Cuando el fraude digital llega en papel: anatomía de un fraude híbrido

Imagen 1 fuente: Generación IA

El timo que no llegó por email: cuando el phishing se esconde en tu buzón

Vivimos en un estado de alerta casi permanente. Nos han enseñado a desconfiar de cada enlace sospechoso que recibimos en un SMS, un correo electrónico o un mensaje de WhatsApp. La mayoría de nosotros ya no caemos en la trampa de hacer clic en enlaces acortados que prometen paquetes imposibles o facturas impagadas. Pero ¿qué sucede cuando el vector de ataque abandona la pantalla y se materializa en un objeto tan cotidiano y aparentemente inofensivo como una carta dentro de un sobre, depositada en el buzón de casa?

Ese fue el caso que nos llegó. Un ataque de phishing que no comienza con un clic, sino con el gesto físico de abrir el correo postal. Y la primera e importantísima alerta no la dio el mensaje del interior, sino el propio sobre que lo contenía.

La primera trampa: cuando el anzuelo se esconde tras un espejismo de tranquilidad

El caso es una variante sofisticada de las campañas de suplantación de identidad que la empresa Ledger, el conocido fabricante francés de carteras frías de criptomonedas, lleva tiempo denunciando. En su página oficial sobre campañas de phishing, Ledger advierte activamente sobre cómo los estafadores han comenzado a enviar cartas fraudulentas por correo postal, haciéndose pasar por comunicaciones oficiales. El formato varía, pero el objetivo es siempre el mismo: que el usuario escanee un código QR o visite un sitio web falso e introduzca su Frase de Recuperación de 24 palabras, la llave maestra de sus fondos.

Lo verdaderamente insidioso de esta carta es que su vector de entrada es pacífico y tranquilizador. No tiene el tono urgente y amenazante de un email fraudulento clásico. Todo en ella está diseñado para adormecer nuestras defensas naturales. La comunicación habla de un producto que sabemos que tenemos. Menciona a una empresa en la que realmente compramos. Incluye incluso direcciones web genuinas de la compañía, creando una sensación de normalidad y transparencia. Es una coreografía perfecta para generar confianza.

Y entonces, tras ese meticuloso paseo por lo familiar y lo correcto, cuando la guardia ya ha bajado, aparece el anzuelo: un código QR. No un enlace que podamos inspeccionar, no una URL que invite a la sospecha, sino un simple código impreso que, según la carta, está ahí precisamente para facilitarnos el acceso. "Para su comodidad", "acceso rápido", "para agilizar el proceso de verificación". Es la fachada de un servicio excelente cuando, en realidad, es la puerta de entrada a un dominio fraudulento. Así funciona el *quishing*: un caballo de Troya impreso que convierte un acto de confianza en el inicio de un expolio digital.

La primera línea de defensa: la documentoscopia del sobre

Aquí reside el verdadero punto de inflexión. Aunque la carta en sí era una réplica casi perfecta de una comunicación oficial de Ledger, la primera alerta de que algo no cuadraba no vino de su contenido, sino de su **continente**: el sobre.

Uno de los aspectos que más nos hizo sospechar fue que Ledger tiene su sede social en Francia, pero la carta que recibimos no llegó de allí. El matasellos era inequívoco: Madrid. Y el franqueo no era el típico sello de un gran envío comercial, impreso mecánicamente, sino un sello físico pegado en la esquina del sobre y matasellado. Un detalle que habría pasado desapercibido para la mayoría, pero que es una bandera roja enorme para cualquiera que observe lo que tiene entre las manos.

Imagen 2 fuente: Propia

Este detalle es un ejemplo perfecto de **documentoscopia forense**, la ciencia que estudia y analiza documentos para determinar su autenticidad. Esta disciplina examina elementos como el papel, la tinta, la impresión y, en este caso, los sellos y matasellos. En nuestro caso, el análisis del sobre reveló la contradicción geográfica entre el origen declarado de la empresa y el lugar real desde el que se envió la carta. Una incoherencia que pasaría desapercibida para la mayoría, pero que es una bandera roja enorme para cualquier persona entrenada en verificar la autenticidad de un documento.

El origen de los datos: por qué sabían quién eras y qué compraste

La pregunta inevitable es: ¿cómo consiguieron los delincuentes tu nombre, tu dirección y el dato exacto de que posees un dispositivo Ledger? La respuesta es tan inquietante como sencilla: la propia empresa sufrió filtraciones masivas de datos de sus clientes. No se trató de un ataque a tu ordenador ni a tu teléfono; el fallo de seguridad estuvo en la base de datos de la compañía a la que confiaste tu información.

