

Seguridad de correo: del engaño a la decisión

El correo es el comienzo. El impacto puede ir más lejos.

Proteger el correo empresarial exige entender qué intenta conseguir un atacante, qué decisiones puede manipular y qué acceso puede obtener. Este ensayo propone un recorrido para conectar esas preguntas con las consecuencias del negocio y con criterios útiles de evaluación.

1. El problema: decisiones y accesos

Un mensaje fraudulento puede buscar que alguien transfiera dinero, entregue documentación o cambie una instrucción. El daño puede consumarse sin instalar malware: basta con que una petición convincente produzca una acción favorable al atacante. El fraude por correo empresarial, conocido como BEC, pertenece a este campo de engaño y manipulación de decisiones.

Otra ruta consiste en obtener una posición dentro de la organización. El robo de credenciales o de una sesión puede permitir utilizar una cuenta ajena; un adjunto malicioso puede facilitar una infección. Las acciones posteriores dependen de los accesos disponibles y de las demás barreras. El movimiento lateral y el ransomware son posibles desenlaces, no consecuencias inevitables de cada mensaje.

Las dos rutas pueden combinarse. Una cuenta comprometida permite revisar conversaciones y enviar solicitudes desde una identidad que sus destinatarios ya conocen. Por eso conviene distinguir entre confiar en el remitente y comprobar que una petición es legítima.

2. Cómo ocurre: el contexto hace creíble el engaño

La suplantación intenta aparentar una identidad. La toma de cuentas utiliza un acceso real de forma indebida. El engaño dentro de una conversación aprovecha su continuidad y contexto. Aunque puedan producir mensajes parecidos, investigar cada mecanismo exige evidencias distintas.

Un estudio publicado en USENIX Security analizó 113 millones de correos enviados por empleados de 92 organizaciones y documentó phishing desde cuentas empresariales comprometidas [1]. El trabajo ayuda a comprender el mecanismo; no establece su prevalencia actual ni compara la eficacia de las soluciones que hoy se comercializan.

La pregunta operativa es concreta: ¿qué sucede cuando la apariencia de una conversación normal deja de ser suficiente para decidir con seguridad?

3. Consecuencias: más allá del buzón

El perjuicio puede afectar dinero, información, continuidad y tiempo de trabajo. Investigar lo ocurrido, contener accesos, reconstruir sistemas y restablecer relaciones también consume recursos, incluso cuando no existe una transferencia fraudulenta.

Dinero y decisiones de negocio

El IC3 registró en 2025 pérdidas reportadas por BEC superiores a US\$3,046 millones [2]. La cifra corresponde a denuncias recibidas por el organismo: no es un censo mundial, una estimación específica de México ni una predicción de cuánto perderá una empresa.

Ubiquiti informó ante la SEC que la suplantación de empleados y solicitudes fraudulentas dirigidas a finanzas provocaron transferencias por US\$46.7 millones en 2015 [3]. Hubo recuperaciones posteriores; el monto transferido no equivale a la pérdida final irrecuperable. El caso muestra por qué la verificación de instrucciones de pago importa además del análisis técnico del mensaje.

Información y confianza

Un buzón puede contener documentos, acuerdos y relaciones comerciales. El acceso indebido también puede permitir observar quién autoriza, qué lenguaje utiliza y cuándo espera una respuesta. La información obtenida puede hacer más creíble un engaño posterior. La confianza asociada a la cuenta se convierte entonces en parte del problema.

Continuidad e investigación

El servicio de salud irlandés, HSE, explica que un adjunto de phishing abrió acceso a su red en marzo de 2021; el ransomware se activó en mayo [4]. El caso ilustra una cadena de ataque con consecuencias operativas, no demuestra que cualquier correo de phishing produzca ese desenlace.

Un estudio sobre la experiencia irlandesa documentó la interrupción de radioterapia de 513 pacientes en cinco centros públicos [5]. Los autores no determinaron los efectos oncológicos y psicológicos finales. Esa distinción permite comunicar la gravedad del incidente sin atribuirle daños clínicos que el estudio no probó.

Estos datos no deben convertirse en una suma de pérdidas potenciales para un prospecto. Su valor es hacer visibles procesos que necesitan protección: pagos, intercambio de información, accesos y continuidad de servicios. Para priorizar inversiones hay que relacionarlos con el contexto real de la organización.

4. Las defensas existentes

Las protecciones nativas del correo, filtros y gateways aportan controles sobre mensajes, enlaces, adjuntos y otras señales. Su cobertura depende del producto, la licencia, la configuración y su operación. Hablar de una categoría completa como si todas sus implementaciones fueran iguales impide evaluar con precisión.

La autenticación del correo ayuda a verificar aspectos del dominio remitente. Los controles de identidad protegen accesos y sesiones. La capacitación enseña a reconocer situaciones y reportarlas. Los procedimientos de negocio añaden comprobaciones antes de pagar o compartir información. Cada capa responde a una pregunta distinta; ninguna justifica abandonar las demás.

Ante un cambio de cuenta bancaria, por ejemplo, la empresa puede necesitar una verificación por un canal conocido, además de inspeccionar el correo. Frente a una cuenta comprometida, también importa quién puede revocar accesos y cómo continúa la respuesta. La protección del correo convive con equipos, redes, respaldos y recuperación [6].

5. Resultados y límites: medir lo que importa

Una capacitación completada demuestra participación, pero no basta para concluir que las personas actuarán mejor ante cualquier engaño. Un estudio del NIST describe la importancia del contexto del usuario para entender la susceptibilidad al phishing [7]. Su alcance es concreto; no debe extrapolarse a todos los empleados o industrias.

