



**쿠팡 개인정보 유출사고를 빙자한
보이스피싱·스미싱 피해사례가 확인됨에 따라
소비자경보를 상향합니다!! (주의 → 경고)**

- “개인정보 도용”, “피해보상” 등을 미끼로 접근하여 피싱사이트, URL 접속 및 자금이체 유도
- 문자·전화 수신시 즉시 신고하고 「안심차단 서비스 3종 세트」에 가입하여 사전에 피해 차단

■ 소비자경보 2025 - 28호			
등급	주의 경고 위험		
대상	금융소비자 일반		

■ 소비자경보를 ‘주의’ 에서 ‘경고’ 로 상향

지난 12.1일 쿠팡 개인정보 유출사고와 관련하여 보이스피싱 등의 2차 피해를 예방하고자 소비자경보 ‘주의’를 발령*하였으나, 최근 피해사례가 확인되고 관련 제보도 증가함에 따라 소비자경보 등급을 ‘경고’로 한 단계 상향합니다.

* 「쿠팡 개인정보 유출사고에 따른 보이스피싱·스미싱 등 피해에 주의하세요(금융위·금감원)」


특히, 최근 수법은 개인정보 유출에 따른 명의도용 범죄발생 또는 피해보상 등을 언급하며, 금융소비자들의 불안감과 피해보상 심리 등을 교묘히 파고들고 있어 금융소비자들의 각별한 주의가 필요합니다.

■ 쿠팡 관련 보이스피싱·스미싱 발생사례 주요특징

- ※ 최근 제보된 사기범들의 실제 목소리(통화) 녹음파일, 문자 등을 분석하여 작성
- 쿠팡 개인정보 유출사고를 빙자한 보이스피싱 사기의 주요 특징 및 수법은 아래와 같습니다.



① [접근 : 쿠팡 개인정보 유출사태] 정보유출에 따른 **금융소비자의 '불안감' 악용**

감·경찰, 공정위 등 주로 정부기관을 사칭하는 사기범들은 쿠팡 관련 문자 수신 여부를 확인하는 등 정보유출 사태 대응업무를 수행하는 척하고, 개인정보 유출로 대포통장 개설, 자금세탁 등 범죄에 연루되었다며 소비자의 불안감을 악용하는 방식으로 접근합니다.

쿠팡 개인정보 유출사고 빙자 보이스피싱 수법(실제사례)	
접근 단계	<p>▶  "안녕하세요. ○○○씨 맞으시죠? 저는 공정거래수사1팀 이진호 사무관이고요. 최근 쿠팡에서 개인정보 유출됐다는 문자 받으셨죠? 쿠팡에서 유출된 정보로 ○○○씨 계좌가 불법적인 자금세탁 용도로 사용된 기록이 확인되어 연락드렸어요"</p> <p>→ 성명을 언급하며 의심을 최소화하고, 쿠팡에서 보낸 문자를 미끼로 접근</p>

② [기망 : 개인정보 도용사고] 피해사실 확인 등을 미끼로 **피싱사이트 접속 유도**

사기범들은 소비자를 피싱사이트에 접속시키기 위하여 다양한 명목의 거짓말을 하는데, 최근에는 범죄사건 관련 등기가 반송되었으니 인터넷으로 열람하라고 하거나, 피해여부 확인 등이 필요하다는 수법이 자주 사용됩니다.

