

2차 소비쿠폰 신청 문자에는 URL이 없습니다. 절대 클릭하지 마세요

- 소비쿠폰 조화·신청 사칭 스미싱 소비자경보 상향(주의→경고) -

■ 소비자경보 2025 - 22 호

등급	주의	경고	위험
대상	금융소비자 일반		

소비자경보 내용

- 오는 9월 22일부터 시작되는 2차 민생회복 소비쿠폰 신청·지급과 관련하여, 심각한 스미싱* 피해 발생이 우려되는 상황입니다.
 - * 문자메시지(SMS)+피싱(Phishing)의 합성어로 악성앱 주소(url)이 포함된 휴대폰 문자(SMS)나 카카오톡 등 메시지를 대량 전송 후 이용자가 클릭하도록 유도, 개인정보 등을 탈취하는 수법
- 지난 1차 소비쿠폰 지급기간(7.21.~9.12.) 중 430건의 스미싱 문자, 정부24 사칭 악성앱 유포 사례 등을 확인하였으며, 2차 소비쿠폰 지급기간에도 다양한 스미싱 시도가 발생할 것으로 예상됩니다.
- 금융당국은 지난 '25.7월 소비자경보 발령(주의)에도 불구하고 스미싱 시도 사례가 지속 발생함에 따라 소비자경보 등급을 주의에서 경고로 상향하고, 금융소비자의 각별한 주의를 당부합니다.
 - 금융회사가 발송하는 2차 민생회복 소비쿠폰 관련 소비자 안내에는 URL이 일절 포함되어 있지 않으므로, 소비쿠폰 신청·지급 명목으로 전달받은 URL을 절대 클릭하지 마시기 바랍니다.

<소비자 유의사항>

- ① 문자메세지에 포함된 출처가 불분명한 인터넷주소(URL)는 절대 클릭 금지
- ② 민생회복 소비쿠폰 신청 명목으로 신분증 등 개인정보·금융정보 요구시 진행 중단
- ③ 휴대폰 보안 위험 자동 차단기능 설정(안드로이드)
- ④ 스미싱 문자 발신 전화번호 신고
- ⑤ 스미싱 피해 발생시 신속한 신고 및 지급정지 요청
- ⑥ 금융피해 예방을 위한 안심차단서비스, 명의도용 방지 서비스 적극 이용

1. 소비자경보 상향 배경

- 금융당국은 지난 '25.7.18. 민생회복 소비쿠폰 관련 스미싱 피해 예방을 위해 소비자경보(주의)를 발령한 바 있습니다.
 - 소비자경보 발령 이후 1차 소비쿠폰 지급기간(7.21.~9.12.) 중 430건의 스미싱 문자, 정부24 사칭 악성앱 유포 사례 등이 확인*되었습니다.
 - * 현재까지 소비쿠폰 관련 스미싱으로 인한 금융피해는 발생하지 않은 것으로 파악
- 2차 소비쿠폰 지급기간(9.22.~10.31.) 중에도 다양한 스미싱 시도가 발생할 것으로 예상됨에 따라, 소비자경보 등급을 주의에서 경고로 상향합니다.
 - 금융소비자에게서는 금융회사가 발송하는 2차 민생회복 소비쿠폰 관련 소비자 안내에는 URL이 포함되지 않는 점을 명심하시어, 소비쿠폰 신청·지급 명목으로 전달받은 URL을 절대 클릭하지 마시기 바랍니다.

소비쿠폰 관련 스미싱 사례

[민생회복 소비쿠폰 신청 안내]
귀하는 민생회복 소비쿠폰
신청 대상자에 해당되므로
온라인 센터(<https://www.kobis.or.kr>)
(<https://www.kobis.or.kr>)에서 지원하시기 바랍니다.

