

이메일해킹을 통한 무역사기 사례

⑥ 이메일사기

- 거래 당사자가 아닌 제3자가 개입하는 사기 형태로 6년간의 조사 기간('15~'20.8) 중 가장 많이 발생하였으나 최근('19.9~'20.8) 발생 비중은 소폭 감소함.

• 6년간 전체 무역사기 중 23.1%를 차지했으나, 최근 발생 비중 감소(19.5%→13.3%)

< 해외무역관에 접수된 이메일사기 건수 >

유형/시기	'15~'17.8	'17.9~'18.8	'18.9~'19.8	'19.9~'20.8	합계
전체 무역사기(건)	139	137	82	166	524
이메일사기(건)	58	25	16	22	121
이메일사기 비중(%)	41.7	18.2	19.5	13.3	23.1

- 이메일사기 피해가 지속되며 관련 사기 형태에 대한 우리기업의 관심과 주의가 커져 발생 비중이 다소 감소한 것으로 분석됨.
- 주로 거래기업 간 주고 받는 이메일을 오랫동안 지켜보다가 결정적인 순간에 계좌번호 변경을 요청하며 대금을 가로채는 형태
- 기업규모, 바이어 소재국과 무관하게 어떤 기업이라도 타깃이 될 수 있음.
- 특정 기업을 겨냥한 사이버 공격범죄인 '스피어피싱(Spearphishing)' *의 한 종류로, 수법이 정교해 사기를 인지하지 못하고 당하는 경우가 많음.
- 작살을 의미하는 스피어(Spear)와 보이스 피싱(Voice phishing)의 피싱(phishing)이 결합된 용어로 이메일사기에서 가장 많이 발견되는 타깃형 공격 범죄

< 전 세계에서 주목하고 있는 이메일사기 >

이메일사기는 불특정한 다수의 개인보단 특정 기업을 노리는 타깃형 온라인 범죄인 스피어피싱의 한 종류이다. 해커들은 특정 기업을 택한 후, 영업비밀이 포함되어있는 비즈니스 이메일을 탈취하거나 오랜 기간 기업 간 주고받는 내용을 지켜본다. 그리고 결정적인 순간에 계좌번호가 변경되었다는 메일을 보내 제3의 해외계좌에 대금을 입금하도록 유도해 이를 가로챈다.

이밖에도 컴퓨터 사용자의 키보드 움직임을 탐지해 아이디, 패스워드, 계좌번호 등과 같은 중요한 정보를 탈취해가는 키로거(Key Logger) 공격수법 또한 사용되고 있다. 악성코드를 설치하여 컴퓨터에 입력하는 중요한 데이터를 빼앗기 때문에 컴퓨터 보안 프로그램의 설치도 중요하다.

특히 이메일사기는 국내와 해외 등 최소 3개국 이상을 경유해 발생하는 경우가 많아 사건 해결을 위해서는 국제 사법공조가 요구되는 복잡한 케이스로 사전예방이 가장 중요하다.

자료출처 : kotra

< 이메일사기 유형 대표 사례 >

□ 이메일 해킹을 통한 수출대금 갈취

- 발생시기: 2020년 5월
- 발생국가: 과테말라
- 피해금액: US\$ 59,113
- 피해금액(US\$ 118,225) 중 절반은 바이어 부담

국내기업 A사는 과테말라 바이어 B사와 오랜 기간 좋은 관계를 유지해왔다. 그러던 중 B사는 코로나19로 한국은행 시스템에 기술적인 문제가 있어 미국 은행으로 대금을 송금해달라는 A사의 메일을 수신하였다. 제3세계 은행이 아닌 미국 은행으로의 송금 요청으로 B사는 의심 없이 대금을 송금하였다. 대금이 입금되지 않은 것을 확인한 A사가 B사에 확인을 요청하면서 무역사기가 발생했음을 뒤늦게 인지하게 되었다. B사가 받은 이메일은 A사 담당자의 이메일 주소와 동일했고, A사 담당자의 메일계정에서는 관련 메일의 수·발신 기록(계좌변경 요청 발신, 송금증 수신)이 모두 삭제된 상황이었다.

B사는 은행에 지급정지를 요청했으나 자금은 이미 인출된 상황이었다. 이에 양사는 그간의 비즈니스 관계 및 미국에서 금융관련 소송을 제기하는 것에 대한 부담 등을 고려해 손실금액을 공동 부담하는 것으로 마무리하였다.

□ 코로나19를 핑계로 한 이메일 사기로 수출대금 갈취

- 발생시기: 2020년 5월
- 발생국가: 콜롬비아
- 피해금액: US\$ 48,000

국내기업 A사와 콜롬비아 바이어 B사는 첫 계약을 체결하였다. 그 후 B사는 코로나19로 인한 환전수요 증가로 한국정부가 새로운 조세정책을 시행하여 세금손실(송금액의 12%)이 발생할 수 있으니 멕시코소재 계좌로 대금을 송금해달라는 A사의 이메일을 수신하였다. B사는 대금을 송금하였고, 대금을 받지 못한 A사가 확인을 요청하며 무역사기를 인지하게 되었다.

