


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

“금융은 튼튼하게, 소비자는 행복하게”

	<h1>보도자료</h1>		
	보도	2017. 12. 12.(화) 조간	배포
담당부서	불법금융대응단 김상록 팀장(3145-8129), 김 흠 선임조사역(3145-8155)		

제 목 : 가짜 금융회사 앱(App)을 설치하지 마세요!

- 대출권유전화를 받으면 일단 전화를 끊고, 「파인」을 통해 확인하세요

I 현황

□ 최근 금융감독원 『불법사금융 피해신고센터(☎ 1332)』에 문자메시지 등을 이용하여 가짜 금융회사 앱(App)을 설치하게 한 후 이를 악용하는 사기 신고가 증가*

* '17.7월 32건 → '17.8월 79건 → '17.9월 63건 → '17.10월 58건 → '17.11월 153건

○ 이들은 전화와 가짜 앱(App)으로 소비자를 안심시키면서 햇살론 등 저금리 서민지원 대출을 명목으로 금전을 편취하는 것이 특징

※ 검·경 등 공공기관 뿐만 아니라 저축은행 등 금융회사를 사칭하는 대출 사기 신고*는 지속 발생

* '17.7월 2,222건 → '17.8월 2,355건 → '17.9월 2,014건 → '17.10월 1,432건 → '17.11월 2,498건

☞ 연말연시 서민들의 절박한 자금수요 사정을 악용하여 금전을 편취하는 대출사기 피해 예방을 위해 금융소비자의 각별한 주의를 당부할 필요

II

구체적 피해유형

□ 사기범들은 금융회사를 사칭하며 대출을 권유하는 전화통화 중에 문자메시지·카카오톡 등을 발송하여 가짜 앱을 설치하도록 유도

* 금융회사 앱을 가장한 '발신전화 가로채기' 기능의 앱

- 앱 설치 후 피해자가 금융감독원(1332), 금융회사 전화번호로 확인전화를 걸면 사기범에게 연결되어 마치 대출심사가 진행중인 것처럼 안내
- 이후 사기범은 기존 대출금 상환, 공탁금, 법무사 비용, 보증보험 등 다양한 명목으로 금전을 편취*

* 가짜 앱의 상담신청화면을 통해 성명, 주민등록번호(생년월일), 직장 등 개인정보도 탈취

< 문자메시지 등 안내에 따라 설치한 가짜 앱 화면 >

카카오톡·문자메시지	가짜 웹페이지	가짜 앱 화면

※ <붙임> 가짜 금융회사 앱을 이용한 대출사기 피해 사례

Ⅲ

소비자 유의사항

□ (악성코드 감염 유의) 출처가 불분명한 문자메시지의 인터넷 주소, 애플리케이션 등은 확인하거나 설치하지 말고 보는 즉시 바로 삭제

- 스마트폰을 '알 수 없는 소스'를 통한 앱 설치 허용하지 않도록 설정*할 필요

* 설정 → 보안 → 휴대폰 관리 → '알 수 없는 소스 허용하지 않음' 설정

- 또한, 최신 백신프로그램을 이용하여 주기적으로 휴대전화의 보안 점검을 실시하는 것도 좋은 방법

□ (제도권 금융회사 확인) 전화, 문자메시지 등으로 대출을 권유받는 경우 일단 전화를 끊고 금융소비자정보포털 '파인(<http://fine.fss.or.kr>)'에서 제도권 금융회사 여부를 확인할 것

- 특히, 발신 전화번호는 변작되어 금감원, 금융회사 등의 전화 번호로 허위 표시될 수 있으므로,

- 악성코드 감염 우려가 없는 유선전화 등으로 해당 금융회사 공식 대표 전화번호*로 전화하여 대출관련 사실여부를 확인할 것

* '파인(<http://fine.fss.or.kr>)' 검색, 114 또는 금감원(☎1332) 문의, 공식 홈페이지 (포털사이트에서 직접 검색)를 통해 직접 확인

□ (피해신고) 대출사기로 의심되는 전화 등을 받은 경우에는 경찰서 (☎112)나 금융감독원(☎1332)에 신속하게 신고할 것

- 특히, 금전적 피해를 입은 경우 당황하지 말고 신속하게 경찰서 (☎112)나 해당 금융회사에 신고하여 지급정지를 신청해야 피해 구제를 받을 수 있음

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

[사례 1]

- ① 사기범은 'OO캐피탈'을 사칭하여 피해자 A씨에게 **전화**하여 저금리로 전환 대출이 가능하다고 **대출상담** 진행
- ② 사기범은 피해자 A씨에게 **인터넷 URL** 주소를 알려주면서 'OO캐피탈'의 대출 관련 **앱**이라고 기망하며 이를 **설치하도록 유도**
- ③ 이후 사기범은 대출을 받기 위해서는 '공탁금이 필요하다', '계좌 잔고가 있어야 한다', '법무사 비용이 든다', '거래 내역이 있어야 한다'며 각종 명목으로 수수료를 요구
- ④ 피해자 A씨는 사기범의 말을 확인하기 위해 **금감원 콜센터(☎1332)**로 **전화**했으나 **악성코드 감염**으로 인해 금감원 직원을 사칭한 **사기범에게 연결**되었고,
 - 피해자는 안심하고 사기범이 지정해준 계좌(사기범의 대포통장)로 수차례에 걸쳐 총 0백만원을 송금하자 사기범은 이를 인출하여 잠적

[사례 2]

- ① 사기범은 피해자 B씨에게 'OO저축은행'을 사칭하여 **전화**하여 대출이 가능하다고 **대출상담** 진행
- ② 사기범은 피해자 B씨의 휴대폰에 **문자메시지(URL 포함)**를 보내 'OO저축은행' **앱**이라고 기망하며 이를 **설치하도록 유도**
- ③ 이후 사기범은 **기존 대출금을 상환**하여야 대출이 가능하다고 하면서 **지정된 계좌(사기범의 대포통장)로 상환**하라고 기망
- ④ 피해자 B씨는 해당 내용 확인차 **대출받은 금융회사에 전화**하였으나 **악성 코드 감염**으로 인해 금융회사 직원을 사칭한 **사기범에게 연결**되었고,
 - 기존 대출금 0천만원을 입금하자 사기범은 이를 인출하여 잠적