민생회복 소비쿠폰 신청이
접수되었습니다. 다시 한번 확인
부탁드립니다. (<https://www.kobis.or.kr>)

[정부24] 민생회복 소비쿠폰 지급금액
확인 및 신청방법 안내
<https://gov24.kr/apply>

소비쿠폰 관련 악성앱 유포 사례

<설치 유도 화면>



<악성앱 아이콘>



보조금24

<악성앱 실행화면>

2. 소비자 유의사항

□ 문자메세지에 포함된 출처가 불분명한 URL주소는 절대 클릭 금지

- 사기범이 보낸 출처가 의심스러운 URL주소 클릭시 악성앱이 설치되어 개인정보 유출 및 금융피해가 발생*할 수 있으니 절대 클릭하지 마세요

* 반드시 정식 앱마켓(구글플레이, 애플스토어 등)을 통해서만 앱을 다운로드하고, 신원이 확인되지 않은 사람이 보낸 앱 설치 요구는 절대로 응해서는 안됨

악성앱의 주요 기능

- ◆ 발신번호 조작 : 피해자 휴대폰에 표시되는 발신 전화번호를 112 등 임의의 번호로 조작
- ◆ 전화 가로채기 : 피해자 휴대폰의 통화 기능을 제어(강제수신·강제발신)
- ◆ 개인정보 탈취 : 휴대폰에 저장된 신분증, SMS, 연락처 등 모든 개인정보를 탈취
- ◆ 원격제어 : 사기범이 피해자 휴대폰의 모든 기능을 통제

□ 민생회복 소비쿠폰 신청 명목으로 신분증 등 개인정보·금융정보 요구시 진행 중단

- 사기범은 금융기관 등을 사칭해 가짜 웹페이지를 제작하여 정보를 탈취하므로 과도한 개인·금융정보 요구시 즉시 진행을 중단하고 공식 홈페이지 주소를 확인하세요

* 민생회복 소비쿠폰 관련 문의 : 정부민원안내센터 국민콜 110

가짜 웹페이지 사례

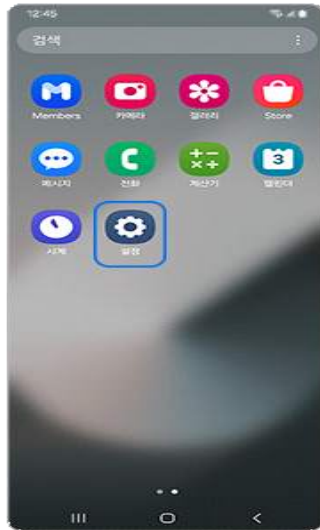
The screenshot shows a web page for 'IBK기업은행' (IBK Business Bank) with a '대출신청' (Loan Application) form. The form includes fields for '이름' (Name), '휴대폰' (Mobile Phone), '주민번호' (Resident Number), '직장명/사업자명' (Company Name), '연봉/매출' (Annual Salary/Sales), '필요금액' (Required Amount), and '대출신청사항' (Loan Application Details). A '신청하기' (Apply) button is at the bottom.

The screenshot shows a web page with a 'VISA' logo and a '신분증을 촬영해주세요.' (Please scan your ID card) instruction. It features a '나의 정보 조회' (Check My Information) section with fields for '이름' (Name), '생년월일' (Date of Birth), and '휴대폰번호' (Mobile Number), along with a '조회하기' (Check) button. On the right, there is a '성함' (Name) field and a '연락처' (Contact) field. At the bottom, there are social media icons and a '신청하기' (Apply) button.

