CiberConscientes
Creando nidos seguros en redes inseguras

PLAYBOOKS

Fraude del CEO: el pedido de transferencia que no era

Un mail del dueño pidiendo una transferencia urgente. Un proveedor de siempre que avisa que cambió el CBU. Son los dos fraudes que más plata le cuestan a las empresas argentinas, y ninguno usa un virus: usan la confianza y el apuro. Este playbook te da el control que los frena, qué hacer en las primeras horas si ya pasó, y cómo instalarlo en el equipo sin volverse insoportable.

Versión 1.1 · Agosto 2026

> ¿Ya pasó?
> Si la transferencia ya salió, andá directo a la sección 5. Las primeras horas son las únicas en las que a veces se puede frenar el dinero.

1. Qué es y por qué funciona

El fraude del CEO —también llamado compromiso de correo corporativo— consiste en hacerse pasar por una figura de autoridad o por un proveedor conocido para conseguir que alguien del área de administración haga un pago o cambie un dato bancario.

No hay malware, no hay hackeo espectacular. Hay una persona apurada que hace lo que le pidió su jefe. Por eso los controles técnicos no alcanzan: lo que falla es el proceso.

Variante	Cómo llega	Qué pide
El jefe apurado	Mail con el nombre del dueño y una dirección parecida, o WhatsApp desde un número nuevo.	Una transferencia urgente y confidencial, «estoy en una reunión, después te explico».
El cambio de CBU	Respuesta dentro de una cadena de mails real con un proveedor.	Que pagues la factura de siempre a una cuenta nueva.
La factura falsa	Adjunto que imita el formato del proveedor habitual.	El pago de un servicio que parece legítimo.
El estudio jurídico	Llamada o mail sobre una operación confidencial en curso.	Discreción absoluta y un pago rápido para «no frenar el negocio».

> La señal que nunca falla
> El pedido de confidencialidad es la señal más fuerte de todas. Ninguna operación legítima necesita que la persona que paga no consulte con nadie. Ese requisito existe solo para evitar la verificación.

2. Señales de alerta

- Urgencia desmedida. El plazo siempre es hoy, ahora, antes del cierre bancario.
- Pedido de silencio. «No lo comentes con nadie», «es confidencial», «después le explico a contabilidad».
- El canal cambió. Alguien que siempre escribió por mail ahora escribe por WhatsApp desde un número nuevo, o al revés.
- La dirección de correo es casi igual. Una letra cambiada, un dominio con «.com.ar» en vez de «.com», una «rn» que parece una «m».
- Cambio de datos bancarios en una relación que ya venía funcionando. Casi nunca es legítimo por mail.
- Apelación a la jerarquía. «Confío en vos», «te lo pido a vos porque sos de confianza», o directamente presión.
- Cuenta a nombre de otra persona o en un banco distinto al habitual del proveedor.
- Errores de estilo. Un tono más formal o más neutro del que usa esa persona normalmente.

3. El control que lo frena: verificación por segundo canal

Es un solo control y no cuesta plata. Todo lo demás es complemento.

REGLA DE ORO — sin excepciones, para todos

1. Ninguna transferencia nueva ni cambio de CBU se ejecuta con la sola confirmación del canal por el que llegó el pedido. Si llegó por mail, se verifica por teléfono. Si llegó por WhatsApp, se verifica por teléfono a un número que ya teníamos.
2. El número se busca en la agenda propia, nunca en el mensaje. El teléfono que figura en el correo sospechoso lo puso el atacante.
3. No se responde el mail para verificar. Si la casilla está comprometida, responde el atacante.
4. Quien recibe el pedido tiene autoridad explícita para frenarlo. Esto se le dice al equipo en voz alta: «si dudás, frená, aunque el mail parezca mío. No te vas a meter en problemas por verificar».

Controles complementarios, por orden de costo-beneficio:

- Doble firma para montos altos. Definí un umbral ([MONTO]) por encima del cual hacen falta dos personas. Es el control más barato de todos.
- Alta de proveedores con circuito propio. El CBU se carga una vez, verificado, y modificarlo requiere el mismo circuito que darlo de alta.
- Segundo factor en el correo y en el homebanking. Corta el acceso a la casilla, que es de donde salen las variantes más creíbles.
- Marcado de correos externos. Que el sistema agregue un aviso visible a los mails que vienen de afuera. Delata al que se hace pasar por interno.
- Registro de configuración SPF, DKIM y DMARC en tu dominio, para que sea más difícil falsificar tu propia dirección.

4. Cómo instalarlo en el equipo

Un control que la gente esquiva porque molesta no es un control. Tres cosas que hacen la diferencia:

- ☐ Que el dueño lo diga primero. La persona que podría ser suplantada tiene que anunciar la regla: «si te llega un pedido mío de plata, llamame antes, siempre». Sin eso, verificar se siente como desconfiar del jefe.

