Ninguna operadora esta libre de que por medios ilegales obtengan tus datos. A continuación, os detallo los principales riesgos, junto con medidas preventivas para protegerte:

Riesgos Potenciales

1. Suplantación de Identidad (Phishing y Vishing)
   - Los atacantes pueden contactarte (por SMS, correo electrónico o llamadas telefónicas) haciéndose pasar por tu banco o por un servicio que uses, tratando de obtener información adicional, como códigos de acceso o contraseñas, para completar transacciones.

2. Fraude Bancario
   - Aunque solo el IBAN no es suficiente para realizar pagos o retirar dinero, en combinación con otros datos (como tu nombre y número de teléfono), el atacante podría intentar engañar a tu banco o a terceros para realizar transacciones o cambios no autorizados.

3. Fraude con Cuentas y Servicios Vinculados al Teléfono
   - Con el número de teléfono, los hackers pueden intentar redirigir SMS de verificación o recibir códigos de autenticación de dos factores. Esto les permitiría acceder a servicios que dependen de tu número de teléfono para la autenticación.

4. Ingeniería Social
   - Los atacantes pueden utilizar la información robada para engañar a amigos, familiares o colegas haciéndose pasar por ti o logrando que otros divulguen más datos sensibles.

Medidas Preventivas

1. Asegura la Autenticación de Dos Factores (2FA)
   - Evita la verificación por SMS: Usa autenticación de dos factores (2FA) basada en aplicaciones como Authy, Google Authenticator o Microsoft Authenticator en lugar de SMS, que es más vulnerable a redirecciones de SIM.
   - Activa 2FA en todos los servicios importantes: banca, correo electrónico, redes sociales y cualquier otra cuenta importante.

2. Configura Alertas de Seguridad en tu Banco
   - Activa las notificaciones de actividad en tu cuenta bancaria para recibir alertas de cualquier movimiento sospechoso o intento de cambio en los datos de acceso.

3. Bloquea la Portabilidad de SIM
   - Contacta a tu operadora de telefonía para solicitar un bloqueo de cambio de SIM. De esta forma, solo podrás hacer un cambio de SIM en persona con una identificación oficial.

4. Monitorea tu Cuenta Bancaria y Reporta Actividad Sospechosa
   - Revisa tus movimientos bancarios con frecuencia. Ante cualquier transacción o cambio sospechoso, notifícalo de inmediato a tu banco.

5. Cuidado con Llamadas o Mensajes de Desconocidos
   - Sé escéptico ante mensajes o lla´madas no solicitadas, incluso si parecen ser de tu banco o de un servicio legítimo. Los bancos nunca te solicitarán información sensible (como PIN o contraseñas) a través de llamadas o mensajes de texto.

6. Usa un Administrador de Contraseñas y Genera Contraseñas Seguras
   - Si tienes varios servicios, utiliza un administrador de contraseñas como Bitwarden o LastPass para crear y almacenar contraseñas únicas y complejas. Esto dificulta que un atacante adivine o acceda a tus cuentas.

En Caso de Sospecha de Fraude

- Reporta a tu Banco cualquier actividad sospechosa para que puedan bloquear temporalmente la cuenta.
- Informa a tu Operadora si crees que tu número de teléfono ha sido comprometido.
- Contacta a Autoridades:
https://www.guardiacivil.es/es/colaboracion/form_contacto/delitos_telematicos.html

https://www.incibe.es/

Con estas medidas puedes reducir considerablemente los riesgos y protegerte frente a intentos de fraude o ataques.