

TIPS DE SEGURIDAD EN TWITTER



CONFIGURAR VERIFICACIÓN DE INICIO DE SESIÓN

Configurar la cuenta para recibir alertas de inicio de sesión mediante la dirección de correo electrónico. Twitter proporciona mediante este control un código de respaldo en caso de pérdida o robo de información.



GESTIONAR PERMISOS DE APLICACIONES DE TERCEROS

Las aplicaciones de terceros son aplicaciones que compilan los desarrolladores externos en la plataforma de Twitter. Twitter no las posee ni está a cargo de su manejo. Cuando conectas una aplicación de terceros a tu cuenta de Twitter, le concedes a esa aplicación el acceso para utilizar tu cuenta. Configura adecuadamente los permisos de acceso de estas aplicaciones.



ELIMINAR LA UBICACIÓN

Evitar compartir tu geolocalización mediante los mensajes publicados (Tweet), Twitter permite eliminar la localización de publicaciones realizadas.



ATENCIÓN A LOS DMS

Los mensajes directos, también conocidos como DMs, es el medio por el cual puede ser víctima de ataques de phishing, no ofrezcas sus datos de username y password cuando lo soliciten por esa vía. En ese caso puedes reportar los DMs como spam en Twitter.

REFORZAR LAS CONTRASEÑAS

No olvidar crear contraseñas seguras, utilizar una contraseña única para cada una de tus cuentas, usar un gestor de contraseñas y configura doble factor de autenticación.



DENUNCIAR CUALQUIER VIOLACIÓN

Puedes denunciar directamente desde un perfil o un Tweet determinados incumplimientos, por ejemplo: spam, contenido abusivo o perjudicial, anuncios inapropiados, autolesiones y suplantación de identidad.



CSIRT
EQUIPO DE RESPUESTA A
INCIDENTES DE SEGURIDAD
DE LA INFORMACIÓN

E-Mail: info@cert.pa
Phone: +507 520-CERT (2378)
Web: <https://cert.pa>
Twitter: @CSIRTPanama