

금융생활에 필요한 모든 정보, 인터넷에서 「파인」 두 글자를 쳐보세요

“금융은 튼튼하게, 소비자는 행복하게”



보도자료

보고	2018. 3. 19.(월) 조간	배포	2018. 3. 16.(금)
----	--------------------	----	-----------------

담당부서	불법금융대응단	이명규 팀장(3145-8521), 김흠 선임조사역(3145-8155)
------	---------	--

제 목 : 정부기관을 사칭한 보이스피싱으로 9억원 피해 발생!
- 검찰·경찰·금감원 등 정부기관을 사칭한 보이스피싱에 각별한 주의 필요

1 피해 내용*

* 피해자 개인정보 보호를 위해 일부 내용 편집

□ 최근 70대 고령자가 금융감독원을 사칭하는 보이스피싱 사기범에게 속아 9억원*을 사기당한 피해 발생

* 기존 1인 최대 피해금액은 8억원('17.12월)으로 현재까지 1인 피해금액 최대

① 사기범은 발신번호가 '02-112'로 보이도록 피해자에게 전화하여 금융감독원 팀장을 사칭, 피해자 명의의 대포통장이 개설되어 범죄에 이용되었다며 불안감을 조성

- 처벌을 피하기 위해서는 범죄에 연루된 피해금을 맡겨야 한다고 속여 돈을 송금할 것을 요구

② 피해자는 2일에 걸쳐 3개 금융기관 5개 지점을 방문하여 정기예금 및 보험을 해지한 후 사기범이 알려준 대포통장 3개 계좌로 총 9억원을 송금

- 특히, 보이스피싱을 의심한 은행 창구직원이 피해자에게 예금 해지 및 자금사용 목적을 문의하였지만,

사기범이 피해자를 현혹하여 '친척에게 사업자금을 보내는 것'이라고 답하도록 유도함으로써 피해를 막을 수 없었음

2 소비자 유의사항

- 전화로 정부기관이라며 돈을 보내라고 요구하면 일단 보이스피싱 의심
 - 수사기관·금감원 직원 등이라는 전화를 받은 경우 당황하지 말고 소속, 직위 및 이름을 확인한 후 전화를 끊고*
 - * 전화를 끊지 못하도록 하거나 이름을 말하지 않고 불이익을 받을 수 있다는 등 고압적인 말투로 재촉하는 경우 보이스피싱을 의심
 - 주변 지인에게 통화내용을 설명하여 도움을 받거나 해당 기관의 공식 대표번호*로 전화하여 반드시 사실여부를 확인할 것을 당부드림
 - * 대검찰청(☎02-3480-2000), 경찰청(☎112), 금감원(☎1332)
 - 한편, 송금인 정보를 변경하여 타인 명의의 계좌로 금전을 보내라고 요구한다면 100% 보이스피싱임을 명심
- 보이스피싱 의심전화를 받은 경우 지체없이 경찰서(☎112)나 금융감독원(☎1332)에 신고
 - 특히, 보이스피싱 피해를 입은 경우에는 신속하게 경찰서나 해당 금융회사에 신고하여 지급정지를 신청해야 피해구제를 받을 수 있음

3 향후 대응방안

- 금융회사에 60세 이상 고령층에 대해 보이스피싱 위험 안내를 강화하도록 지도하는 한편, 맞춤형 홍보물을 제작하여 대한노인회에 제공하는 등 동 사례를 집중 전파
- 한편, 현재 창구에서 예·적금 중도해지시 일부 금융회사에서 자율적으로 운영중인 문진제도를 다른 금융회사에도 확대하는 방안을 검토

☞ 본 자료를 인용하여 보도할 경우에는 출처를 표기하여 주시기 바랍니다.(<http://www.fss.or.kr>)

보이스피싱! 이것만 알아도 당황하지 않습니다!

① 전화로 정부기관이라며 자금이체를 요구하면 일단 보이스피싱 의심

검찰·경찰·금감원 등 정부기관은 어떠한 경우에도 전화로 자금의 이체 또는 개인의 금융거래정보를 요구하지 않습니다. 정부기관을 사칭, 범죄에 연루되었다며 금융거래 정보를 요구하거나 안전조치 등을 명목으로 자금의 이체 등을 요구하는 경우는 100% 보이스피싱이므로 이러한 전화를 받는 경우 전화를 끊고 해당 기관의 **대표전화***로 전화하여 사실여부를 반드시 확인하시기 바랍니다.

