Guía informativa de concienciación y prevención del fraude en operaciones de envío de dinero

La presente guía informativa tiene como finalidad informar y concienciar a clientes, empleados, agentes sobre las principales tipologías de fraude asociadas a los servicios de transferencia de dinero, así como establecer recomendaciones de prevención y canales de comunicación ante posibles incidentes.

1. Objetivo y Alcance

Las siguientes modalidades representan algunas de las casuísticas de fraude más habituales detectadas en el sector del envío de dinero.

Esta lista no es exhaustiva y podrá actualizarse periódicamente conforme a la evolución de los riesgos.

2. Principales Tipologías de Fraude

2.1 Estafa de Lotería, Premios y Sorteos

El estafador comunica falsamente a la víctima que ha resultado ganadora de un premio o sorteo, solicitando un pago previo para cubrir impuestos, gastos administrativos o comisiones. Tras recibir el dinero, el delincuente desaparece.

2.2 Estafa de Préstamos o Créditos Rápidos

En este caso, los estafadores se hacen pasar por agentes de crédito que ofrecen préstamos con condiciones muy atractivas (tipos de interés bajos, plazos flexibles, etc.). A cambio, solicitan pagos adelantados por conceptos como costes de apertura o tasas de gestión.
Tras recibir el dinero, no se otorga ningún préstamo y el estafador desaparece.

2.3 Estafa en Compras Online o Pago por Adelantado

A través de plataformas online, los delincuentes publican anuncios falsos de productos a precios muy bajos. Solicitan pagos por adelantado y, tras recibir el dinero, nunca entregan los bienes prometidos.

2.4 Estafa de los Abuelos o Emergencia Familiar

En este fraude, el estafador se presenta como un miembro de la familia o un tercero (como un médico o miembro de la policía) informando a la víctima de que un familiar cercano ha sufrido un accidente o está en una situación de emergencia.

Se solicita dinero de forma urgente para cubrir gastos médicos o cualquier otro tipo de gasto relacionado con el incidente.

2.5 Estafa Romántica o de Relación Online

La víctima conoce a una persona que vive fuera de España, a través de una red social o un sito online de citas y entabla una relación sentimental.

Posteriormente, el estafador empieza a solicitar dinero alegando emergencias, inversiones, gastos médicos o viajes. Una vez que el estafador recibe el dinero, corta toda comunicación y desaparece.

2.6 Estafa de Empleo

Los estafadores publican anuncios falsos de trabajos muy atractivos, a menudo con promesas de altos ingresos trabajando desde casa.

Los interesados deben pagar una cuota por materiales, formación o kits para poder comenzar a trabajar. En ocasiones, se envía un cheque falso a la víctima, que es solicitado para ser depositado y que devuelva el dinero "sobrante" por medio de una transferencia.

2.7 Estafa en Compra de Vehículos de Segunda Mano

El estafador publica anuncios falsos en portales de compra y venta de vehículos. Los vehículos están a un precio significativamente inferior al valor de mercado.

Una vez contactada la víctima, el vendedor alegará que el coche está fuera del país y pedirá un pago adelantado para enviarlo.

2.8 Estafa en Alquiler de Inmuebles

El estafador publica anuncios de propiedades inexistentes o que no están disponibles, solicitando depósitos o pagos por adelantado para asegurar una reserva. La víctima realiza el pago y nunca obtiene acceso al inmueble.
En algunos casos, los estafadores utilizan identidades de propietarios legítimos para realizar estos fraudes.

2.9 Robo de Identidad

El robo de identidad ocurre cuando un delincuente obtiene información personal de una víctima, ya sea a través de la sustracción de documentos o por medio de métodos fraudulentos como el phishing, para realizar operaciones de envío de dinero sin consentimiento del titular legítimo.

2.10 Fraude del Falso Proveedor o Factura Falsa

El estafador suplanta a un proveedor legítimo y solicita pagos urgentes alegando cambios en la cuenta de cobro o problemas administrativos.

2.11 Fraude de Inversión o Criptoactivos

Promesas de inversiones de alta rentabilidad (criptomonedas, trading, minería, plataformas falsas), solicitando transferencias de dinero para “activar” o “desbloquear” beneficios.

2.12 Fraude de Soporte Técnico

El delincuente se hace pasar por personal de soporte técnico (banco, empresa tecnológica, entidad de pago) e indica que existe un problema de seguridad que requiere un envío inmediato de dinero.

2.13 Fraude de Reembolso o Devolución

Se informa falsamente a la víctima de un reembolso pendiente o un error de pago, solicitando una transferencia para “regularizar” la operación.

3. Recomendaciones de Prevención

Les indicamos a continuación unos consejos importantes para protegerse contra el fraude en las operaciones de transferencia de dinero:

- **Verifique siempre la identidad del destinatario**: Nunca envíe dinero a una persona que no haya conocido en persona o a la que no confíe plenamente.

