eti
Tecnologías de la Información BioCubaFarma

Intrusos en tus redes sociales

OCTUBRE 2023

CIBER-CAMPAÑA CSIRT-BCF

Contribuimos a su cultura sobre ciberseguridad

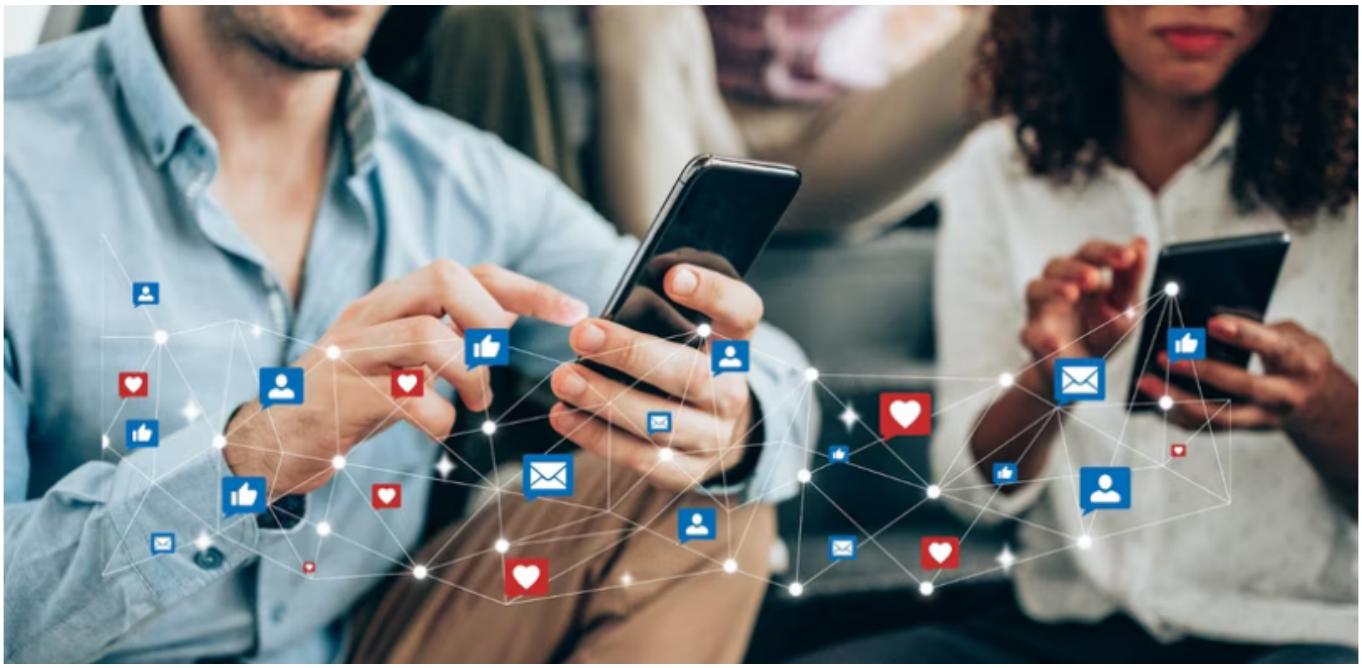
https://csirt.biocubafarma.cu/

Intrusos en tus redes sociales

csirt-bcf
equipo de respuesta a incidentes de ciberseguridad
BioCubaFarma

Recibes una notificación en tu smartphone: “Hemos detectado un intento de inicio de sesión inusual desde Río de Janeiro, Brasil”. Aunque el intento de inicio de sesión proceda de donde vives, o del otro lado del mundo, desde tu mismo modelo de teléfono o desde un dispositivo completamente distinto, la intención aquí es hacer que entres en pánico. Pero no te asustes.

Independientemente de que alguien esté intentando acceder a tu cuenta o no, no sirve de nada alterarse. A continuación, te contamos lo que podría ocurrir y qué hacer para ayudarte a mantener la calma y sobrevivir a este incidente con las mínimas pérdidas.



¿Cómo podría ocurrir?

Vamos a empezar averiguando cómo es posible que un extraño pueda haber accedido a tu cuenta. Puede ocurrir de varias formas.

1. Filtración de datos y el relleno de credenciales

Las noticias sobre filtraciones y violaciones de datos son muy frecuentes. Aunque estas fugas no involucren directamente a Facebook o Instagram, si se violó la seguridad de otro sitio web y los datos comprometidos incluyen la información de tu cuenta, los ciberdelincuentes tendrán tus credenciales en su poder. Con una lista de nombres de usuario de correo electrónico y contraseñas, pueden llevar a cabo un ataque de relleno de credenciales, es decir, pueden introducir las credenciales robadas en otras páginas. El éxito de esta práctica se debe a que los usuarios utilizan la misma contraseña para varias cuentas, un error involuntario, pero que es muy común.

2. Phishing

Los estafadores también pueden obtener tu nombre de usuario y contraseña mediante una estafa de phishing. Es probable que hicieras clic e introdujeras tus credenciales en una página falsa, pero convincente, de Facebook o Instagram.

3. Robo de contraseñas

Un malware también puede robar credenciales. Por ejemplo, muchos troyanos incluyen un keylogger integrado, un programa que registra las pulsaciones de teclas. Con este tipo de malware, los ciberdelincuentes tendrán todos los nombres y contraseñas que hayas introducido.

4. Robo de tokens de acceso

Tal vez alguien robó tu token de acceso. Para que no tengas que introducir tu contraseña cada que vez que inicies sesión en Facebook o Instagram, la aplicación guarda una parte de la información de inicio de sesión conocida como token de acceso, o solo token. Si un ciberdelincuente roba un token válido, puede acceder a la cuenta sin tu nombre de usuario y contraseña. ambién es posible robar los tokens mediante extensiones de navegador.

5. Inicio de sesión desde otro dispositivo

Seguramente has iniciado sesión alguna vez en Facebook o Instagram desde un dispositivo ajeno (en una fiesta, en la escuela, en el lobby de un hotel) y has olvidado cerrar sesión. O, por ejemplo, puedes haberte olvidado de cerrar tu sesión en un dispositivo que posteriormente has vendido o regalado, concediendo de este modo acceso a tu cuenta al receptor.

¿Qué puedes hacer?

El primer paso es iniciar sesión en tu cuenta, para ello utiliza la aplicación móvil de la red social o introduce la dirección manualmente en el navegador. Si la contraseña no funciona y no puedes acceder, ponte en contacto con el servicio de asistencia técnica de la cuenta e intenta restaurar el acceso a la cuenta afectada.

Si puedes iniciar sesión, dirígete a la configuración de la cuenta y comprueba que la notificación sea auténtica. Haz clic en *Dónde has iniciado sesión* y si no ves inicios de sesión sospechosos, puedes considerar el mensaje como phishing. En caso de que veas algo sospechoso en la lista de inicios de sesión, debes actuar lo antes posible para mitigar los daños: cierra tu sesión en todos los dispositivos de inmediato; configura una contraseña nueva y activa la autentificación en dos pasos.

Referencias

https://www.kaspersky.es/blog/suspicious-login-attempt-facebook-instagram/24803/