쿠팡 개인정보 유출사고 빙자 보이스피싱 수법(실제사례)	
기망 단계	<p>▶  (등기반송 빙자) "그래서 저희가 참고인 조사차 출석요구서를 등기로 발송드렸는데 반송됐더라고요."</p> <p>▶  (피싱사이트 접속유도) "공문 못 받으셨으니까 방문수령 가능하실까요? 방문수령이 어려우실 경우에는 저희가 인터넷 열람을 안내해 드리고 있거든요. 네네. 인터넷 주소창에 소문자로 mn8.kro.kr 쳐주시면요 ... 왼쪽 하단에 나의 사건조회 보이실거예요."</p> <p>→ 등기가 반송되었다고 속이면서 인터넷 열람을 빙자하여 피싱사이트 접속 유도</p>

③ [편취 : 악성앱 설치 및 자금편취] 피해자 **휴대폰을 장악하여 자금이체 유도**

피싱사이트*에 접속하면 본인확인 등을 빙자하여 개인정보 입력과 악성앱·원격제어앱 설치를 유도하는데, 악성앱 등이 설치되면 사기범은 전화번호 조작, 휴대폰 내 개인정보 탈취, 피해자의 실시간 위치확인 등이 가능합니다.

* 피싱사이트의 외형은 정부기관 등의 공식사이트와 거의 동일하게 꾸며놓아 구별이 쉽지 않음

이를 통해 사기범들은 피해자의 심리를 지배하고 피해자는 악성앱 등을 통해 개인정보가 넘어갔음에도, 검·경찰, 금감원 등 공공기관이 파악한 정보로 착각하고, 정교한 시나리오에 의해 가스라이팅 당한 피해자는 사기범들의 요구에 따라 자산 보호, 약식기소 공탁금 등의 명목으로 자금을 이체합니다.

쿠팡 개인정보 유출사고 빙자 스미싱 수법(실제사례)	
<p>▶ [Web 발신] 안녕하세요 △△△님 저희는 다양한 온라인 서비스에서 결제를 처리하는 국내 전자결제 대행사 XXXX페이 입니다. 최근 국내에서 연이어 발생한 대규모 해킹사태(쿠팡 등)와 관련하여, 당사 시스템에도 외부 해킹공격이 있었음을 확인했습니다.</p> <p>【유출 대상자 정보】 성함: △△△ 연락처 : 010-0000-0000 정보유출 은행 : ◇◇◇◇◇◇◇◇◇◇/□□은행</p>	<p>▶ [Web 발신] 이러한 상황에 대해 진심으로 사과드리며, 해당 고객님의께서는 피해보상 절차를 안내드리고자 문자를 드립니다.</p> <ul style="list-style-type: none"> · 피해보상금 : 7,781,208원 · 피해보상 공지확인 : https://dboxx.xxxxxx.xx · 텔레그램 접수 : https://xxx.xxx <p>※ 개인정보 보호를 위해 반드시 텔레그램을 통한 접수만 받도록 하겠습니다.</p> <p>※ 반드시 본인확인 후 보상절차를 진행해 주시기 바랍니다.</p>
→ 유출된 성명, 연락처, 은행 계좌번호 등을 구체적으로 나열하며 불안심리 조장	→ 구체적인 피해보상금 으로 현혹하여 악성 링크(URL) 를 클릭하도록 유도

■ 소비자 주의사항 및 대응 요령

① 법원, 검·경찰, 우체국 등이 '**법원등기 반송**', '**사건 확인**' 등의 명목으로 **특정 사이트, 링크(URL) 접속**이나 **앱 설치**를 요구한다면 **100% 보이스피싱**입니다.

피싱사이트나 문자속 링크(URL) 등에 접속하여 개인정보를 입력하거나 앱 설치를 한다면 사기범이 내 휴대폰을 통제할 수 있으니 주의해야 합니다.

특히, 보안점검 등의 명목으로 공식 앱스토어에서 원격제어 앱*을 다운받게 한 후, 사기범이 원격제어를 통해 직접 악성 앱을 설치할 수 있으므로 제3자의 요구에 의한 앱설치는 공식 앱스토어를 통하더라도 무조건 거절하는 것이 안전합니다.

