PHISHING · FRAUDE BANCARIO EMPRESARIAL

EL EMPLEADO ESCRIBIÓ LA DIRECCIÓN CORRECTA Y AUN ASÍ CAYÓ.

EL PHISHING MODERNO SE DISFRAZA DE LA PÁGINA CORRECTA EN LA DIRECCIÓN CORRECTA

> **EL USUARIO VEÍA LA DIRECCIÓN CORRECTA; LA MÁQUINA SABÍA QUE EL SITIO ERA FALSO.**

Copia forense con millones de registros clasificados: primero se descarta lo interno, con método.

EL PROBLEMA

Una empresa sufrió transferencias no reconocidas de su cuenta corporativa, y la pregunta del encargo decidía su futuro interno: ¿fue un empleado con conducta indebida o una brecha de seguridad externa?

El análisis del equipo usado para la banca en línea respondió con una cronología que vale como manual del phishing moderno: la víctima no hizo nada mal a simple vista. Escribió la dirección correcta del banco. Y aun así cayó.

LA INTERVENCIÓN

Primero se descartó lo interno con método: la copia forense del disco clasificó millones de registros — programas de uso corporativo normal, antivirus activo, sin indicativos de mal uso. Los únicos eventos de nota: modificaciones administrativas en el firewall del equipo y actividad de la consola de administración, poco antes del fraude — indicativos de intervención con alto nivel de acceso.

Después, la escena del fraude reconstruida con los rastros del navegador: el usuario buscó la página del banco y escribió su dirección —lo que descarta el enlace llegado por correo— y veía en la barra la dirección oficial, letra por letra. Sin embargo, al ingresar, el navegador identificó que la página no era la oficial: una página fraudulenta disfrazada de la oficial, servida en la misma dirección visual, capturando las credenciales de quien entraba confiado.

El veredicto quedó ordenado: sin compromiso interno, con intervención de alto nivel y con la trampa documentada, las transferencias fueron resultado de un ataque de phishing externo. No fue un empleado: fue un sitio falso con la cara del banco.

Caso anonimizado para proteger la identidad de las partes. Los detalles técnicos se describen a nivel general.

ESCRIBIR BIEN LA DIRECCIÓN YA NO BASTA.

EL AVISO DEL NAVEGADOR ES EL ÚLTIMO SEMÁFORO ANTES DE ENTREGAR LAS LLAVES

QUÉ SE LOGRÓ

Gracias al análisis forense se probó en la investigación interna que no hubo conducta indebida del empleado: las transferencias no autorizadas fueron el resultado de un ataque externo documentado con cronología, y la empresa evitó destruir a una persona honorable y perder un juicio laboral por señalar la puerta equivocada.

> **La lección para toda empresa: antes de señalar a un empleado, analice su equipo. Y para todos: los sitios falsos modernos se disfrazan de la página correcta en la dirección correcta — lea el aviso del navegador como lo que es, la última alarma.**

POR QUÉ DURIVA ES LA MEJOR OPCIÓN

≡

EFICIENCIA

Metodología propia probada en miles de dictámenes, con equipos que trabajan en paralelo sobre la evidencia.

TIEMPO

Respuesta ágil en escenarios de urgencia procesal, con la misma calidad técnica y documentación completa.

18

TRAYECTORIA

Más de 18 años de cómputo forense en México y América Latina. Creador del primer sistema operativo forense latinoamericano, presidente del Consejo Americano de Ciberseguridad y Cómputo Forense, autor de seis libros especializados.

Si su empresa cayó en un sitio falso, la evidencia decide quién fue: el empleado o la trampa. Somos su aliado digital.

Caso anonimizado para proteger la identidad de las partes. Los detalles técnicos se describen a nivel general.