Fraude door middel van Business Email Compromise

Een beveiligingswaarschuwing voor leveranciers.

MSD neemt fraude en de bescherming van informatie serieus.

Houd er rekening mee dat onze toegenomen afhankelijkheid van virtuele communicatie ook gepaard gaat met een toename van Business Email Compromise (BEC - zakelijke-e-mailfraude). Bij BEC wordt gebruikgemaakt van e-mail en andere elektronische communicatiemiddelen, waarbij iemand zich voordoet als een leidinggevende, werknemer of andere persoon of instantie.
Verzoeken tot betalingen, of toegang tot de salarisadministratie of W2-informatie (alleen in de VS) worden op frauduleuze wijze gedaan of bewerkstelligd namens een bedrijf.

Wat u moet weten

MSD is toegewijd aan het beschermen van uw bedrijfs- en bankgegevens. In overeenstemming met onze wereldwijde privacyafdeling, onze processen en richtlijnen ten aanzien van informatietechnologie en zoals afgestemd met lokale en regionale richtlijnen, past ons opgeleide personeel strikte procedures en controles toe op de verzameling, validatie en vastlegging van gegevens met meerdere controlepunten en reguliere audits van onze procedures en werkwijzen.

Doe het volgende om uw bedrijf beter te beschermen:

- Gebruik secundaire kanalen of tweestapsverificatie om verzoeken tot wijzigingen van rekeninggegevens zelfstandig te controleren.
- Controleer of de URL's in e-mails betrekking hebben op het bedrijf dat de afzender beweert te vertegenwoordigen.
- Wees alert op hyperlinks die spelfouten bevatten in de daadwerkelijke domeinnaam.
- Verifieer het e-mailadres dat wordt gebruikt om e-mails te versturen en controleer of dit gekoppeld is aan de afzender, met name wanneer een mobiel of draagbaar apparaat wordt gebruikt.
- Maak systeemfilters voor toegangsdetectie aan om e-mails te signaleren met bijlagen die eruitzien als zakelijke e-mails. Bijvoorbeeld: een legitieme e-mail van ceo@abc_company.com zou worden gemarkeerd als frauduleuze e-mail van ceo@abc-company.com.
- Controleer financiële rekeningen regelmatig op onregelmatigheden, zoals ontbrekende stortingen.
- Houd alle softwarepatches en alle systemen geüpdatet.
- Zorg ervoor dat de instellingen op computers van werknemers het bekijken van volledige e-mailextensies toestaan.

- Zorg dat u bekend bent met de contactgegevens van uw lokale Resolution Center en waarschuw hen als u denkt dat u een slachtoffer bent van BEC en dit betrekking heeft op Merck of MSD; neem in alle andere gevallen contact op met uw lokale autoriteit voor wetshandhaving.