En julio de 2020, un atacante accedió a la base de datos de comercio electrónico y marketing de Ledger. En un primer momento se habló de 9.500 clientes

afectados, pero a finales de ese año se descubrió que circulaban por foros de hackers los datos detallados de 272.000 clientes: nombres completos, direcciones postales, números de teléfono e información sobre los productos adquiridos. Además, a principios de 2026, un nuevo incidente afectó a un proveedor logístico externo, Global-e, exponiendo nuevamente direcciones y detalles de compra.

Con esa información en sus manos, los estafadores pudieron dejar atrás los ataques masivos y lanzar una campaña de phishing increíblemente personalizada: cartas que llegan a tu buzón con tu nombre real, mencionando tu dispositivo y apelando a una urgencia que imita a la perfección una comunicación oficial.

La pregunta incómoda: ¿por qué seguían ahí mis datos?

Llegados a este punto, surge una cuestión que rara vez se plantea y que, sin embargo, es el verdadero nudo del problema: **¿por qué conservaba la empresa mis datos tanto tiempo después de una única compra?** ¿Es realmente imprescindible guardar el nombre, la dirección y el historial de productos de un cliente que quizá solo adquirió un dispositivo una vez?

Conviene ser justos antes de juzgar. Las empresas como Ledger no conservan datos por capricho. Existen obligaciones legales y operativas que lo exigen. La normativa fiscal europea obliga a mantener los datos de facturación durante un plazo de entre cuatro y seis años. La atención al cliente, las garantías de producto y la propia logística de envío son imposibles sin conservar, al menos, los datos esenciales. El Reglamento General de Protección de Datos no prohíbe almacenar información; exige hacerlo con una finalidad legítima, durante un tiempo proporcionado y con las debidas garantías de seguridad.

El problema, por tanto, no es la existencia del dato en sí. El problema es la **mala gestión del ciclo de vida del dato**. Y ahí es donde muchas empresas fallan de forma sistemática.

El primer pecado es la **sobrerrecogida de información**. Se almacenan más datos de los necesarios: números de teléfono que no son imprescindibles, históricos de compra que se conservan indefinidamente, información que nunca

debió salir de un proceso de compra puntual. Se vulnera así el principio de minimización que exige el RGPD: solo debes guardar aquello que sea estrictamente indispensable.

El segundo es la **retención indebida**. Datos de clientes inactivos durante años, información que ya ha cumplido su finalidad operativa, bases de datos que nadie se ha molestado en depurar. Si ya no necesitas ese dato, conservarlo no es prudencia: es un riesgo innecesario.

El tercero, y más grave, es la **seguridad insuficiente**. Bases de datos mal protegidas, proveedores externos con accesos vulnerables como el caso de Global-e, controles de acceso internos deficientes. El delincuente no crea el dato; simplemente explota una oportunidad que la empresa dejó abierta.

Desde la criminología, la **prevención situacional del delito** ofrece una estrategia clara: reducir el valor y la accesibilidad del objetivo. Aplicado a los datos, esto significa menos datos almacenados, menos tiempo de exposición y mejor protegidos. El mejor dato protegido es el que nunca se almacenó o el que ya fue eliminado a tiempo. La conclusión es meridiana: no se trata de no guardar datos —eso es inviable—, sino de guardar menos, durante menos tiempo y con protecciones reales. Muchos ataques como el que describimos simplemente no existirían si las empresas aplicaran este principio con rigor. El dato que estás protegiendo con tanto celo en tu dispositivo personal ya fue expuesto, sin que tú lo supieras, en un servidor que alguien olvidó blindar.

El cliente no fue responsable

Este punto es crucial para entender la naturaleza del ataque: **el cliente no cometió ningún error de seguridad**. No hizo clic en un enlace sospechoso, no descargó ningún archivo malicioso ni compartió sus datos por descuido. El fallo que permitió a los delincuentes conocer su nombre, su dirección y el tipo exacto de cartera que poseía fue ajeno a él. La responsabilidad principal recayó en la empresa a la que confió esa información. Fue la propia Ledger, primero en 2020 y después a través de un proveedor logístico externo en 2026, quien sufrió brechas que expusieron datos sensibles de cientos de miles de personas. En otras palabras, quien compró un dispositivo para proteger sus activos digitales acabó desprotegido precisamente porque la compañía no custodió correctamente la

información que él le entregó. La carta en el buzón, con su matasellos impostado y su QR fraudulento, es la consecuencia directa de una cadena de seguridad que se rompió en el eslabón corporativo, no en el personal.

