Fraude de compromiso de correo electrónico comercial

Una alerta de seguridad del proveedor.

MSD se toma en serio el fraude y la protección de la información.

Tenga en cuenta que, con la mayor dependencia de la comunicación virtual, la incidencia del Compromiso de correo electrónico comercial (Business Email Compromise, BEC) está en aumento. El BEC utiliza el correo electrónico y otras comunicaciones electrónicas para hacerse pasar por un ejecutivo, empleado u otra persona de autoridad.
Las solicitudes de pago o el acceso a la nómina de empleados o a la información W2 (solo en EE. UU.) se realizan de manera fraudulenta en nombre de una empresa.

Lo que debería saber
MSD se compromete a proteger su información bancaria y comercial. De acuerdo con nuestra Oficina de

Privacidad Global, nuestros procesos y pautas de Tecnología de la Información, y alineados con las regulaciones locales y regionales, nuestro personal capacitado aplica procesos y controles estrictos a la recopilación, validación y captura de datos, con múltiples puntos de verificación y auditorías regulares de nuestros procedimientos y prácticas.

Para proteger mejor su negocio:

- Use canales secundarios, o autenticación de dos factores, para verificar independientemente las solicitudes de cambios en la información de la cuenta.
- Asegúrese de que las URL en los correos electrónicos estén asociadas con la empresa de la que dicen ser.
- Esté atento a los hipervínculos que contienen errores ortográficos del nombre de dominio real.
- Verifique la dirección de correo electrónico utilizada para enviar correos electrónicos y haga que coincida con el remitente, especialmente cuando utilice un dispositivo móvil o de mano.
- Cree filtros del sistema de detección de intrusiones para marcar correos electrónicos con extensiones que se parecen al correo electrónico de la empresa. Por ejemplo, el correo electrónico legítimo de ceo@abc_company.com se marcaría como correo electrónico fraudulento de ceo@abc-company.com.
- Monitoree regularmente las cuentas financieras para detectar irregularidades, como depósitos faltantes.
- Mantenga actualizados todos los parches de software y todos los sistemas.
- Asegúrese de que la configuración en las computadoras de los empleados permita ver extensiones de correo electrónico completas.
- Conozca la información de contacto de su Centro de Resolución local y póngalos sobre aviso si cree que es víctima de BEC y se relaciona con

MSD; de lo contrario, póngase en contacto con la policía local.

Nos llamamos MSD en todas partes, excepto en Estados Unidos y Canadá, donde nos conocen como Merck & Co Inc, Rahway, NJ, EE. UU.