Tips para prevenir suplantación de identidad y fraude digital

¿Cómo prevenir y protegerse ante posibles delitos de fraude digital y suplantación de identidad a través del servicio de telefonía móvil? Movistar Perú ofrece recomendaciones a la población sobre este tema.

Cabe recordar que los fraudes digitales y accesos a cuentas bancarias de los ciudadanos a través del acceso no autorizado a sus líneas móviles requiere que los delincuentes accedan previamente a los datos personales de los usuarios de manera ilegal.

Por ello, Movistar realiza las siguientes recomendaciones para proteger la información personal de los usuarios y evitar caer en estafas:

- No responder correos de personas desconocidas ni dar información personal como nombre completo, DNI, fecha de nacimiento, número de celular, entre otros, en redes sociales, SMS o páginas webs que no sean seguras.

- No acceder a enlaces o links sospechosos que lleguen a través de mensaje de texto (SMS), mensaje de whatsapp, e-mail o llamadas, con mensajes como: “Actualiza tus datos y gana un Celular”,“¡Alo! Ayúdanos a actualizar tus datos aquí”, “Paga tu recibo con 70% de dscto.

ingresando a este link”, “Banco X: tienes una transferencia retenida, ingrese aquí”.

- No proporcionar su usuario y contraseña como respuesta a un SMS o correo electrónico.

- Comprar teléfonos móviles o contratar servicios móviles sólo en puntos de venta autorizados.

- Realizar pagos de servicios solo a través de los canales autorizados por Movistar: App Mi Movistar, Agencias, Bancos y sus aplicativos oficiales, así como billeteras digitales autorizadas.

Detección de fraude digital con la línea móvil

Desde el mes de setiembre 2022 se encuentra activa la Alerta vía SMS para prevenir los delitos de fraude digital bajo la modalidad de sim swapping o contrataciones de servicios no autorizadas por el titular. A través de esta alerta, promovida por OSIPTEL para ser implementada por todas las operadoras de telecomunicaciones, se avisa al cliente sobre el intento de cambio de SIM card o chip o la contratación de un servicio móvil.

En el caso de cambio de simcard, la activación del nuevo chip se hará efectiva luego de 4 horas. Se envía esta alerta para

que en caso el usuario no reconozca la transacción tenga tiempo de alertar a Movistar y/o su banco.

Movistar invoca a sus clientes a prestar especial atención a las alertas SMS y, en caso no reconozcan la transacción, tomar las siguientes acciones inmediatas:

- Contactar a Movistar para informar que se trata de un pedido no autorizado por el titular y proceder al bloqueo de la línea
- Contactar a su banco para el bloqueo de sus cuentas y transacciones.
- Realizar el cambio de las contraseñas de aplicaciones y cuentas de correo.

Cabe recordar que las reposiciones de chips se realizan de manera presencial con verificación biométrica, sin embargo, existen bandas delincuenciales que, a través de la clonación de huellas digitales y documentación falsa logran eludir estos controles. Como parte de las medidas adoptadas, también se ha limitado a un máximo de cinco intentos de verificación biométrica por trámite y por persona en el día para evitar que la verificación se obtenga luego de una cantidad anómala de rechazos, de acuerdo con lo dispuesto por el ente regulador.

Movistar Perú reafirma su compromiso para evitar las suplantaciones de identidad de los usuarios móviles, y reitera la importancia a sus clientes de cuidar de sus datos personales y no compartirlos con terceras personas, así como también realizar la contratación y pagos de servicios y compra de equipos en lugares autorizados.