기업 이메일 공격 사기

공급업체 보안 경보

MSD는 사기와 정보 보호 사안을 심각하게 받아들이고 있습니다.

가상 통신에 대한 의존도가 높아짐에 따라 기업 이메일 공격(이하 "BEC") 사건의 발생률이 높아지고 있음을 인식해 주시기 바랍니다. BEC는 이메일과 기타 전자 통신을 이용하여 임직원 또는 그 밖의 권한을 가진 사람을 사칭합니다.
그런 다음 사기를 치려고 한 기업을 대리하여 결제를 요청하거나 직원 급여 또는 W2 (미국만 해당) 정보를 요청합니다.

알아 두어야 할 사항
MSD는 최선을 다해 귀사의 기업 정보와 및 은행 업무 정보를 보호합니다. 당사의 글로벌 개인정보 취급방침,

정보 기술 처리 및 가이드라인에 따라, 그리고 현지 지역 규정에 따라, 당사의 교육을 받은 직원은 데이터 수집과 확인 및 획득에 엄격한 프로세스와 통제를 적용하며 절차와 실행에 관해 여러 번 점검하고 정기적으로 감사를 실시합니다.

귀사를 더 잘 보호하기 위해:

- 이차적 경로 또는 이중 인증을 이용하여 계정정보에 대한 변경 요청을 별도로 확인하십시오.
- 이메일에 담긴 URL이 표시된 발신 기업과 실제로연관이 있는지 확인하십시오.
- 실제 도메인 이름에서 틀린 철자가 포함된하이퍼링크를 조심하십시오.
- 특히 모바일 기기나 소형 기기를 사용할 때는이메일 발송에 사용된 이메일 주소를 발신인과비교하며 확인하십시오.
- 회사 이메일처럼 보이는 거짓 확장명을 가진이메일을 거를 수 있도록 침투 감지 시스템 필터를만드십시오. 예를 들어, ceo@abc_company.com이적법한 이메일이라고 할 때 ceo@abc-company.com
  에서 발신된 이메일은 사기성으로 표시합니다.
- 입급 누락과 같은 이상이 없는지 정기적으로 금융계좌를 추적 관찰하십시오.
- 모든 소프트웨어 패치를 켜두고 모든 시스템을 최신상태로 유지하십시오.
- 직원 컴퓨터에서 설정을 이메일 확장명 전체가표시되도록 하십시오.
- 현지 해결 센터 연락처를 알아두시고 BEC 피해를입었고 그것이 MSD와 관련이 있다고생각되시면 해당 센터로 알리거나, 현지 사법당국에 신고하십시오.

우리는 Merck & Co Inc, Rahway, NJ USA로 알려진 미국과 캐나다를 제외하고 모든 곳에서 MSD라고 부릅니다.