INFORMATION SECURITY

NEWS AND INFORMATION TO HELP PROTECT CUSTOMERS AND EMPLOYEES

CONCIENTIZACIÓN: PREVENCIÓN DE ATAQUES TIPO(BEC) BUSINESS EMAIL COMPROMISE

En MUFG monitoreamos continuamente la evolución sobre el panorama de amenazas y redoblamos los esfuerzos para ayudar a proteger a nuestros clientes de intentos de fraude cada vez más sofisticados. Es importante que cada cliente de MUFG desarrolle un conjunto de políticas y procedimientos internos apropiados en su organización para ayudar a detener este tipo de fraudes.

Business email compromise (BEC) es uno de los principales intentos de fraude dirigido a clientes de MUFG en todos los sectores e industrias. Según el FBI, el fraude a través de BEC ha costado a las empresas más de 50 mil millones de dólares en pérdidas nacionales e internacionales desde que comenzaron a rastrear estos incidentes en 2013 [1].

En este tipo de fraudes BEC, los delincuentes intentan obtener acceso a su organización mediante ingeniería social, correos electrónicos de phishing o intentos de suplantación de identidad. El estafador puede comprometer una cuenta de correo electrónico y puede hacerse pasar por un remitente (que podría ser su director ejecutivo, director financiero, abogado, contraparte comercial, etc.) y solicitará a uno de sus empleados que esté autorizado (por ejemplo, alguien de su nómina o departamento de contabilidad) a realizar pagos para transferir fondos a la cuenta del defraudador. El defraudador puede utilizar un formato y un lenguaje similar al de la persona por la que se hace pasar, también generalmente el lenguaje o tono tiene carácter de ser una urgencia.

A las instituciones financieras les resulta difícil recuperar esos fondos una vez autorizado y transferido el pago. Los estafadores moverán rápidamente los fondos a múltiples cuentas con poca o ninguna información bancaria rastreable.

QUÉ BUSCAR

Algunas posibles señales de alerta en un intento de fraude tipo BEC pueden incluir las siguientes:

- Solicitud para transferir fondos con urgencia cerca del final del día hábil (u hora límite de pago), antes de los fines de semana o feriados.
- Presión para no seguir los procesos internos establecidos o de validación y mantener la transferencia confidencial.
- Solicitudes de información bancaria nueva o de cambio o envío a una cuenta bancaria en el extranjero.
- Solicitudes de transferencia de fondos por montos en diferentes a las transacciones habituales.

REVISAR SUS CONTROLES DE SEGURIDAD

- Verifique su entorno de seguridad de la información es decir mantenga su software antimalware actualizado y sus sistemas con parches de seguridad. Lleve a cabo capacitaciones periódicas para todos los empleados incluido el nivel ejecutivo.
- Revise los protocolos de ciberseguridad de su proveedor de internet para asegurarse de que sean consistentes y cumplan con los mismos estándares de su organización.
- Utilice contraseñas seguras y complejas con un mínimo de ocho caracteres que sean únicas para cada cuenta.

CONFIRMAR Y CONSULTAR

- Verifique la información de contacto del solicitante utilizando un número de teléfono registrado conocido. Nunca utilice la información de contacto contenida en una firma de correo electrónico.
- No responda a correos electrónicos sin antes confirmar la dirección de correo electrónico del remitente y destino. Los estafadores suelen utilizar direcciones de correo electrónico falsos que parecen idénticos pero que difieren ligeramente de los correctos.

REVISA TU PROCESO DE APROBACIONES INTERNAS

• Revise la lista de empleados autorizados para aprobar pagos y asegúrese de que haya varios firmantes para emitir pagos o cheques.

[1] *"Business Email Compromise: The $50 Billion Scam" FBI Internet Crime Complaint Center, June 9, 2023*
