Fraude por correo corporativo (BEC)

Versión 1.0 · Revisado el 11 oct 2026 · TLP:CLEAR · Para: Finanzas, tesorería, gerencia y responsables de TI.

Qué hacer cuando alguien se hace pasar por un directivo o un proveedor para desviar un pago, o cuando una cuenta de correo real se usa para ese fin. Las primeras horas deciden si el dinero se recupera.

Señales de que está ocurriendo

- Solicitud urgente y confidencial de transferencia por parte de un directivo.
- Proveedor que avisa por correo que cambió su cuenta bancaria.
- Factura legítima con los datos de pago modificados.
- Respuestas que llegan a una dirección distinta de la del remitente.
- Proveedor que reclama un pago que la organización ya realizó.

Qué tan grave es

Crítica	La transferencia ya se realizó.
Alta	Una cuenta de correo interna fue comprometida, aunque no se haya pagado.
Media	Intento detectado antes del pago, desde un dominio externo.

Primera hora

- [ ] **1.** Si ya se transfirió, llama al banco de inmediato y pide detener o revertir la operación.
- [ ] **2.** Pide por escrito al banco que contacte al banco receptor para congelar los fondos.
- [ ] **3.** Suspende todos los pagos pendientes a esa cuenta y a ese proveedor.
- [ ] **4.** Confirma por teléfono, a un número ya conocido, con el directivo o proveedor real.
- [ ] **5.** Conserva todos los correos de la conversación sin modificarlos.
- [ ] **6.** Si se sospecha de un buzón interno, cambia su contraseña y cierra sus sesiones.

Preparación (antes del incidente)

- Exige verificación por un segundo canal para todo cambio de cuenta bancaria.
- Requiere doble aprobación para transferencias arriba de un monto definido.
- Activa verificación en dos pasos en el correo de finanzas y gerencia.
- Marca automáticamente los correos que vienen de fuera de la organización.

Detección y análisis

- Determina si el correo salió de una cuenta real comprometida o de un dominio parecido.
- Revisa en el buzón reglas de reenvío, de borrado y accesos desde ubicaciones inusuales.
- Reconstruye la línea de tiempo: primer contacto, solicitud, pago.
- Identifica qué otra información vio el atacante en el buzón.

Contención

- Bloquea el dominio suplantador en el correo.
- Revoca sesiones y elimina reglas maliciosas del buzón comprometido.
- Avisa a los proveedores y clientes cuyos hilos de correo fueron intervenidos.

Erradicación

- Solicita la baja del dominio parecido al registrador.
- Revisa las demás cuentas de finanzas y gerencia en busca de las mismas reglas.
- Elimina aplicaciones de terceros con acceso al buzón que nadie reconozca.

Recuperación

- Da seguimiento diario con el banco sobre la recuperación de los fondos.
- Valida de nuevo los datos bancarios de todos los proveedores activos.
- Restablece los pagos sólo con el proceso de verificación reforzado.

Lecciones aprendidas

- Identifica qué control faltó: verificación, doble firma o protección del correo.
- Actualiza el procedimiento de pagos y capacita a finanzas con este caso.
- Evalúa un seguro que cubra fraude por transferencia.

Evidencia que debes conservar

- Todos los correos de la conversación, con cabeceras.
- Comprobante de la transferencia y datos de la cuenta destino.
- Registros de acceso del buzón involucrado.
- Constancia de las gestiones realizadas con el banco.

Qué no hacer

- Esperar al día siguiente para llamar al banco: cada hora reduce la posibilidad de recuperar el dinero.
- Confirmar el cambio de cuenta respondiendo al mismo correo.
- Borrar los correos del fraude para “limpiar” el buzón.
- Tratarlo sólo como un asunto contable: suele haber una cuenta comprometida detrás.

A quién avisar

- El banco propio y, a través de él, el banco receptor.
- Gerencia general y asesoría legal.
- Ministerio Público, mediante denuncia con comprobantes y correos.
- El proveedor o cliente suplantado.
- cert.gt, con el dominio y la cuenta usados, para alertar a otros.

Cuándo dar por cerrado el incidente

- El banco confirmó el resultado de la gestión de recuperación.
- La denuncia fue presentada.
- Ningún buzón conserva reglas o accesos del atacante.
- El nuevo control de verificación de pagos está en operación.

cert.gt es una iniciativa privada y comunitaria de Devel Group.

cert.gt · devel.group · Reporta un incidente en cert.gt/reportar o a incidentes@cert.gt

Guía general de buenas prácticas; no sustituye asesoría legal ni técnica especializada para tu caso. No es un documento de una entidad gubernamental. Puedes copiarla y adaptarla citando la fuente (CC BY 4.0).