※ (참고) **원격제어앱** : any**, OS**, Air** 등 다수

▶ 휴대폰, 컴퓨터 등을 원격으로 '제어'할 수 있도록 만든 공식 어플리케이션. 주로 원격근무나 가족(고령, 어린이 등)의 휴대폰 관리 등에 활용되는 유용한 프로그램이나, **사기범들이 설치시 피해자 휴대폰을 통제하여 악성앱을 설치하는 등 악용 가능**

2 금융거래 안심차단 서비스 가입으로 금융사기범죄 피해를 사전에 예방하세요.

「안심차단 서비스 3종 세트」에 가입하면 본인도 모르게 대출·비대면 계좌 개설·오픈뱅킹이 실행되어 피해가 발생하는 것을 사전에 차단할 수 있습니다. 금융회사 영업점*·은행앱 또는 어카운트인포를 통해 간편하게 신청가능합니다.

* 은행, 저축은행, 농협, 수협, 신협, 새마을금고, 산림조합, 우체국 등 한 곳에만 신청하여도 전 금융권에 자동적으로 전파됨

「안심차단 서비스 3종 세트」 개요

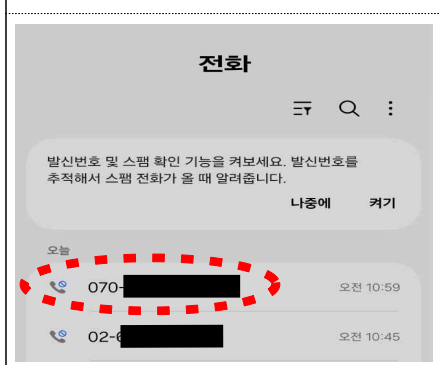
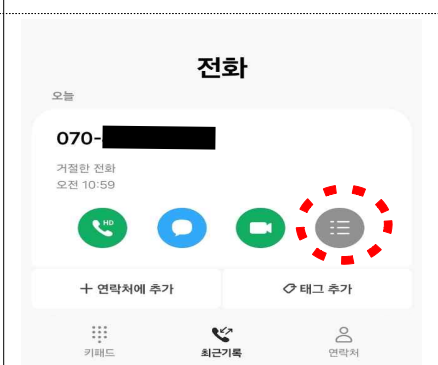
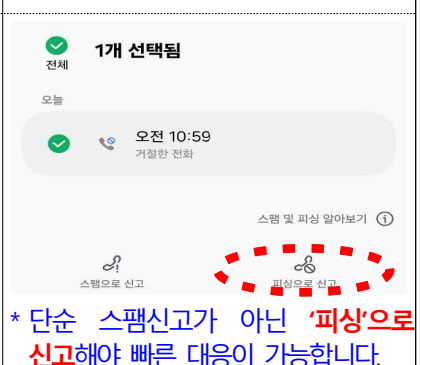
- ① (여신거래 안심차단) 신용대출, 카드로, 신용카드 발급, 할부금융, 예·적금 담보 대출 등 개인 명의의 여신거래를 차단('24.8.23. 시행)
- ② (비대면 계좌개설 안심차단) 범죄조직의 수익의 통로로 사용될 수 있는 대포통장 개설로 인한 피해 방지를 위해 비대면 계좌개설을 차단('25.3.12. 시행)
- ③ (오픈뱅킹 안심차단) 오픈뱅킹을 통한 계좌정보 무단조회 및 이체 등을 방지할 수 있도록 오픈뱅킹 서비스를 차단('25.11.14. 시행)

3 보이스피싱 전화나 문자를 받으면 휴대폰 간편제보 기능을 통해 즉시 신고해 주세요.

'25. 11. 24.부터 삼성전자 휴대전화 단말기에 보이스피싱 신고 기능이 단순 스팸신고와 구분되어 신설되었습니다. 보이스피싱 전화나 문자수신시 **통화기록(전화)**의 '**신고**' 버튼 또는 **문자상단**의 '**메시지 신고(문자)**'를 클릭하여 보이스피싱을 즉시 신고하여 주시기 바랍니다.