- [ ] Ponelo por escrito en una hoja. Quién puede autorizar pagos, hasta qué monto, y cómo se verifica. Pegada donde se hacen los pagos.
- [ ] Practicá el caso raro. Preguntale al equipo en una reunión: «si llega un mail mío un viernes a las seis pidiendo una transferencia urgente, ¿qué hacés?». La respuesta correcta se aprende en frío.
- [ ] Avisá a tus proveedores y clientes que vos tampoco vas a cambiar tu CBU por mail. Es un ataque que va en las dos direcciones.
- [ ] Cuando alguien frene un pago legítimo por verificar, felicitalo en público. Es la señal más barata y más efectiva que podés dar.

5. Ya se transfirió: las primeras horas

El dinero se mueve rápido y se fracciona. Todo lo que sigue hay que hacerlo el mismo día, en paralelo si hay más de una persona.

PRIMERAS HORAS — actuá en este orden

1. Llamá a tu banco de inmediato. Pedí que informen la operación como fraudulenta y que gestionen el retorno de fondos con el banco destinatario. Cuanto antes, más chances: si el dinero todavía no se movió de la cuenta receptora, a veces se retiene.
2. Pedí todo por escrito. Que quede constancia de la fecha y hora del reclamo y del número de gestión. Es la base de cualquier reclamo posterior.
3. Preservá la evidencia. No borres ni respondas los mensajes. Guardá los correos completos con sus encabezados, las capturas de WhatsApp y el comprobante de la transferencia.
4. Verificá si hubo acceso a la casilla. Revisá reglas de reenvío automático creadas sin autorización, sesiones abiertas y dispositivos desconocidos. Cambiá contraseñas y activá el segundo factor.
5. Hacé la denuncia penal. Es un delito. El primer paso es la denuncia en la comisaría, fiscalía u oficina receptora que corresponda a tu domicilio: están obligadas a tomártela. Podés ubicar la más cercana en el mapa de fiscalías del Ministerio Público Fiscal.
6. Además, reportá el caso a la UFECI. Ver el recuadro de abajo: es un canal complementario, no un reemplazo de la denuncia.
7. Avisá al proveedor real si el fraude usó su identidad: puede que su casilla esté comprometida y vos no seas el único afectado.
8. Revisá si tenés cobertura. Algunas pólizas de ciberseguro o de seguro comercial cubren el fraude por suplantación. Consultá a tu productor.

Cómo se hace el trámite con la UFECI

La UFECI es la Unidad Fiscal Especializada en Ciberdelincuencia del Ministerio Público Fiscal. Recibe denuncias y realiza investigaciones preliminares, y asiste a las fiscalías que intervienen en el caso. No reemplaza la denuncia inicial: la complementa.

Se le escribe a denunciasufeci@mpf.gov.ar (con «gov», no «gob»). Está en Sarmiento 663, piso 6, CABA, y atiende al (011) 5071-0040.

Mandá el mismo material que preservaste en el paso 3, indicando qué denuncia ya hiciste y dónde. Una vez presentada la denuncia, seguí las indicaciones del investigador para el resguardo de la prueba: manipularla por tu cuenta puede complicar la causa.

Si el hecho ocurrió en la Ciudad de Buenos Aires, existe además la unidad especializada del Ministerio Público Fiscal porteño, que atiende al 0800-33-347225 las 24 horas.

Dimensión legal

Si en el fraude se comprometieron datos personales de clientes o empleados, evaluá si corresponde dar aviso a la AAIP, autoridad de aplicación de la Ley 25.326. Consultá el criterio vigente y, si el monto es relevante, buscá asesoramiento legal antes de comunicar hacia afuera.

6. Después: cerrar la puerta

- Reconstruí cómo entró. ¿Casilla comprometida, dominio parecido, número nuevo de WhatsApp? La respuesta define qué control falta.
- No busques al culpable, buscá el control que faltaba. Si el equipo aprende que reportar termina en sanción, el próximo fraude se va a esconder.
- Escribí el procedimiento de pagos si todavía no existía, y hacelo firmar.
- Repetí el mensaje cada tanto. Estos ataques vuelven, sobre todo cerca de fin de año, en vacaciones y cuando hay gente nueva en administración.

7. Verificar no es desconfiar

El fraude del CEO no se frena con tecnología, se frena con una llamada de treinta segundos. Lo único que hace falta es que en tu empresa esa llamada sea obligatoria y que nadie se sienta mal por hacerla.

Esto no termina acá

Si querés enterarte de las estafas que están circulando de verdad, qué revisar y los documentos nuevos, sumate al correo de CiberConscientes. Sin vueltas y con baja en un clic. www.ciberconscientes.io

Material orientativo elaborado por CiberConscientes con fines educativos. No reemplaza el asesoramiento legal, contable ni profesional para tu caso particular. Los procedimientos de reclamo bancario, los organismos de denuncia y la normativa aplicable pueden cambiar: verificá las fuentes oficiales vigentes y consultá con tu banco y con un asesor legal ante un caso real.

Versión 1.1 · Agosto 2026 · Próxima revisión: Febrero 2027 · www.ciberconscientes.io