Guía antifraude 2025: las trampas digitales más creativas y cómo desarmarlas

El fraude digital en México no es novedad, lo preocupante es la rapidez con la que evoluciona y la sofisticación de sus métodos. De acuerdo con Sumsub, estas prácticas crecieron 27% en un año y las identidades falsas aumentaron más de 1,200%. Por su parte, la CONDUSEF registró en 2023 más de 20,000 millones de pesos reclamados por fraudes cibernéticos.

Estos delitos ya no se limitan a correos sospechosos. Hoy los defraudadores se hacen pasar por bancos, comercios o incluso por familiares, llegando a imitar voces con inteligencia artificial para engañar. En este contexto, **Héctor Gutiérrez, director de Seguridad de Kueski**, comparte los fraudes más identificados en el ecosistema digital y las recomendaciones clave para no caer en ellos.

Historias que parecen ficción, pero son reales

- **El préstamo fantasma.** Claudia descargó una app de crédito, hizo un "depósito de seguridad" y dio acceso a sus contactos. Nunca recibió el dinero, pero sus conocidos sí recibieron mensajes intimidatorios.
- **La buena samaritana en Facebook.** Al quejarse públicamente por una falla en una app para pagar un servicio, Rosa fue contactada por un perfil "amable" que la guió por WhatsApp a una cuenta falsa para hacer su pago. Agradeció la ayuda, depositó y fue bloqueada al instante.
- **El hijo detenido.** Jorge recibió una llamada con una voz idéntica a la de su hijo, pidiendo dinero urgente para liberarlo tras un supuesto accidente. Era un deepfake. Al llamar directamente a su hijo, descubrió el montaje.
- **Validación de identidad con engaños.** Durante la verificación de antecedentes para el empleo de sus sueños, Juan accedió a que un supuesto gestor le tomara una foto a su rostro en tiempo real y a su INE. Al día siguiente, las alertas de su Buró de Crédito se dispararon: alguien usaba su identidad para solicitar múltiples créditos.
- **El pago adelantado.** Mariana recibió una llamada supuestamente de su tienda departamental ofreciendo liquidar anticipadamente su plan a meses con un descuento exclusivo. El número parecía legítimo. Por suerte, verificó en la app oficial y descubrió que era un fraude.
- **Directivo en apuros.** Laura, administradora en una empresa, recibió un mensaje de WhatsApp del supuesto Director General. Le pidió una transferencia urgente para un proveedor, explicando que estaba en una junta y no podía acceder a sus fondos. La foto de perfil era la misma y el tono autoritario. Al verificar con él, supo que todo era falso.

Estas historias muestran que los criminales ya no buscan solo vulnerar sistemas: buscan vulnerar emociones.

Checklist antifraude 2025: hábitos simples que te protegen

“Los fraudes digitales usan la urgencia y el miedo. El problema no es que las personas no sepan de tecnología, sino que reaccionan bajo presión. Por eso, la mejor defensa no son solo controles técnicos, sino información clara y hábitos financieros seguros”, explica Héctor Gutiérrez, director de Seguridad de Kueski.

Entre las recomendaciones más importantes para evitar caer en fraudes, destacan:

1. **Consulta SIPRES.** Antes de confiar en cualquier entidad financiera, verifica si está en el registro de la Condusef. Si no aparece, evita esa empresa.
2. **No pagues adelantos.** Ningún crédito legítimo solicita un depósito previo para liberar fondos.
3. **Válida llamadas sobre tus pagos.** Si tienes planes a meses en tarjetas de crédito, tiendas departamentales o apps, recuerda: ninguna institución te llamará para pedir un pago adelantado si vas al corriente.
4. **Ten claros tus días de pago y montos.** Llevar un control personal de fechas de corte, pagos mínimos y saldos pendientes te permite identificar de inmediato llamadas fraudulentas.
5. **Desconfía de la urgencia.** Si un mensaje te presiona con frases como “última oportunidad” o “paga ya”, detente y confirma directamente con la institución.
6. **Pregunta de seguridad con tu círculo cercano.** Establece una palabra clave con familiares o amigos para confirmar emergencias reales.
7. **Cuidado con números extraños.** Si un contacto cercano te escribe o llama desde una lada que no corresponde al país donde vive, sospecha de inmediato.
8. **No hagas clic en links dudosos.** Evita abrir enlaces de SMS, correos o WhatsApp; entra siempre directo a la app o sitio oficial.
9. **Fíjate en qué permisos pide una app.** Si solicita acceso a contactos, fotos o ubicación sin razón, es una alerta.
10. **Verifica siempre los canales oficiales.** Llama únicamente a los números publicados en la página oficial. Nunca compartas contraseñas ni códigos por teléfono.

A medida que la tecnología se vuelve más compleja, también lo hacen las estafas. Frente a esto, la defensa más poderosa sigue siendo el criterio: detenerse, verificar y preguntar antes de actuar. A veces, un minuto basta para proteger tu información y tu dinero.

Por eso, estos consejos compartidos por el equipo de seguridad de Kueski, por simples que parezcan, pueden marcar la diferencia entre ser víctima de un fraude o mantener el control sobre tus finanzas.