비즈니스 이메일 침해(BEC) 예방법

Member FDIC

정보

비즈니스 이메일 침해(BEC)는 재정적으로 가장 큰 손해를 야기하는 온라인 범죄 중 하나입니다. BEC는 많은 기업이 이메일을 통해 비즈니스를 수행한다는 사실을 악용합니다. BEC 사기 수법에서 사기꾼은 확인된 출처에서 보낸 것처럼 보이는 이메일을 보내 적법한 요청인 것처럼 보이게 합니다. 사기 이메일은 다양한 시나리오로 전신환이나 ACH를 통해 자금을 보낼 것을 요구합니다. 확인된 전화번호로 간단히 다시 전화를 하여 요청을 확인한다면 BEC 피해자가 되는 것을 막는 데 도움이 될 수 있습니다.

배경/세부 정보

FBI에 따르면 지난해 BEC 사기로 인한 비즈니스 손실액은 27억 달러 이상이었습니다. 다음은 주의 깊게 살펴봐야 할 몇 가지 예시입니다.

1. 사기꾼은 여러분이 주기적으로 거래하는 업체인 척하며 향후 청구서 지불에 사용하기 위한 새로운 지불 지침을 이메일로 보냅니다.
2. 사기꾼은 회사 간부인 척하며 긴급하게 지불을 요청하는 이메일을 보내고 이와 관련하여 유선상으로 이야기할 수 없다고 설명합니다.
3. 사기꾼은 여러분이 아는 사람이거나 여러분과 일하는 회사의 일원인 척하며 향후 행사, 파티, 기타 상황을 위해 수십 개의 기프트카드를 구매할 것을 요청하는 이메일을 보냅니다. 사기꾼은 자신에게 바로 이메일을 보낼 수 있도록 일련 번호를 공유할 것을 요청합니다.

필요한 조치

1. ACH 또는 전신환 처리를 요청하기 전에 BEC 사기에 당한 것은 아닌지 확인하십시오.

   확인해야 할 몇 가지 질문:

   - 업체에게서 청구서 지불을 위해 여러분에게 은행계좌(계좌번호/은행)를 변경할 것을 요청하는 이메일/문자/팩스를 받았습니까? 만약 그렇다면 공급업체의 확인된 전화번호로 전화하여 은행 정보 변경을 요청했는지 확인했습니까?
   - 회사/개인에게 즉시 송금할 것을 요청하는 이메일을 받았습니까? 요청 상태가 긴급하고 비밀을 유지해야 합니까? 만약 그렇다면 회사/개인의 확인된 전화번호로 전화하여 송금을 요청했는지 확인했습니까?

2. 비즈니스 이메일 침해(BEC)는 정기적으로 직원들과 함께 논의되어야 합니다.

참고 자료

Business Email Compromise(BEC)에 대한 추가 정보를 제공하는 아래 참고 자료를 참조하시기 바랍니다.

1. https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/business-email-compromise
2. https://www.bankofhope.com/ko/privacy-and-security/online-security-information
3. 사기 인식 및 보호 체크리스트(The Fraud Awareness and Protection Checklist)에는 비즈니스 이메일 침해(BEC)를 방지하는 방법에 대한 '거래 보호' 모범 사례가 포함되어 있습니다. 사기 인식 및 보호 체크리스트 문서는 가까운 Bank of Hope 지점에 문의하십시오.

문의사항

비즈니스 이메일 침해(BEC) 관련 문의 사항이 있으면 **Global Treasury Management Solutions** **tmsoperations@bankofhope.com** 또는 **1-800-788-4580**으로 문의해 주십시오.

Bank of Hope®

Bankers. Experts. Neighbors.