* 대검찰청(☎02-3480-2000), 경찰(☎112), 금감원(☎1332)

② 전화·문자로 대출 권유받는 경우 무대응 또는 금융회사 여부 확인

전화 또는 문자를 통한 대출광고는 대출빙자형 보이스피싱일 가능성이 높으므로 이러한 연락을 받은 경우 반드시 금융회사의 실제 존재여부를 우선 확인한 후, 대출을 권유하는 자가 금융회사 직원인지 또는 정식 등록된 대출모집인인지 여부를 확인하시기 바랍니다.

* 제도권 금융회사 조회(<http://www.fss.or.kr>)
 대출모집인 등록 조회(<http://www.loanconsultant.or.kr>)

③ 대출 처리비용 등을 이유로 선입금 요구시 보이스피싱을 의심

정상적인 금융회사는 전산비용, 보증료, 저금리 전환 예치금, 선이자 등 어떠한 명목으로도 대출과 관련하여 선입금하라고 요구하지 않으므로, 이러한 요구에 절대로 응해서는 안됩니다.

④ 저금리 대출 위한 고금리 대출 권유는 100% 보이스피싱

정상적인 금융회사는 저금리 대출을 받기 위해서 고금리 대출을 먼저 받으라고 요구하지 않습니다. 저금리 대출을 받기 위해서는 거래실적을 쌓아야 한다며 고금리 대출을 먼저 받으라고 하는 경우는 100% 보이스피싱입니다. 또한 대출금 상환시에는 해당 금융회사의 계좌가 맞는지 여부를 반드시 확인하시기 바랍니다.

⑤ 납치·협박 전화를 받는 경우 자녀 안전부터 확인

자녀가 다쳤다가거나 납치되었다는 전화를 받았을 때에는 침착하게 대처해야 합니다. 사기범의 요구대로 급하게 금전을 입금하기 보다는 먼저 준비해 둔 지인들의 연락처를 이용하여 자녀가 안전한지 여부부터 확인하시기 바랍니다.

⑥ 채용을 이유로 계좌 비밀번호 등 요구시 보이스피싱 의심

정상적인 기업의 정식 채용절차에서는 급여계좌 개설 또는 보안관련 출입증 등에 필요하다면서 체크카드 및 금융거래정보(비밀번호, 공인인증서, OTP 등)를 절대 요구하지 않습니다. 급여계좌 등록은 실제로 취업된 후에 이루어지는 것으로, 본인 명의 계좌번호만 알려주면 됩니다.

⑦ 가족 등 사칭 금전 요구시 먼저 본인 확인

가족 및 지인 등이 메신저로 금전을 요구하는 경우 반드시 유선으로 한번 더 본인임을 확인하시기 바랍니다. 만약 상대방이 통화할 수 없는 상황 등을 들어 본인 확인을 회피하고자 하는 경우 직접 신분을 확인할 때까지는 금전요구에 응하지 말아야 합니다.

⑧ 출처 불명 파일·이메일·문자는 클릭하지 말고 삭제

출처가 불분명한 파일을 다운받거나 의심스러운 인터넷 주소가 포함된 문자를 클릭하면 악성 코드에 감염되어 개인정보가 유출될 수 있습니다. 악성코드 감염은 금융거래시 파밍 등을 일으키는 주요 원인이므로 이러한 파일이나 문자는 즉시 삭제하시기 바랍니다.

* 악성코드 치료 방법 : 한국인터넷진흥원(KISA)의 "인터넷 보호나라"사이트>"자료실"메뉴>공지사항 109번 게시글 참고

⑨ 금감원 팝업창 뜨고 금융거래정보 입력 요구시 100% 보이스피싱

인터넷 포털사이트에 접속시, 보안관련 인증절차를 진행한다는 내용의 금감원 팝업창이 뜨며, 이를 클릭하면 보안승급을 위해서라며 계좌번호, 비밀번호, 보안카드 번호 등 금융거래정보를 입력하라고 요구하면 보이스피싱(파밍)이니 절대 응해서는 안됩니다.

⑩ 보이스피싱 피해발생시 즉시 신고 후 피해금 환급 신청

사기범에게 속아 자금을 이체한 경우, 사기범이 예금을 인출하지 못하도록 신속히 경찰 또는 해당 금융회사에 전화하여 계좌에 대한 지급정지 조치를 하시기 바랍니다.

지급정지 조치 후 경찰서에 방문하여 피해 신고를 하고, 금융회사에 피해금 환급을 신청하시기 바랍니다. 해당 계좌에 피해금이 인출되지 않고 남아 있는 경우 피해금 환급제도에 따라 별도의 소송절차 없이 피해금을 되찾을 수 있습니다.