Más allá de la pantalla: la seguridad que mira, escucha y toca

Este caso nos obliga a replantear por completo lo que entendemos por "seguridad". Durante años, la ciberseguridad se ha centrado en proteger el mundo virtual: contraseñas robustas, doble factor de autenticación, antivirus, enlaces sospechosos... Pero la realidad es que las amenazas ya no entienden de fronteras entre lo digital y lo físico. La seguridad moderna exige una visión integral, una higiene de vida digital y física que va mucho más allá de no hacer clic en enlaces extraños.

Hoy, la seguridad también significa prestar atención a lo que está en nuestras manos. Un sobre con matasellos de Madrid cuando la empresa está en Francia debe activar las mismas alarmas que un remitente desconocido en un email. Un código QR pegado en una pegatina en un parquímetro merece la misma desconfianza que un enlace acortado en un SMS. La seguridad empieza por lo que vemos, por lo que tocamos, por lo que decidimos abrir físicamente.

Significa también ser conscientes de lo que decimos y de lo que compartimos. No solo en redes sociales, sino en cada interacción. Las filtraciones de datos convierten información inocua —nombre, dirección, un modelo de dispositivo— en la munición perfecta para un ataque dirigido. Y, sobre todo, significa aceptar que nuestra seguridad no depende únicamente de nuestras acciones, sino también de cómo protegen nuestros datos aquellos a quienes se los confiamos.

La gran lección de este timo híbrido es que el buzón de casa es ahora una extensión más de la bandeja de entrada. En un mundo donde el fraude puede llevar matasellos y presentarse en papel de alta calidad, la prevención no puede limitarse a un antivirus. Hay que educar la mirada, mantener una sana suspicacia ante lo que no cuadra y recordar que, por muy convincente que parezca una carta, siempre es más fácil falsificar un sobre que una confianza.

Una mirada criminológica: cuando el delincuente adapta su método

Desde Forentia 360, analizamos este caso no solo como un incidente de ciberseguridad, sino como un fenómeno que la criminología explica con precisión. El fraude híbrido que acabamos de describir encaja con varios marcos teóricos que los profesionales de la seguridad y del derecho deberían conocer, no por erudición académica, sino porque estas teorías nos ayudan a anticipar el comportamiento delictivo y a diseñar mejores medidas de prevención.

La *Teoría de las Actividades Rutinarias* (Cohen y Felson, 1979) establece que el delito ocurre cuando confluyen tres elementos: un delincuente motivado, una víctima u objetivo adecuado y la ausencia de guardianes capaces. En este caso, los tres factores se materializan con llamativa claridad. El objetivo era adecuado porque los datos filtrados de Ledger identificaron con exactitud quién poseía activos valiosos. La ausencia de guardianes se produjo porque el canal postal no estaba bajo ningún sistema de alerta o filtrado, a diferencia del correo electrónico. Y la motivación del delincuente estaba sobradamente garantizada por el valor económico potencial del activo a robar: una cartera de criptomonedas cuya llave de recuperación, una vez obtenida, permite el vaciado instantáneo e irreversible de los fondos.

Igualmente, relevante es la *Teoría de la Elección Racional* (Clarke y Cornish, 1985), que nos recuerda que el delincuente no actúa por impulso ciego, sino que evalúa costes y beneficios antes de ejecutar su acción. La elección del correo postal como vector de ataque es, en este marco, una decisión racional: los sistemas de alerta colectiva se han entrenado para detectar amenazas digitales, por lo que cambiar al entorno físico reduce de manera significativa el riesgo de detección y la probabilidad de que la víctima active sus mecanismos de defensa aprendidos. El delincuente elige el medio que maximiza sus posibilidades de éxito, no el que más le resulta cómodo.

Por último, la *Teoría de la Prevención Situacional* (Clarke, 1980) nos ofrece la hoja de ruta más práctica para la respuesta: si queremos reducir la oportunidad delictiva, debemos aumentar el esfuerzo percibido por el atacante, incrementar el riesgo de ser detectado y reducir las recompensas esperadas. En términos concretos, esto se traduce en educación del ciudadano para que reconozca

indicios documentoscópicos básicos, en protocolos de verificación que no dependan exclusivamente del canal recibido y en una mayor exigencia regulatoria a las empresas sobre la custodia de datos personales, porque sin esos datos, el ataque personalizado y convincente es imposible.

