RECOMENDACIONES DE SEGURIDAD EN REDES SOCIALES

Instituto para la Protección de Personas Defensoras de Derechos Humanos y Periodistas

Medidas de seguridad para proteger cuentas de redes sociales

Te sugerimos las siguientes prácticas recomendadas para mantener tu cuenta protegida:

Acciones recomendadas:

- Crea una contraseña que tenga un mínimo de 10 caracteres. Cuanto más larga, mejor.
- Combina mayúsculas, minúsculas, números y símbolos.
- Usa una contraseña diferente para cada sitio web que visites.
- Conserva tu contraseña en un lugar seguro. Considera la posibilidad de usar algún software de administración de contraseñas para almacenar todas tus credenciales de inicio de sesión de manera segura.

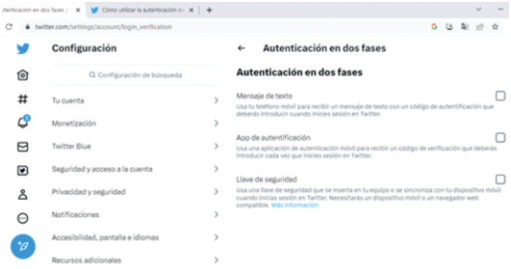
Acciones NO recomendadas:

- No utilices información personal en tus contraseña, como tu números de teléfono, fecha de nacimiento, tu mismo nombre, etc.
- No uses palabras comunes del diccionario, como "contraseña", "tequiero", etc.
- No uses secuencias del tipo "abcd1234" ni secuencias del teclado, como "qwerty".
- No uses la misma contraseña en distintos sitios web. La contraseña de tu cuenta de tu red social debe ser exclusiva para tu red social.

"Te aconsejamos que crees una contraseña segura y original".

Guía para TWITTER: Usa autenticación de dos pasos.

Haz clic en el ícono "Más" y selecciona "Configuración" y privacidad en el menú desplegable.



Para la versión de escritorio:

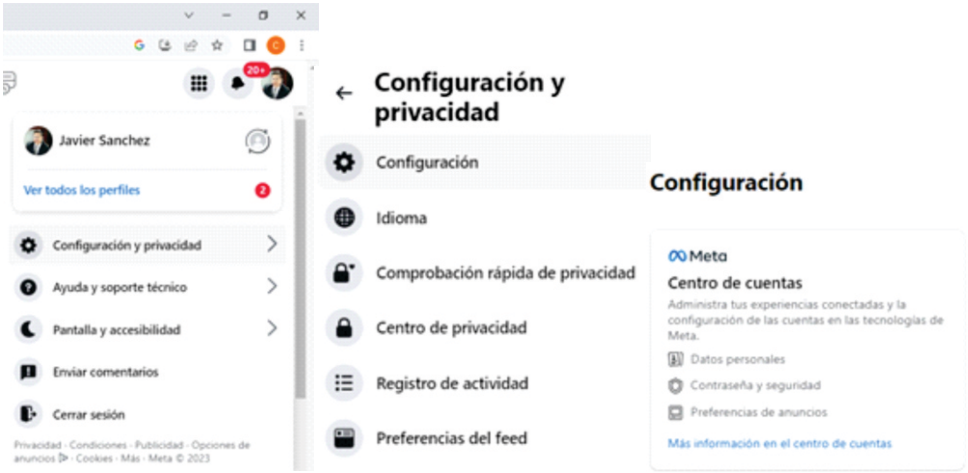
Paso 1. En el menú lateral, haz clic en "Más" y, luego, en "Configuración" y privacidad.
Paso 2. Haz clic en "Seguridad" y acceso a la cuenta y, luego, haz clic en "Seguridad".
Paso 3. Haz clic en "Autenticación" de dos fases.
Paso 4. Puedes elegir entre tres métodos: Mensaje de texto, App de autenticación o Clave de seguridad.
Paso 5. Una vez que te hayas inscrito e inicies sesión en tu cuenta, se te pedirá que indiques el método de autenticación de dos pasos que utilizaste en tu inicio de sesión anterior, junto con tu contraseña. También verás la opción para "Seleccionar otro método de autenticación de dos fases". Si deseas continuar, simplemente haz clic en el mensaje para seleccionar otro método. Sigue las instrucciones que se indican en pantalla para finalizar el inicio de sesión.

Sugerencia:

- Al utilizar la App de autenticación, tendrás que tener una App en tu teléfono celular, para que a través de ella te genere un código de seguridad cada vez que ingreses a tu red social (Ejemplo: Google Authenticador).
- El método de llave de seguridad requiere de una memoria USB para guardar código de recuperación.

Guía para FACEBOOK: Ofrece diferentes métodos de seguridad.

Ingresa a configuración y privacidad en el perfil de tu cuenta, y luego a configuración, luego en el centro de cuenta, ingresa a Contraseña y Seguridad.



Posteriormente selecciona los diferentes métodos de seguridad que te ofrece tu aplicación, se pueden seleccionar uno o más de los siguientes métodos.

Sugerencia:

- De igual manera que para TWITTER, si utilizas el método de App de autenticación, requieres la App en tu teléfono para generar código de autenticación, para poder ingresar a tu cuenta. (Ejemplo: Google Authenticador).
- El método de llave de seguridad requiere de una memoria USB para guardar código de recuperación.

⚠ Guía para INSTAGRAM: Cómo activar autenticación en dos pasos.

1. Abre Instagram desde tu app y ve al menú de configuración
2. Busca hacia abajo en la sección de seguridad
3. Selecciona autenticación en dos pasos

- Además de una contraseña segura es conveniente tener activada la VF2 en todas tus cuentas digitales. La mayoría de los servicios en línea y redes sociales tienen esa opción: cuando intentas acceder a tu cuenta con usuario y contraseña te pedirá además un código de verificación que te llegará a tu celular por medio de SMS o correo electrónico.

- La verificación o autenticación en dos pasos (VF2) es una capa extra de seguridad digital que protege tus cuentas en línea, evitando que alguien más acceda a ellas.

⚠ ¡Como evitar estafas!

Una técnica común usada para el robo de datos es el phishing, a través de ella los atacantes crean cuentas falsas para hacerse pasar por canales oficiales, cuentas de soporte de marcas o servicios. Desde ahí lanzan "anzuelos" o trampas para engañar y lograr que descargues un archivo o abras un enlace y facilites tus datos personales, como contraseñas y datos bancarios. Es importante reportar este tipo de cuentas cuando te encuentres con ellas.

Otro aspecto a tener en cuenta es la insignia de "cuenta verificada" con la palomita azul, esto pareciera ser señal de una cuenta confiable, pero incluso una cuenta verificada puede ser vulnerada y tener comportamientos sospechosos. Tome precaución con cuentas con comportamientos extraños, sospechosos. Lo mismo puede ocurrir con correos fraudulentos que incluyan logos oficiales. Por esta razón es importante mantenerte alerta y si algo te parece extraño, es mejor ignorar el mensaje y reportarlo.

Consulta herramientas recomendadas en:
https://socialtic.org/blog/seguridad-digital-estafas-instagram/

¡El IPPPDDHyP de Sinaloa te orienta y protege!

¡Acude a nosotros!

Calle Carlos Lineo #1997, Plaza Botánico,
Primer Piso, Locales 206-210
Col. Chapultepec, Culiacán, Sinaloa.

Teléfonos: 667 709 7521 y
6677097500 Ext. 100

Teléfono de Guardia:
66 74 89 98 32