La formación merece una evaluación propia: pertinencia de escenarios, claridad de las instrucciones y capacidad de verificar y reportar. Una reducción de clics puede ser engañosa si las simulaciones posteriores son más fáciles. La comparación necesita considerar el periodo, la dificultad y la población participante.

Las detecciones también requieren interpretación. Una anomalía no prueba por sí sola una intrusión. Un mensaje identificado no equivale automáticamente a dinero ahorrado. Cuando varias herramientas coexisten, sus registros y tiempos deben contrastarse antes de atribuir un fallo a una de ellas.

La automatización puede simplificar tareas, pero su utilidad depende de la calidad de las decisiones y del trabajo que permanece. Por eso conviene observar falsos positivos, escalaciones, intervención humana y efectos sobre el correo legítimo. La ausencia de incidentes durante una prueba corta tampoco demuestra ausencia de riesgo.

5. RESULTADOS Y LÍMITES / UNA PREGUNTA CENTRAL

¿Por qué siguen pasando ataques si ya tienes protección?

La presencia de herramientas no equivale a cobertura completa. La respuesta está en cómo se combina el engaño con los accesos, qué señales observa cada control y cómo actúa la organización cuando algo se aparta de lo esperado.

Un riesgo persistente, amplificado por la IA

El NCSC británico evalúa que la IA mejora técnicas existentes, incluida la ingeniería social, y prevé que aumente el volumen e impacto de las intrusiones hasta 2027 [8]. Es una evaluación de amenaza; no una medición de cuántos correos fraudulentos fueron generados con IA.

Las 24,768 denuncias BEC recibidas por el IC3 en 2025 [2] muestran que el problema persiste. No permiten atribuir todos esos casos a IA ni identificar las herramientas instaladas en cada víctima. La IA amplifica un riesgo anterior; el fraude por correo nunca estuvo definitivamente superado.

El engaño puede superar una comprobación aislada

Una solicitud fraudulenta puede carecer de archivo malicioso. Una cuenta comprometida puede conservar una identidad auténtica. Una conversación conocida puede incluir una instrucción que favorezca al atacante. Ninguno de esos elementos, aislado, permite concluir que una solicitud es legítima.

Las reglas y firmas ayudan a reconocer patrones definidos, pero por sí solas pueden dejar fuera variaciones nuevas o engaños vinculados al contexto. Las soluciones actuales combinan técnicas diferentes: no es correcto reducirlas todas a reglas ni afirmar que un solo fabricante puede detener cualquier ataque. También influyen la configuración, los permisos y los procedimientos del negocio.

La propuesta de Dimensions

Proponemos evaluar Abnormal AI por su análisis de identidad, comportamiento y contenido dentro del entorno de la organización [9]. El objetivo es comprobar qué aporta ante esas dificultades y cómo puede complementar los controles existentes o cubrir una sustitución definida. Su enfoque conductual es el argumento técnico; los resultados de una evaluación deben sostener la decisión comercial.

Una mejor pregunta que «¿tenemos una herramienta?» es «¿qué engaños y usos indebidos podemos reconocer, qué respuesta ejecutamos y qué evidencia tenemos de ello?».

6. Criterios para una mejor defensa

Una evaluación útil comienza con las preguntas del cliente y termina con una decisión explicable. Debe considerar el contexto de los mensajes, el uso indebido de cuentas, la investigación, la respuesta, la formación y el impacto sobre el trabajo legítimo.

Acordar: escenarios prioritarios, alcance, permisos, datos, participantes y criterios de aceptación.

Observar: casos confirmados, errores, tiempos y esfuerzo. **Concluir:** valor demostrado, límites y preguntas pendientes. Una prueba en observación estudia detecciones; comprobar remediación exige que las acciones estén habilitadas y autorizadas.

Dimensions es partner comercial de Abnormal AI. Esta relación es explícita: proponemos evaluar sus capacidades frente a las necesidades del cliente, como complemento o dentro de una sustitución de alcance definido. El resultado debe sustentar la recomendación. La investigación sobre el problema no constituye por sí misma una prueba de superioridad universal de un fabricante.

La tecnología elegida debe ayudar a proteger decisiones y accesos, mientras las personas reciben apoyo para verificar y reportar. Ese es el vínculo entre seguridad de correo y responsabilidad de negocio: comprender qué puede ocurrir, comprobar qué aportan los controles y decidir qué mejora tiene sentido.

Fuentes y alcance

1. Ho et al. (2019), USENIX Security: phishing lateral en organizaciones.
2. FBI / IC3, Internet Crime Report 2025, pérdidas reportadas por BEC.
3. Ubiquiti, Form 10-Q, septiembre de 2015, nota 14.
4. HSE: explicación institucional de lo ocurrido en el ciberataque.
5. Flavin et al. (2022), The Irish Experience, Advances in Radiation Oncology.
6. CISA: guía de prevención y respuesta frente a ransomware.
7. NIST / Greene et al. (2018): contexto y susceptibilidad al phishing.
8. NCSC (2025): impacto de la IA en la amenaza cibernética hasta 2027.
9. Abnormal AI: Inbound Email Security, documentación del fabricante.

Edición: Dimensions. Síntesis de investigación para orientar una conversación de negocio. Los casos y estudios conservan sus fechas y límites; no predicen el riesgo individual de una organización.