Documentoscopia aplicada: leer el sobre antes de abrir la carta

La documentoscopia forense es la disciplina que estudia la autenticidad de documentos mediante el análisis de sus elementos físicos y gráficos: el soporte material, los sistemas de impresión, las tintas, los sellos, los matasellos y la coherencia entre todos esos elementos. Habitualmente asociada a la investigación de falsificaciones de pasaportes, billetes o contratos, su aplicación en este caso resulta reveladora y, sobre todo, preventiva.

En el caso analizado, el continente del mensaje, es decir, **el sobre físico, contenía más información relevante que el propio contenido de la carta**. Los indicadores documentoscópicos que activaron la alerta fueron los siguientes: en primer lugar, la incoherencia geográfica entre el origen declarado de la empresa, con sede social en París, y el matasellos de Madrid, que revelaba que la carta había sido franqueada y depositada localmente en España. En segundo lugar, el tipo de franqueo: los envíos postales de empresas con volumen comercial se realizan de manera habitual mediante franqueo mecánico impreso directamente sobre el sobre, no mediante sello físico adhesivo matasellado a mano, que es más propio de envíos particulares o de pequeñas tiradas. Este detalle, aparentemente menor, es un indicador de baja industrialización del envío, incompatible con una campaña corporativa legítima de alcance internacional.

Estas son las preguntas que un ciudadano informado, o un profesional que ha recibido formación básica en verificación documental, debería hacerse antes de interactuar con cualquier comunicación postal que solicite una acción urgente: ¿el matasellos es coherente con el país de origen declarado del remitente? ¿El tipo de franqueo es compatible con el perfil de una empresa del tamaño indicado? ¿El sobre tiene indicaciones de envío certificado o acuse de recibo, habituales en comunicaciones corporativas relevantes? ¿Existe algún número de referencia o localizador que permita verificar el envío de manera independiente? La ausencia

o la incoherencia en cualquiera de estos elementos no confirma el fraude, pero sí justifica una pausa y una verificación adicional antes de escanear cualquier código o visitar cualquier enlace.

Vida híbrida, amenaza híbrida: la extensión de la guerra híbrida al ciudadano

En el ámbito geopolítico y de seguridad nacional, la guerra híbrida describe el uso combinado de medios convencionales y no convencionales, de acciones visibles e invisibles, para desestabilizar a un adversario sin cruzar los umbrales formales del conflicto. La combinación de desinformación, ciberataques, operaciones de influencia y acciones en el mundo físico ha dejado de ser exclusiva de los estados y ha permeado hacia el crimen organizado y el fraude a gran escala.

Vivimos una vida híbrida. Compramos en tiendas físicas y en plataformas digitales. Recibimos facturas en papel y en el correo electrónico. Firmamos contratos de forma presencial y mediante firma electrónica. Esa hibridación de nuestra vida cotidiana es, al mismo tiempo, una hibridación de nuestra superficie de exposición al riesgo. Los delincuentes lo saben y lo explotan. Si las defensas del ciudadano se han especializado en el entorno digital, el atacante racional migrará, total o parcialmente, al entorno físico. Y viceversa: cuando las defensas se refuercen en el plano físico, el vector volverá a desplazarse. La amenaza no tiene canal favorito; tiene el canal que en cada momento presenta menor resistencia.

Este caso ilustra además un patrón de escalada que merece atención. Cuando los programas de concienciación en ciberseguridad empezaron a dar frutos, los delincuentes no desaparecieron: migraron hacia el SMS, luego hacia el WhatsApp, y ahora hacia el correo postal. La amenaza no tiene canal favorito; tiene el canal que en cada momento presenta menor resistencia. Por eso la prevención no puede limitarse a alertar sobre amenazas concretas: debe aspirar a formar un criterio crítico transversal, capaz de aplicarse a cualquier soporte, en cualquier momento.

Recomendaciones de prevención: el protocolo ante cualquier comunicación que exija acción

Lo que sigue no es un decálogo de buenas prácticas ni una lista de verificación técnica. Es un protocolo de sentido común aplicado al mundo híbrido en que vivimos: el conjunto de preguntas que cualquier ciudadano, profesional del derecho o responsable de seguridad debería hacerse antes de interactuar con cualquier comunicación —postal o digital— que exija una acción con consecuencias irreversibles.

Ante cualquier comunicación postal que solicite una acción con consecuencias en el entorno digital, lo primero es examinar el continente antes que el contenido: analizar el matasellos, el tipo de franqueo y la coherencia entre el remitente declarado y el origen geográfico del envío. Si el matasellos no corresponde al país donde la empresa dice tener su sede, ese solo elemento justifica una pausa.

