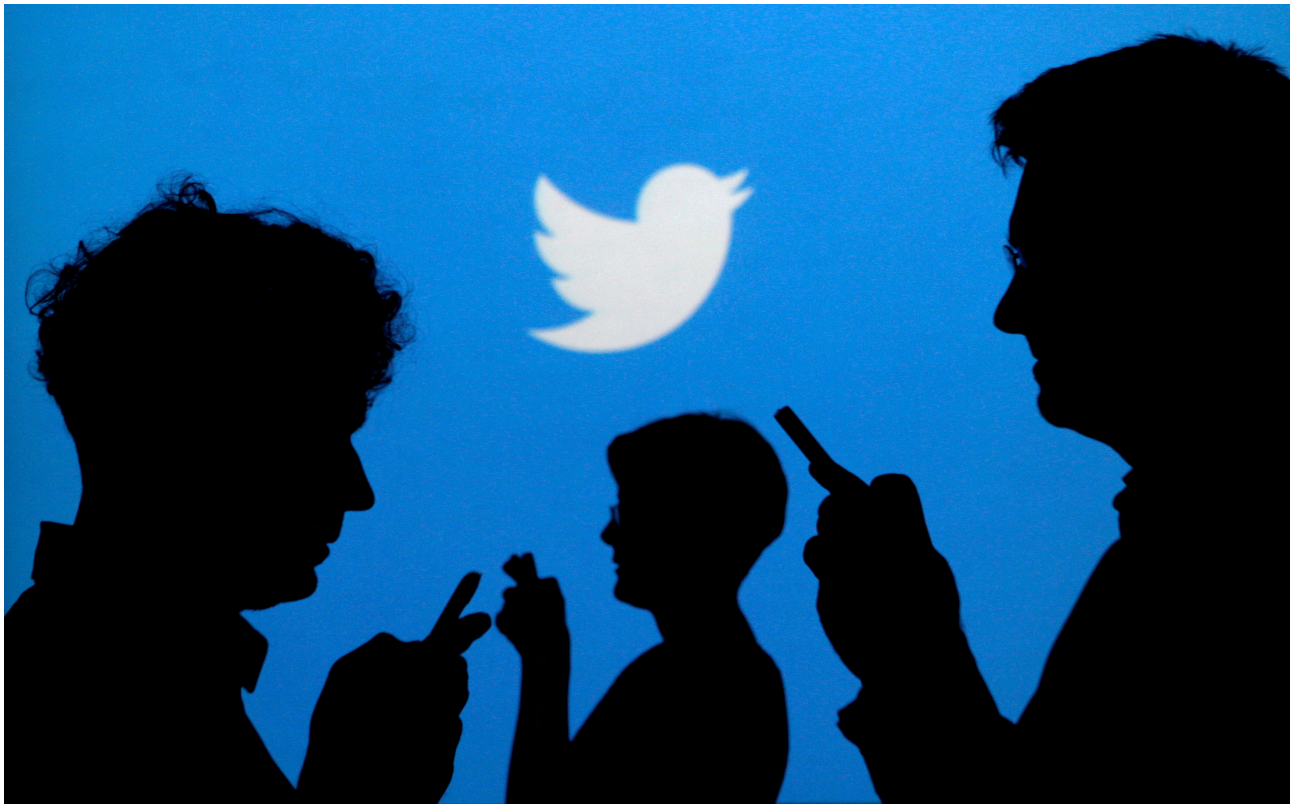
– Asegurarse de no descargar ningún tipo de archivo adjunto o hacer clic en un enlace dudoso. **Eliminarlo** de la bandeja es lo más adecuado.

– No se deben **compartir datos** de inicio de sesión o credenciales de acceso a la cuenta.

– Para evitar que pase nuevamente se pueden configurar las opciones para controlar qué tipo de usuario puede enviar mensajes directos.

Cómo mantener la cuenta segura

Si el usuario considera que la seguridad de su cuenta ha sido comprometida, lo primero que debe hacerse es **cambiar la contraseña**. La nueva clave debe incluir una mezcla de mayúsculas, minúsculas, número y caracteres especiales (#$%&). Usar un gestor de contraseñas es una buena opción.



Para proteger su cuenta, los usuarios deben asegurarse de no descargar ningún tipo de archivo adjunto o hacer clic en un enlace dudoso. (REUTERS/Kacper Pempel/Illustration/File Photo)

La contraseña de la cuenta de Twitter no debe ser similar ni la misma que se usa en otras redes sociales o sitios web.

Otra acción para reforzar la seguridad es activar la **autenticación en dos pasos** en la cuenta. De esta forma los usuarios podrán identificar inicios de sesión no deseados y se podrá prevenir el acceso a la cuenta desde dispositivos no autorizados.

Evitar compartir o dar permisos a otras personas o sitios web para acceder a la contraseña de la cuenta, sobre todo si se promete aumentar la cantidad de seguidores u obtener dinero de forma gratuita.

Tener en el dispositivo un buen sistema antivirus puede ayudar a evitar ser víctima de algún tipo de malware transmitido por medio de descargas o links maliciosos.

Fuente: Infobae