OPINIÓN

DESPUÉS DE LA PANDEMIA

Estamos en 2026: no te van a "hackear", te van a "convencer"

Enrique Dans

Publicada 11 marzo 2026 02:40h

La ciberdelincuencia financiera de 2026 ya no se parece a la caricatura del hacker encapuchado tecleando en la oscuridad. Es mucho más simple y, precisamente por eso, mucho más eficaz: consiste en conseguir que seas tú quien abra la puerta.

El cóctel es perfecto: el móvil como centro de nuestra vida financiera (banca, Bizum, compras, autenticación, mensajería) y la inteligencia artificial como multiplicador del engaño, capaz de generar mensajes, voces y contextos verosímiles a escala industrial. El resultado no es un ataque técnico sofisticado, sino **un ataque psicológico optimizado.**

Conviene entenderlo desde el principio: la inmensa mayoría de fraudes actuales son ingeniería social. No "rompen" el sistema, te convencen para que lo uses contra ti. El mensaje puede llegar por correo, SMS, WhatsApp, redes sociales o llamada telefónica.

El guion casi siempre es el mismo: urgencia, miedo, recompensa o culpa. "Tu cuenta será bloqueada", "te han hecho un cargo", "tienes un reembolso pendiente", "hay un problema con tu paquete". Si te meten prisa, ya estás dentro del diseño. Esa emoción no es casual: **es el mecanismo.**

La regla de oro es brutalmente sencilla y, sin embargo, es la que más se incumple: no confíes nunca en un enlace que te llega empujado por un tercero. Ni por email, ni por SMS, ni por mensajería. Si el aviso parece real, no lo compruebes pinchando.

La autenticación de doble factor sigue siendo una de las mejores barreras

Entra tú por tu propio camino: abre la app oficial del banco, escribe la dirección en el navegador, llama al número que ya tienes guardado. El *phishing* y el *smishing* funcionan porque nos ahorran un paso y nos venden comodidad. Ese clic "rápido" es el negocio del estafador.

Segunda idea clave: los códigos de un solo uso no son un trámite, son dinero. Si alguien te pide un código "para cancelar una operación", "para verificar tu

identidad" o "para reforzar la seguridad", detente.

En muchísimos fraudes recientes el atacante no necesita tu contraseña; necesita que tú le dictes el código que el banco te está enviando para autorizar la operación. Es perverso porque el sistema funciona bien: **el banco te avisa, pero tú entregas la llave temporal al delincuente.**

La autenticación de doble factor sigue siendo una de las mejores barreras, pero solo si la usas con criterio. Actívala siempre que esté disponible. Y, cuando puedas, prioriza métodos más resistentes que el simple SMS: aplicaciones de autenticación, confirmaciones dentro de la app oficial o passkeys.

El secuestro de SIM (SIM swapping) no es ciencia ficción: si alguien consigue duplicar tu tarjeta o tomar control de tu número, puede recibir tus códigos. Si pierdes cobertura de repente o tu operadora te notifica un cambio que no has pedido, trátalo como una emergencia.

> *Las redes de mulas financieras crecen porque el fraude necesita dispersar fondos rápidamente antes de que el banco pueda bloquearlos*

El móvil merece un capítulo aparte porque se ha convertido en el punto único de fallo más frecuente. Si tu banco, tu correo, tu mensajería y tu segundo factor viven en el mismo dispositivo, ese dispositivo es tu caja fuerte.

Configúralo como tal: PIN largo mejor que patrón, biometría activada, sistema y apps actualizados, instalación solo desde tiendas oficiales y revisión periódica de permisos. No instales aplicaciones "para que el banco te ayude": ningún banco serio te pedirá que instales software remoto para "proteger" tu cuenta.

La inteligencia artificial añade un matiz inquietante: **la voz ya no prueba nada.** El viejo vishing o llamada fraudulenta se refuerza ahora con voces generadas que imitan tonos y estilos.

El llamado "fraude del CEO" o del familiar en apuros puede llegar en forma de nota de voz convincente. La tecnología lo facilita, pero el patrón es el de siempre:

urgencia y aislamiento.

“No cuelgues”, “hazlo ahora”, “no se lo digas a nadie”. Si alguien que supuestamente es tu banco te pide mover dinero a otra cuenta “segura”, dictar un código o instalar algo, estás ante un guion clásico con envoltorio nuevo.

Otra norma útil: no utilices el mismo canal para resolver el problema que ese canal te plantea. Si el aviso llega por SMS, no respondas al SMS. Si llega por llamada, no sigas en la llamada. Corta y verifica por un canal alternativo que tú controles. Esa separación es una de las pocas cosas que el estafador no puede neutralizar con creatividad.

También conviene desconfiar de las oportunidades demasiado bien empaquetadas: inversiones “garantizadas”, criptomonedas con rentabilidad fija, empleos que consisten en “mover dinero” entre cuentas a cambio de comisión. Las redes de mulas financieras crecen porque el fraude necesita dispersar fondos rápidamente antes de que el banco pueda bloquearlos. Si te usan como intermediario, no eres una víctima ingenua: **puedes acabar con responsabilidad penal.**

Europa está introduciendo medidas como la verificación del nombre del beneficiario frente al IBAN para reducir errores y fraudes en transferencias, pero ninguna regulación sustituye al sentido común. La seguridad no es un estado, es un hábito. Y el hábito más importante es introducir fricción: parar, respirar, comprobar.

Si, pese a todo, caes, el tiempo es decisivo. Contacta de inmediato con tu banco por los canales oficiales, bloquea tarjetas y accesos, cambia contraseñas desde un dispositivo limpio, revisa sesiones abiertas y denuncia. Cuanto antes actúes, **más posibilidades hay de frenar o revertir el movimiento del dinero.**

En realidad, la guía completa cabe en unas pocas líneas: no pinches enlaces que te empujan; no dictes códigos; no instales nada porque **“te lo pide el banco”;** activa el doble factor; protege tu móvil como si fuera tu cartera.

Porque lo es. En 2026 no te van a hackear con una técnica exótica. Van a intentar convencerte. Y la diferencia entre perderlo todo o no suele estar en unos segundos de pausa.

***Enrique Dans es profesor de Innovación en IE University.

MÁS EN OPINIÓN

La fatuidad del pacifismo de Sánchez

Lorenzo Bernaldo de Quirós

¿Otra crisis energética?

Miguel Sebastián

¿Zapatero, entre el lobby y la consulta?

José Ramón Pin Arboledas

Un "no a la guerra" falso para entregar España a China

Daniel Lacalle

SE EL PRIMERO EN COMENTAR

VER COMENTARIOS