EDUCACIÓN FINANCIERA EN TU INSTITUCIÓN

FRAUDES FINANCIEROS
¡CUÍDATE DEL SIM SWAPPING!

¿Qué es el SIM Swapping?

El SIM Swapping en una forma de fraude financiero en la que duplican la tarjeta SIM o chip para suplantar la identidad de sus víctimas y acceder a sus cuentas bancarias ligadas al número telefónico.

¿Cómo se realiza?

1. **Identifican a la víctima.** En la mayoría de los casos, los atacantes cuentan con información que les permite ubicar a sus potenciales víctimas.
2. **Cambian la tarjeta SIM.** El atacante influye en la compañía de telefonía móvil y convence a un representante para transferir el número de teléfono de la víctima a una nueva tarjeta SIM.
3. **Restablecen contraseñas.** El atacante inicia el restablecimiento de las contraseñas de las cuentas que estén ligadas al teléfono móvil.
4. **Acceden a las cuentas.** El atacante accede a las cuentas de la víctima e identifica las claves y las carteras que estén almacenadas en ellas.
5. **Roban.** Transfieren los fondos de la cuenta de la víctima a cuentas controladas por los atacantes.

Recomendaciones para evitar ser víctima de este fraude:

- Configura la doble autenticación y métodos de seguridad en tus aplicaciones.
- Ante el robo o extravío de tu celular, repórtalo a tu compañía telefónica y a tu institución financiera para proteger tu información personal y financiera.
- Actualiza tus contraseñas y las opciones de recuperación de tus cuentas de banca en línea, correo, redes sociales, entre otros.
- Si eres víctima del SIM Swapping o percibes que el chip de tu teléfono móvil dejó de funcionar, comunícate inmediatamente con tu compañía telefónica y tu institución bancaria.

¡Infórmate y protégete de los fraudes!

HACIENDA
SECRETARÍA DE HACIENDA Y CRÉDITO PÚBLICO

CONDUSEF
COMISIÓN NACIONAL PARA LA PROTECCIÓN Y DEFENSA DE LOS USUARIOS DE SERVICIOS FINANCIEROS

condusef.gob.mx