B사는 은행에 지급정지 및 환불을 요청했으나 자금은 이미 인출된 상태였다. 이에 A사와 B사는 콜롬비아 상공부 등에 해결책을 의뢰했으나, 해킹 사건이 제3국에서 발생했고 이미 대금이 인출된 상황으로 해결이 어렵다는 답변을 받았다. 이에 양사 간 협의를 통한 해결방안을 마련 중에 있다.

□ 이메일 해킹으로 인한 무역대금 결제 피해

- 발생시기: 2020년 3월
- 발생국가: 몽골
- 피해금액: US\$ 34,336

국내기업 T사는 몽골 바이어 O사에 수년간 건강제품을 공급해왔다. 홍삼캔디 공급계약을 체결하고 교신하던 중 이메일 해킹으로 거래 관련 중요 메일이 삭제되는 사건이 발생하였지만 T사와 O사는 이를 인지하지 못하고 거래를 진행하였다. 해커는 O사에게는 최종물량 선적을 안내하고 잔금 80%를 홍콩은행 계좌로 송금하도록 유도했으며, T사에게는 잔금에 대한 은행 송금증 사본을 보내는 등 양측을 안심시키는 치밀함을 보였다.

T사와 O사는 2개월 동안 동 사실을 인지하지 못하고 있었으나, 이후 업무 연락 과정에서 무역사기를 인지하고 다툼이 발생하였다. 결국 양사는 마땅한 해결책을 찾지 못하였고 T사는 수출대금을 회수하지 못하였다.

□ 이메일 사기를 통한 대금 입금계좌 변경 시도

- 발생시기: 2019년 10월
- 발생국가: 카자흐스탄
- 피해금액: 없음

국내 화장품기업 S사는 카자흐스탄 바이어 B사와 계약을 체결하였다. 대금 입금시점에 B사는 2차례에 걸쳐 S사로부터 이메일로 인보이스를 받았다. 인보이스에 대금 수령자는 개인이며, 은행은 말레이시아와 스웨덴에 소재해 있었다. 이메일에는 기업 감사로 인해 자사의 해외 지사로 은행계좌를 바꾼다고 설명되어 있었다. 이를 이상하게 여긴 B사는 알마티 무역관에 메일 내용 및 인보이스의 진위여부를 확인해 줄 것을 요청하였다.

무역관은 S사가 한국소재 은행의 법인명의 계좌만 이용하고 있다는 사실, 그리고 해외지사는 없으며 어떠한 기업 감사도 진행되고 있지 않다는 사실을 파악하였다. 무역관은 S사에 이메일 해킹 사실을 알렸고, B사에 S사의 답변 내용을 전달하여 무역사기 피해를 막을 수 있었다.

□ 해킹사실 인지도도 불구하고 이메일사기 발생

- 발생시기: 2019년 9월
- 발생국가: 캐나다
- 피해금액: US\$ 129,507

국내기업 A사는 캐나다 바이어 B사와 독점계약을 체결하고 지속적으로 거래량을 늘려가고 있었다. A사는 2019년 7월, 다른 기업과의 거래 중 해킹 위험이 감지되어 B사에게 대금 송금을 중단하고 기다려줄 것을 요청하였다. 하지만 해당 내용을 확인한 해커가 B사를 사칭하여 A사에 계좌정보를 요청하였고 A사로부터 받은 서류의 계좌정보를 수정하여 B사에 송부하였다. 이에 B사는 별다른 의심 없이 변경된 계좌로 송금을 진행하였다.

무역사기가 발생하였음을 뒤늦게 인지한 양사는 은행 측에 지급정지를 요청하였지만 이미 자금은 빠져나간 상태였으며, 해커의 계좌 소재지인 홍콩 경찰에도 신고하였지만 피해 금액의 회수 가능성은 거의 없다는 안내를 받았다.

□ 이메일 주소가 변경된 것을 발견해 무역사기 피해 예방

- 발생시기: 2019년 9월
- 발생국가: 스페인
- 피해금액: 없음

국내기업 L사는 스페인 바이어 S사와 오랜 기간 거래를 하였다. 어느 날 S사는 L사로부터 입금 계좌가 변경되었다는 안내 이메일을 받았다. 그러나 변경된 계좌가 중국 소재 은행임을 확인한 S사는 이상함을 느끼고 해당 이메일을 면밀히 확인해보았다. 확인결과 계좌변경을 안내했던 이메일은 L사의 기존 이메일과 교묘하게 다른 주소를 사용하고 있었다.

S사는 좀 더 명확한 확인을 위해 마드리드 무역관에 연락하였다. 마드리드 무역관이 L사와 함께 확인한 결과, 해커가 L사의 이메일을 해킹하여 S사와의 거래 사실을 훑쳐본 뒤 유사한 이메일 계정을 생성해 S사에게 이메일을 보낸 것이었다. 다행히 S사가 송금하기 전 이메일사기 사실을 발견하여 양사는 무역사기로 인한 피해를 방지할 수 있었다.