※ 신고시 발신번호·문자 내용(음성) 등이 '통합대응단(경찰청)으로 전송되며, 통합대응단은 피싱이 의심되는 경우 통신사 등에 차단을 요청

삼성전자 휴대폰 단말기의 보이스피싱 신고 기능







▶ 통화 ① 통화목록에서 의심번호 선택	② '상세보기' 아이콘 클릭	③ '피싱으로 신고' 선택
 <p>발신번호 및 스팸 확인 기능을 켜보세요. 발신번호를 추적해서 스팸 전화가 올 때 알려줍니다.</p> <p>나중에 켜기</p> <p>오늘</p> <p>070-... 오전 10:59</p> <p>02-... 오전 10:45</p>	 <p>오늘</p> <p>070-... 거절한 전화 오전 10:59</p> <p>HD, 메시지, 영상, 신고</p> <p>+ 연락처에 추가 태그 추가</p> <p>키보드, 최근기록, 연락처</p>	 <p>1개 선택됨</p> <p>오늘</p> <p>오전 10:59 거절한 전화</p> <p>스팸 및 피싱 알아보기 ⓘ</p> <p>스팸으로 신고 피싱으로 신고</p> <p>* 단순 스팸신고가 아닌 '피싱'으로 신고해야 빠른 대응이 가능합니다.</p>

【 사례 ① 】

<p>접근 단계</p>	<p>[정부기관 소속직원 사칭범] (피해자에게 전화하여) “안녕하세요. 김○○님 맞으실까요? 네, 수고하십니다. 저는 공정거래수사 1팀 이진호 사무관 이고요.</p> <p>[피해자] 네?</p> <p>[정부기관 소속직원 사칭범] 공정거래수사 1팀 이진호 사무관이에요. 최근 쿠팡에서 개인정보 유출됐다는 문자 받으셨죠?</p> <p>[피해자] 네.</p>
<p>기망 단계</p>	<p>[정부기관 소속직원 사칭범] 이거 해당 사건 관련해가지고 저희가 공문을 등기로 발송을 해드렸는데 반송이 됐더라고요</p> <p>[피해자] 등기 왔다는 문자를 못 받았는데요?</p> <p>[정부기관 소속직원 사칭범] 우체국에서 연락을 못 받으신 거예요?</p> <p>[피해자] 네. 아예 연락이 안 왔었는데요.</p> <p>[정부기관 소속직원 사칭범] 쿠팡 측에서 문자 내용 전달은 받으셨죠?</p> <p>[피해자] 네.</p> <p>[정부기관 소속직원 사칭범] 일단 본인 계좌가 이용이 된 정황이 있어가지고 저희가 참고인 조사차 출석 요구서 보내드린 거고요. 02 번호로 사건 내용은 전달받으셨죠?</p> <p>[피해자] 아니요.</p> <p>[정부기관 소속직원 사칭범] 02 번호로 전화를 갔을 텐데 못 받으셨나요?</p> <p>[피해자] 전화 자체가 안 왔는데요.</p> <p>[정부기관 소속직원 사칭범] 02 번호 전화가 안 온 거예요? 아니면 본인이 안 받으신 거예요?</p> <p>[피해자] 전화자체가 안 왔어요. 제가 전화를 다 받는데 안 왔어요.</p> <p>[정부기관 소속직원 사칭범] 그럼 본인이 직접 사건 조회를 하시고 내용 열람만 해보셔야 될 것 같은데 사건 조회하시는 법 아시죠?</p> <p>[피해자] 제가 일단은 바쁘니까 다시 연락 주실래요? 이따가?</p> <p>[정부기관 소속직원 사칭범] 아니 사건 조회하시는 법 아시냐고요? 사건 조회 하려면 이 사이트로 들어가셔야 해요.</p>