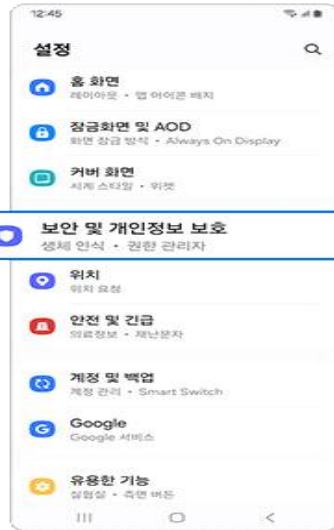
□ 휴대폰 보안 위험 자동 차단기능 설정(안드로이드)

- 악성앱 설치로 인한 전화 강제 수·발신 등 통화 제어, SMS·연락처·사진 등 정보 탈취 방지를 위해 사전에 휴대폰 보안설정을 강화하세요

휴대폰 보안설정 강화(안드로이드)



1. 스마트폰 '설정' 앱 클릭



2. '보안 및 개인정보 보호' 메뉴 접속



3. '보안 위험 자동 차단' 활성화

- 악성앱을 이미 설치했다면 ①모바일 백신앱(V3, 시티즌코난 등)으로 검사 후 삭제, ②휴대폰 초기화, ③한국인터넷진흥원 상담센터(☎118)에 도움을 요청하세요

□ 스미싱 문자 발신 전화번호 신고

- 스미싱 문자를 받은 경우 발신 전화번호 이용 중지를 위해 보이스피싱 통합신고대응센터*에 제보해 주세요

* 포털에서 **통합신고대응센터** 검색 (홈페이지 주소 : www.counterscam112.go.kr)

□ 스미싱 피해 발생시 신속한 신고 및 지급정지 요청

- 자금 이체 등 금융 피해가 발생한 경우 ①본인 또는 사기범 계좌의 금융회사나 ②보이스피싱 통합신고대응센터(112)로 지체없이 신고하여 지급 정지를 요청하세요
- 개인정보 유출로 인한 추가 피해 예방을 위해 『개인정보 노출자 사고 예방 시스템*』, 『본인계좌 일괄지급정지 서비스**』를 활용하세요

* 금융감독원 홈페이지 파인(pdfss.or.kr)에서 신청 가능, 신청시 신규 계좌개설 카드 발급 등이 제한

** 금융결제원 홈페이지 야카운트인포(www.payinfo.or.kr)에서 신청 가능 본인계좌에서의 모든 출금거래 정지

□ 금융피해 예방을 위한 안심차단서비스, 명의도용 방지 서비스 적극 이용

- 개인정보 유출 등으로 본인이 모르는 무단 대출, 신규 계좌개설을 사전에 차단할 수 있도록 여신·비대면계좌개설 안심차단 서비스를 적극 이용하세요
 - 거래중인 금융회사 영업점*을 방문하거나, 은행 모바일 앱을 통해 간편하게 신청할 수 있습니다.
- * 은행, 저축은행, 농협, 수협, 신협, 새마을금고, 산림조합, 우체국
- 또한 본인 모르게 개통된 휴대폰을 조회하거나 추가 개통을 차단하기 위해 『명의도용 방지서비스(www.msafes.or.kr)』를 이용해보세요

< 명의도용방지 서비스(Msafer) >

로그인

- 인증서 로그인을 통한 서비스 이용을 위해서는 약관 동의가 필요합니다.
- 동의하시기 전 이용약관 안내문을 반드시 읽어주세요.
- 회원의 신상정보는 [개인정보보호법]에 의해 철저하게 보호됩니다.

서비스 이용에 대한 약관 동의 ☐ 전체 약관 동의

- ☐ (필수) 서비스 이용 약관 - [자세히보기](#)
- ☐ (필수) 개인정보 수집 및 이용 동의 - [자세히보기](#)
- ☐ (필수) 제3자 제공동의 - [자세히보기](#)
- ☐ (필수) 금융사실정보 처리동의 - [자세히보기](#)

공동인증서 **금융인증서**

공동금융 인증서를 통한 본인확인 후 서비스 이용이 가능합니다.
로그인 관련 도움말이나 다른 사용자가 자주 찾는 질문을 확인해보세요.