이메일사기 대응방안

● 이메일사기

- **계좌번호가 변경되었다면서 제3의 계좌로 돈을 송금토록 유도하는 것은 이메일 무역사기의 전형적인 패턴이므로 주의 필요**
 - 거래기업이 변경된 계좌번호를 안내할 때는 유선, 팩스, 화상회의 등 이메일 외 교신수단을 이용해 재확인 요망
 - * 중요 거래정보를 포함한 서류는 별도 전송시스템을 구축해 공유하거나 다양한 방법으로 중복 전달하고 안전하게 수신되었는지 등 추가 확인 필요
 - 해외기업 소재지와 대금 수취은행 소재지가 상이할 경우 주의 필요
 - * (예시) 몽골 소재 기업과 거래 중 대금은 홍콩 은행으로 송금 요청을 받을 경우

< 계약서 작성 시 TIP >

계약서에 특약사항으로 거래조건이나 거래정보 변경시 양측에서 취해야 할 행동을 명문화하면, 이메일사기를 통한 대금 오지급을 1차적으로 차단할 수 있다. 또한 오지급이 발생하더라도 어떠한 행동절차를 취했는지에 따라 책임소재를 명확히 할 수 있다. 예를 들어, 사고 발생 시 50:50 책임 분담 등의 내용을 계약서에 명시하면 양사 모두가 거래에 주의를 기울일 수 있다.

- **이메일 보안은 철저하게, 이메일 발신자 정보는 꼼꼼하게 확인할 것**
 - 이메일 비밀번호는 자주 변경하고, 최신 보안 프로그램 설치 필요
 - 의심스러운 이메일은 절대 열람하지 말고 즉시 삭제
 - * 특히 첨부파일 열람 금지. 첨부파일 내 악성코드를 통해 서버에 침투 가능
 - 회사 이메일계정 외에 상용메일을 사용할 경우, 특히 보안에 주의
 - * 회사 이메일 계정 사용 시에도 상용메일과의 연동은 자제하는 것이 바람직

< 이메일 주소를 교묘하게 변경한 사례 >

- ① widgetspo@freemail.com -> widgettpo@freemail.com (중간철자 삭제)
- ② acmepof868@freemail.com -> acmepof686@freemail.com (숫자 재배치)
- ③ iamthebest@kora.com -> iamthebest@krea.com (도메인변경)
- ④ sales@gmail.com -> sales@gmail.com (글자변환)
 - * 소문자 l을 대문자 I로 변경함. (글꼴 크기를 키워서 확인해보면 구분 가능)

○ 피해 발생 시 가장 먼저 은행에 지급정지 요청

- 이메일사기로 탈취한 대금은 중간지 은행을 경유해 최종 도착지로 입금되기 때문에 곧바로 은행에 지급정지를 요청
- 상대 국가에서도 수사가 진행될 수 있도록 상대 거래기업에게 협조 요청
 - * 최초 송금은행, 중간지 은행, 최종 수취은행까지 모든 은행에 지급정지 요청
 - ** 우리기업이 지급정지를 요청하더라도 상대국가에서 수사가 이루어지지 않으면 지급정지가 진행되지 않을 수 있음.
- 지급정지 요청 후, 계좌 상세 내역이 포함된 송금확인증과 해커가 발송한 이메일, 이메일 접속 아이피 등을 취합해 관할 경찰서에 신고

< 이메일사기 신고 순서 >



< 이메일사기 경찰서 신고방법 (온라인) >



주1: (컴퓨터) 경찰청 홈페이지 > 사이버안전 지킴이 > 사이버범죄 신고/상담
 주2: (모바일) 사이버캡 > 사이버범죄 신고/상담

IV

무역사기 대응 핵심 행동요령 및 관련 웹사이트

□ 무역사기 대응 핵심 행동요령

- 무역사기 피해 예방을 위한 행동요령
 - KOTRA, 한국무역보험공사 등 다양한 서비스 활용

기관명	서비스명	내용
KOTRA (☎ 1600-7119)	무역투자상담	기업실존여부 확인 등
	해외수입업체 연락처 확인	
한국무역보험공사 (☎ 1588-3884)	수출입보험	무역관련 보험
	국외기업 신용조사	바이어 신용정보 조사

- 무역사기 피해 발생 후 행동요령

거래은행에 지급정지 신청 → 가까운 경찰서 민원실에 신고

거래은행	· 한국은행 및 거래 상대국가의 은행에도 지급정지 신청
경찰관서	· (PC) 경찰청 홈페이지 → 사이버안전 지킴이 → 사이버범죄 신고/상담 · (모바일) 사이버캡 → 사이버범죄 신고/상담 · (사이버범죄 신고 상담, 24시간 운영) ☎ 02-3150-2659 · 필요증빙: 계좌 상세내역이 포함된 송금확인증, 해커가 발송한 이메일, 이메일 접속 아이피 등

기관명	서비스명	내용
9988 중소기업법률지원단 (☎ 02-2110-3867)	국제사건 법률자문	소송을 위한 법률자문
나이스신용정보 (☎ 02-2122-2000)	해외미수채권 회수서비스	미수금액 회수 지원
대한상사중재원 (☎ 02-551-2000)	중재제도	바이어와의 중재 지원

자료출처 : kotra