

Business Email Compromise Fraud



Eine Sicherheitswarnung für Lieferanten.

MSD nimmt Betrug und Datenschutz
sehr ernst.

Da wir zunehmend auf virtuelle Kommunikation zurückgreifen, sollten Sie sich bewusst sein, dass auch CEO-Fraud oder Business Email Compromise (BEC) ebenfalls vermehrt auftritt. Bei BEC wird vorgetäuscht, dass eine E-Mail oder andere Art der elektronischen Kommunikation von einem Mitglied der Geschäftsleitung, Mitarbeiter oder einer anderen Autoritätsperson stammt.

Bei diesem Betrug wird im vermeintlichen Namen eines Unternehmens um Zahlungen, Zugang zur Entgeltabrechnung für Mitarbeiter oder W2 (Nur in den USA)-Steuerinformationen gebeten.



Was Sie wissen sollten

MSD widmet sich dem Schutz Ihrer Unternehmens- und Bankinformationen. Gemäß unserem Global Privacy Office, unseren Informationstechnologie-Prozessen und -Richtlinien und im Einklang mit lokalen und regionalen Vorschriften befolgen unsere qualifizierten Mitarbeiter strikte Prozesse und Kontrollen beim Sammeln, Validieren und Erfassen von Daten, wobei mehrere Prüfpunkte und regelmäßige Prüfungen unserer Prozeduren und Praktiken durchgeführt werden.

Mit diesen Schritten können Sie Ihr Unternehmen besser schützen:

- Verwenden Sie Sekundärkanäle oder Zwei-Faktor-Authentifizierung, um Anfragen zur Änderung von Kontoinformationen unabhängig zu bestätigen.
- Achten Sie darauf, dass die URLs in E-Mails auch mit dem Unternehmen übereinstimmen, von dem sie angeblich stammen.
- Achten Sie besonders auf Hyperlinks, in denen der tatsächliche Domainname fehlerhaft erscheint.
- Verifizieren Sie die E-Mail-Adresse, mit der die E-Mails gesendet wurden und gleichen Sie diese mit dem Absender ab, besonders wenn Sie ein Mobilgerät verwenden.
- Erstellen Sie Intrusion-Detection-System-Filter, um E-Mails mit Erweiterungen zu erkennen, die wie Firmen-E-Mail erscheinen. Beispielsweise würde die legitime E-Mail `ceo@abc_company.com` als betrügerische E-Mail `onceo@abc-company.com` identifiziert werden.
- Überwachen Sie Finanzkonten regelmäßig auf Unregelmäßigkeiten wie fehlende Einzahlungen.
- Achten Sie darauf, dass alle Software-Patches und alle Systeme aktualisiert werden.
- Stellen Sie sicher, dass die Computer von Mitarbeitern so eingerichtet sind, dass die

vollständigen E-Mail-Erweiterungen angezeigt werden.

- Sie sollten die Kontaktinformationen Ihres lokalen [Resolution Center](#) kennen und es darauf aufmerksam machen, wenn Sie der Meinung sind, einem BEC in Bezug auf Merck oder MSD zum Opfer gefallen zu sein. Wenden Sie sich in allen anderen Fällen an Ihre lokale Polizei.

Außerhalb von den USA und Kanada ist Merck als MSD bekannt.