Nunca se debe verificar una comunicación usando los medios de contacto que la propia comunicación proporciona, ya sean el código QR, el número de teléfono o la URL impresos en la carta. Siempre hay que ir directamente al sitio web oficial de la empresa, accediendo desde el navegador de forma manual, o contactar con su servicio de atención al cliente a través de los canales publicados en fuentes independientes. Las empresas serias, y Ledger lo reitera explícitamente en su página de alertas, nunca solicitan la frase de recuperación de veinticuatro palabras bajo ningún concepto.

Desde el punto de vista de la responsabilidad empresarial, las organizaciones que gestionan datos personales de sus clientes deben asumir que una filtración no solo genera un daño reputacional inmediato, sino que convierte esos datos en munición utilizable durante años. En este sentido, el Reglamento General de Protección de Datos no solo establece obligaciones reactivas ante una brecha, sino que exige una gestión proactiva del riesgo desde el diseño. Las empresas que custodian datos asociados a activos de alto valor, como ocurre en el sector de las criptomonedas, tienen una responsabilidad especialmente cualificada, y sus clientes, el derecho de exigirla.

Quien ya ha recibido una comunicación de este tipo tiene una última responsabilidad que no debería subestimar: documentar y denunciar. Conservar

el sobre, la carta y el código QR como evidencia y presentar denuncia ante las Fuerzas y Cuerpos de Seguridad del Estado no es un trámite burocrático sin consecuencias. La denuncia sistemática permite a los analistas trazar patrones de actividad delictiva, identificar redes operativas y, en el mejor de los casos, contribuir al desmantelamiento de la organización responsable. El silencio de la víctima no es discreción: es el aliado más valioso del estafador.

Conclusión: prevenir en todos los planos

La criminología no es una disciplina que observa el delito desde la distancia académica. Es, en su mejor expresión aplicada, una herramienta de anticipación. Cuando analizamos este caso desde Forentia360, no lo hacemos solo para describirlo, sino para extraer las claves que permitan a ciudadanos, empresas y profesionales del ámbito legal y de la seguridad actuar antes de que el daño se produzca.

El buzón de casa es, desde hoy, una extensión más de la bandeja de entrada. El matasellos de Madrid en una carta francesa es la bandera roja que no aparece en ningún antivirus. La documentoscopia, ciencia de la autenticidad, ha pasado de los laboratorios forenses a la puerta de nuestro domicilio. Y la criminología nos recuerda que el delincuente no tiene fidelidad al canal: tiene fidelidad al resultado. Frente a esa adaptabilidad, solo cabe una respuesta equivalente: una conciencia de seguridad igualmente adaptable, igualmente híbrida, igualmente alerta en todos los planos de nuestra vida. Porque la lección más incómoda de este caso no la da el sobre falso ni el QR fraudulento: la da el hecho de que **ninguna empresa puede ser el garante último de tu seguridad**. Esa responsabilidad, en el fondo, siempre ha sido tuya.

Reflexión final

Hay una dimensión de este caso que merece ser nombrada con precisión. Lo que ha permitido analizar este fraude en todos sus planos —el digital, el físico, el jurídico, el conductual— no es la suma de varias especialidades trabajando en paralelo, sino la **visión integradora que aporta la criminología**. Es precisamente esa capacidad de localizar nexos entre el mundo virtual y el mundo tangible, entre la brecha de datos y el sello de correos, entre la teoría del delito y el matasellos de Madrid, lo que convierte a la criminología aplicada en una

disciplina pericial de primer orden. Un peritaje criminológico no se limita a describir lo ocurrido: identifica el patrón, selecciona los medios y recursos de análisis adecuados a la naturaleza concreta del caso, y traduce esa lectura en criterios útiles para la prevención, la investigación y, cuando es necesario, la acción legal. En un entorno donde las amenazas ya no respetan la frontera entre lo físico y lo digital, las pericias que sigan ancladas en un solo plano serán, por definición, pericias incompletas.

Trazabilidad documental del caso. Fuentes y documentación de referencia:

Filtración de datos de clientes — julio 2020 Comunicado oficial del CEO de Ledger https://www.ledger.com/message-ledgers-ceo-data-leak

Campañas de suplantación de identidad en curso
https://www.ledger.com/es/phishing-campaigns-status

Incidente de Global-e en datos de pedidos — enero 2026
https://support.ledger.com/es/article/Global-e-Incident-to-Order-Data---January-2026