

El fraude ya no roba: convence

Así operan los nuevos



En los últimos años, los fraudes financieros dejaron de ser casos aislados para convertirse en parte del día a día. No porque las personas sean distraídas, sino porque las personas delincuentes perfeccionaron sus métodos y aprendieron a aprovechar algo muy humano: la prisa, confianza, el cansancio y la costumbre de hacer todo a través del celular.

Hoy, más que “personas estafadoras”, enfrentamos operaciones que analizan cómo reaccionamos y qué emoción activar para que demos clic donde no deberíamos. Por eso incluso quienes tienen experiencia digital pueden caer. El fraude ya no es solo tecnológico; ahora es conductual.

¿De qué estamos hablando?

Reportes recientes de la CONDUSEF muestran una tendencia clara: ya no buscan robar por la fuerza, sino convencer. La persona estafadora no necesita entrar a un banco; basta con hacer creer que quien llama, escribe o envía un enlace es alguien legítimo.

Por eso abundan las llamadas que simulan ser de instituciones bancarias, mensajes con el tono exacto, enlaces que parecen oficiales y perfiles falsos que ofrecen créditos exprés o inversiones milagrosas. Todos comparten la misma estrategia: **generar urgencia para que la persona actúe rápido y piense poco.**

Uno de los patrones más frecuentes es el engaño telefónico disfrazado de “verificación”. No inician pidiendo datos; empiezan creando alarma: un supuesto movimiento extraño, un cargo no reconocido o una alerta de seguridad. Funciona porque apela al instinto de proteger lo propio.

Aunque la CONDUSEF ha insistido en que los bancos nunca solicitan claves por teléfono, las personas delincuentes modifican su discurso para sembrar duda. No buscan información: quieren que la persona reaccione impulsivamente.

Otros tipos de fraudes

1

Enlaces falsos y páginas clonadas

Ya no son mensajes con errores; ahora replican páginas completas con logotipos, colores y tipografías idénticas. Los enlaces llegan con supuestas devoluciones, beneficios o “correcciones urgentes”.

Este tipo de engaño se aprovecha de la familiaridad: cuando algo “se parece” a lo oficial, el cerebro se relaja y es justo ahí donde ocurre la captura de datos.

2

Redes sociales y perfiles falsos

Esta tendencia se ha fortalecido en redes sociales: créditos fáciles, inversiones “garantizadas”, supuestos asesores que escriben por mensaje directo y ofertas que “solo duran unas horas”.

Los perfiles falsos que se hacen pasar por instituciones o intermediarios financieros también están en aumento. Funcionan porque mezclan inmediatez con confianza: si algo aparece en el celular todos los días, parece real.

3

Fraudes con inteligencia artificial (IA)

Gracias al uso de inteligencia artificial, hoy es posible imitar voces con tanta precisión que incluso las personas más cautas pueden confundirse. Existen casos donde la llamada suena idéntica a la de un familiar o a la de un ejecutivo real.

Las voces sintéticas replican acentos, pausas y tonos, provocando que la reacción emocional gane terreno. Lo mismo ocurre con imágenes, mensajes o comprobantes falsificados con IA. Ya no dependen de textos sospechosos; dependen de imitaciones casi perfectas. La lección es clara: aunque todo parezca auténtico, siempre hay que verificar por un canal oficial.

4

Skimmers y robo de datos en cajeros

Mientras los fraudes digitales evolucionan, otros siguen presentes de forma tradicional, como los skimmers. Estos dispositivos se colocan en cajeros automáticos o terminales y copian la información de la tarjeta sin que la persona lo note.

Aunque su tecnología no ha cambiado tanto, su modo de operar sí: los colocan en horarios de poco movimiento, en cajeros con baja vigilancia o en establecimientos donde la tarjeta se entrega por unos segundos. Por eso es indispensable revisar la ranura del cajero, tapar el NIP y evitar equipos con daños visibles. Es un fraude antiguo, pero vigente.

5

Promociones y estafas estacionales

Quienes realizan este tipo de acciones aprovechan temporadas específicas: inicio de año, regreso a clases, vacaciones o semanas de descuentos. En esos momentos aumentan las promociones falsas, sorteos inexistentes o supuestas devoluciones. La lógica es simple: fechas con presión generan menos tiempo para verificar.

A esto se suman los trámites “urgentes”: renovaciones, supuestas multas o pagos “obligatorios”. Basta un archivo, una notificación o un número de referencia para generar alarma. No requieren tecnología avanzada; basta con provocar miedo o presión temporal.

El fraude moderno ya no ataca sistemas, sino rutinas, por eso la prevención debe cambiar. No basta con saber que existen personas delincuentes: hay que entender cómo operan. La Educación Financiera busca justo eso: reconocer señales de alerta, saber que un crédito legítimo no pide anticipos, que ninguna institución presiona con urgencia y que voces o mensajes pueden falsificarse. Los fraudes seguirán evolucionando, pero también nuestra capacidad para detectarlos y anticiparlos. La clave está en pausar unos segundos para revisar y verificar: esa atención consciente es hoy la mejor defensa.