- **Desconfíe de pagos por adelantado**: Sea especialmente cauteloso si le solicitan pagos por adelantado para recibir un préstamo, un premio, un producto o una propiedad.

- **Ofertas *"demasiado buenas para ser verdad":*** Si una oferta parece demasiado atractiva o irrepetible, es probable que sea una estafa. Mantenga una actitud crítica frente a oportunidades que prometen grandes beneficios con poco esfuerzo.

- **Emergencias familiares**: Desconfíe si recibe una llamada telefónica o un mensaje urgente en las que se le informa que un familiar ha sufrido un accidente o se encuentra en estado de necesidad por una emergencia. Verifique siempre la identidad del solicitante por canales independiente antes de realizar cualquier pago. Los estafadores frecuentemente utilizan estos engaños para presionar emocionalmente a las víctimas.

- **No comparta nunca datos personales, bancarios o códigos de verificación:** nunca debe facilitar a terceros sus datos personales, bancarios o credenciales de seguridad, ya que esta información permite a los delincuentes suplantar su identidad y realizar operaciones de envío de dinero sin su consentimiento. Esto incluye, entre otros, su documento de identidad, número de cuenta bancaria, tarjetas de pago, contraseñas, códigos PIN, claves de acceso, códigos de un solo uso (OTP), códigos enviados por SMS, correo electrónico o aplicaciones de autenticación.

- **Compre productos de plataformas y proveedores reconocidos:** Asegúrese de que las transacciones en línea se realicen a través de plataformas verificadas y evite comprar productos a personas que se encuentren fuera de su país sin garantías de seguridad.

4. Responsabilidades y Buenas Prácticas del Cliente

Con el objetivo de prevenir el fraude, el uso indebido de los servicios de envío de dinero y los riesgos relacionados con el blanqueo de capitales y la financiación del terrorismo, se recomienda a los clientes de seguir las siguientes buenas prácticas cuando utilicen los servicios de la entidad.

4.1 Buenas Prácticas del Cliente

Se recomienda al cliente:

- **Facilitar información correcta y actualizada al registrarse** en la plataforma web y app de la empresa (*GiroDirecto*) para la realización de operaciones de envío de dinero online, así como al realizar operaciones presenciales en los agentes autorizados por I-Transfer, ya que datos incompletos o incorrectos pueden impedir la ejecución de la transferencia o retrasar su tramitación.

- **Custodiar adecuadamente su documentación, justificantes de operación y credenciales**, evitando su pérdida o uso indebido, especialmente en operaciones realizadas a través de canales digitales.

- **Verificar cuidadosamente la identidad del destinatario**, la relación con el mismo y el motivo del envío antes de confirmar la operación, especialmente cuando el beneficiario se encuentra en otro país o es una persona desconocida.

- **Utilizar los servicios de envío de dinero únicamente para fines legítimos**, evitando cualquier operación cuyo objetivo real no conozca o no pueda justificar adecuadamente.

- **Actuar con especial cautela ante solicitudes urgentes de envío de dinero**, promesas de premios, inversiones, préstamos, ofertas de empleo o situaciones de emergencia familiar, ya que son tipologías habituales de fraude en el sector de remesas.

- **Revisar los datos de la operación en el comprobante de liquidación antes de su confirmación**, teniendo en cuenta que los envíos de dinero, especialmente los internacionales, pueden ser difíciles o imposibles de recuperar una vez ejecutados.

- **Comunicar de inmediato a la entidad cualquier sospecha de fraude**, uso indebido de su identidad, pérdida de documentos o detección de operaciones que no reconozca. Asimismo, ante cualquier sospecha, recomendamos que cambie su contraseña de acceso a la plataforma de la entidad lo antes posible para prevenir futuros riesgos.

4.2 Actuación de la Entidad

Conforme a la legislación vigente en materia de prevención del blanqueo de capitales y financiación del terrorismo y fraude, la entidad informa de que:

- Podrá **realizar verificaciones adicionales** sobre determinadas operaciones de envío de dinero en conformidad con la normativa vigente en materia de PBC-FT o cuando se detecten factores de riesgo

- Podrá **solicitar información y/o documentación adicional** al cliente sobre el origen y procedencia de los fondos, el destino del envío o la relación con el beneficiario.

- En determinados casos, la entidad podrá **no ejecutar o bloquear una operación**, cuando existan indicios de fraude, uso indebido del servicio o riesgos PBC-FT.

5. Comunicación de Incidentes y Fraudes

Si sospecha o confirma haber sido víctima de fraude, deberá comunicarlo de inmediato a través de los siguientes canales:

- Correo electrónico al mail: antifraude@i-transfer.net

- Atención al Cliente: +34 91 502 5800

Asimismo, se recomienda presentar denuncia ante las Fuerzas y Cuerpos de Seguridad del Estado.

Nota:
La presente guía tiene carácter meramente informativo y preventivo, y no sustituye a las condiciones contractuales aplicables al servicio de envío de dinero de I-Transfer Global Payments EP, S,A.