【 사례 ② 】

<p>접근 단계</p>	<p>[정부기관 소속직원 사칭범] (피해자에게 전화하여) “여보세요. 권△△님 되시죠? 네. 안녕하세요. 저희 서울중앙지법 행정과고요. 최근 쿠팡에서 개인정보 유출된 사태에 대해서 들어보신 적 있으실까요?. 권△△님 해당 쿠팡에서 본인계좌가 불법적으로 세탁 용도로 사용된 기록이 확인돼서요.</p>
<p>기망 단계</p>	<p>[정부기관 소속직원 사칭범] 저희가 해당 통지서 발송해드렸는데 미수령 확인돼서 연락드렸고요. 해당 공문을 의무적으로 열람해주셔야 하는데 혹시 방문 수령 가능하실까요? [피해자] 서울까지 제가 오라고요? 제가 아산 사는데 서울까지 그걸 가지러 가야 돼요? [정부기관 소속직원 사칭범] 혹시 방문이 조금 어려우시면 직장인이실까요? [피해자] 아니요. 집에 있긴 한데 보통 아산에서 서울까지 가지러 가기는 힘들지 않나요? [정부기관 소속직원 사칭범] 방문수령 어려우실 경우에는 저희가 공무원 인터넷 열람으로 안내해드리고 있거든요. 인터넷 사용 가능하실까요? [피해자] 네. [정부기관 소속직원 사칭범] 인터넷 창 켜주시고요. 일단은 불러드리고 열람 후에 저희가 고지해드릴 내용이 있어요. 인터넷 창 켜주시고 저한테 얘기해 주시면 바로 안내해 드릴게요. [피해자] 잠시만요. 네. 네. 켜어요. [정부기관 소속직원 사칭범] 인터넷 창 PC인가요? 모바일인가요? [피해자] PC요. [정부기관 소속직원 사칭범] 아 네, PC면 그 도메인 주소창에 소문자로 mn 그리고 숫자 8.kro. 마지막으로 kr이요. 들어가주시면 왼쪽 하단에 나의 사건 조회 보이실 거예요.</p>

<p>① 홈 화면-"메뉴" 클릭</p> 	<p>② 인증/보안 클릭</p> 	<p>③ 안심차단서비스 클릭</p> 
<p>④ 여신거래 차단 선택</p> 	<p>⑤ 약관 동의</p> 	<p>⑥ 신청 완료</p> 

① 홈 화면-“전체메뉴” 클릭



② 비대면 계좌개설 안심차단 클릭



③ 안심차단 신청



④ 오픈뱅킹 이용정보 확인



⑤ 동의서 작성



⑥ 결과 확인



붙임4

오픈뱅킹 안심차단서비스 신청방법(어카운트인포 앱)

① “내 금융 안심차단” 클릭



② 안심차단 신청 화면



③ 신청 가능 금융회사 확인



④ 오픈뱅킹 이용정보 확인



⑤ 가입 신청



⑥ 결과 확인



보이스피싱 피해시 대응요령

01 피해신고 및 지급정지 요청



경찰(112), 금감원(1332), 금융회사에 피해신고 및 지급정지 요청

02 개인정보 노출등록



개인정보 노출자 사고예방시스템
[<http://pd.fss.or.kr>] 사고등록

03 계좌 일괄 지급정지 신청



계좌정보통합관리서비스[www.payinfo.or.kr] 및 금융회사 영업점에서 일괄지급정지

04 명의도용 신고



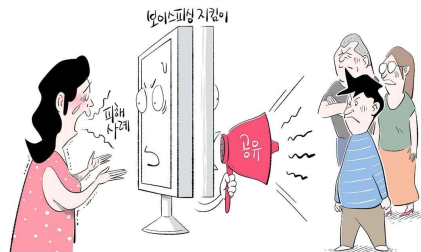
명의도용방지서비스[www.msafes.or.kr]에 명의도용 신고로 휴대전화 개설 방지

05 악성앱 삭제 및 휴대전화 초기화



악성코드 감염시 바로 삭제 및 휴대전화 초기화

06 피해사례 공유



보이스피싱지킴이 사이트에 접속하여 피해사례 공유

