Estrategias de seguridad móvil para tesoreros: Cómo prevenir el SIM Swapping

Recopilado por Amalia Beltrán

Como líder financiero, gestionas la liquidez de tu empresa, tomas decisiones críticas y, por naturaleza, debes evitar el riesgo innecesario.
En un entorno operativo donde tu celular es una herramienta clave para autorizar transferencias internacionales o monitorear los movimientos de tu banca digital, la seguridad de tu dispositivo es tan crítica como la de las finanzas corporativas.
Hoy en día, las amenazas no sólo atacan los servidores corporativos, sino también las líneas personales de los tomadores de decisión mediante tácticas como el SIM Swapping (suplantación de la tarjeta SIM). Para garantizar la continuidad y seguridad de tus operaciones, te compartimos un protocolo de seguridad fundamental para proteger tu línea móvil.

El Registro Telefónico en México: ¿Qué es y por qué es un pilar de tu seguridad?

El registro telefónico en México es el proceso formal mediante el cual vinculas tu identidad a una línea móvil y a una tarjeta SIM, trámite que se hace únicamente a través de los operadores de telecomunicaciones oficiales.
Para un tesorero o CFO, este paso trasciende un simple trámite administrativo. Hoy en día, tu número celular funciona como un autenticador fundamental (token) para validar identidades, aprobar operaciones internacionales y recibir contraseñas de un solo uso (OTP). Si el registro de tu línea se ve comprometido o se realiza a través de canales no oficiales, abres una brecha para que ciberdelincuentes suplanten tu identidad y desvíen fondos.
Controlar este registro es el primer eslabón para blindar la tesorería de tu empresa.
A continuación, te compartimos el protocolo de seguridad que debes implementar en tu dispositivo corporativo o personal:

Antes del registro telefónico en México: Medidas de protección

La seguridad comienza en el momento de dar de alta tu línea. Para evitar vulnerabilidades desde el día uno:
Utiliza exclusivamente los medios oficiales de tu proveedor para el registro de tu línea.
Evita realizar pagos a externos o terceros por el registro de tu línea.
Protege tu identidad: no proporciones tu CURP, INE, RFC ni datos biométricos para dar de alta números que no te pertenecen.
Asegúrate de guardar los comprobantes del proceso, tales como folios, capturas de pantalla o correos de confirmación.

Protección Activa contra SIM Swapping

El SIM Swapping ocurre cuando un ciberdelincuente logra transferir tu número telefónico a una tarjeta SIM bajo su control, interceptando así tus llamadas y códigos de verificación.
Para proteger tu línea contra esta amenaza:
Establece un NIP de seguridad para tu tarjeta SIM.
Procura no depender exclusivamente de los mensajes SMS como método de validación de identidad siempre que existan otras alternativas.
Mantén la privacidad de tu número telefónico evitando su difusión en plataformas digitales y redes sociales.
Preserva tu seguridad al no emplear tu celular como un dato de identificación pública, a menos que resulte estrictamente indispensable.

Monitoreo de Actividad Sospechosa

La detección temprana es tu mejor herramienta para mitigar el riesgo de fraude. Debes mantener un monitoreo constante sobre el comportamiento de tu servicio móvil:
Mantente alerta ante la recepción de códigos OTP que no han sido solicitados.
Reporta de inmediato cualquier interrupción inesperada del servicio o señal móvil.
Presta atención a las notificaciones sobre trámites de portabilidad que no se iniciaron.

El eslabón humano: Control de tu información personal

La ingeniería social es el principal facilitador de los fraudes móviles. Reducir tu huella digital y cuidar los canales por los que compartes información sensible es vital:
Procura no divulgar tu número telefónico a través de las redes sociales.
Mantén a salvo tu información personal evitando el envío de imágenes de identificaciones como INE o CURP por canales no seguros.
Mantén precaución ante llamadas de desconocidos que posean tus datos personales; el hecho de que conozcan tu nombre no garantiza la autenticidad del contacto.