- 공동금융 인증서가 없는 경우 서비스 이용방법
- 자세히보기
- 비밀번호 및 위독인(예외국인) 인증서 발급 방법
- 자세히보기

1. www.msafes.or.kr 에서 '가입사실현황조회서비스' 클릭

서비스 구분	사업자	가입인	상태	고객센터
이동통신	한계	2		
이동통신	KT	1		1588-0010
이동통신	SK/통신KT(이동통신)	1		1599-0999

2. 공동인증서를 통하여 로그인

가입제한서비스

이동통신 신규가입 및 번호이동, 명의이전, 기기변경(LGU+만 해당)을 내 통지 없이 할 수 있도록 사전에 차단하는 서비스로 통신사 대리점에 직접 방문하지 않고 온라인상에서 신청할 수 있는 편리한 서비스입니다.

본 서비스는 사용자가 신청한 가입제한제 정보에 통신사에 연동하여, 가입제한 및 해제 처리는 통신사에서 담당하시니 오류 발생 시 해당 통신사 고객센터에 확인하시기 바랍니다.

가입을 제한한 이동통신사

- 전체
- SKT
- KT (일명론 포함)
- LG U+ (일명론 포함)
- KCT
- 새콤 텔레콤
- LG헬로비전 (KT)
- SKT 알뜰폰

[제약해제](#)

3. 조회 결과 명의도용으로 인한 개통이 확인되면 해당 통신사에 연락하여 회신 해지신청 및 명의도용 신고

4. '가입제한서비스'를 통하여 통신사별로 휴대폰 신규 가입을 사전 차단 가능

※ 명의도용방지 서비스는 휴대폰 PASS앱 및 카카오뱅크 앱에서도 신청 가능


담당 부서 <총괄>	금융위원회	책임자	서기관	김태훈 (02-2100-2970)
	금융안전과	담당자	사무관	유은지 (02-2100-2974)
<공동>	금융감독원	책임자	국 장	정재승 (02-3145-8150)
	금융사기대응총괄팀	담당자	팀 장	김태근 (02-3145-8130)

- 정부, 카드사 및 지역화폐사 등은 **온라인 신청 시** 문자메시지를 악용하는 개인정보 피해(스미싱)를 예방하기 위해 국민께 **URL, 링크 등이 포함된 문자메시지를 보내지 않습니다.**

[민생회복 소비쿠폰 관련 스미싱 주의 안내 문자메시지]

민생회복 소비쿠폰 신청·지급시기와 맞물려 정부나 카드사 등을 사칭하여 민생회복 소비쿠폰 지급대상·금액, 카드 사용 승인, 충전 등 안내 정보를 가장하여 의심스러운 인터넷 주소 클릭을 유도(앱 설치 유도)하는 스미싱 시도가 빈번하게 일어날 것으로 예상됩니다. 원칙적으로 정부 및 카드사 등은 민생회복 소비쿠폰 온라인 신청 시 피해를 예방하기 위해 국민께 URL, 링크 등이 포함된 문자메시지를 보내지 않습니다. 그러므로, 문자 속 인터넷 주소(URL)를 클릭하거나, 전화를 할 경우 피해를 입을 수 있으니 각별히 주의하시기 바라며 아래 유의 사항을 반드시 숙지하시기 바랍니다.

- ① 발신인이 불명확하거나 의심스러운 인터넷 주소(URL)를 포함한 문자는 절대 클릭하지 마세요.
- ② 의심 문자를 받았거나, 악성앱 감염이 의심되는 경우, 한국인터넷진흥원 118센터(☎118)로 신고하시기 바랍니다.



민생회복 소비쿠폰 지급을 사칭한 스미싱·스팸문자를 주의하세요!

정부 및 카드사 등은 민생회복 소비쿠폰 온라인 신청 시 피해를 예방하기 위해 국민께 URL, 링크 등이 포함된 문자메시지를 보내지 않습니다.

[민생회복 소비쿠폰 신청 안내]
귀하는 민생회복 소비쿠폰 신청 대상자에 해당되므로 온라인 센터(<https://...>)에서 지원하시기 바랍니다.


민생회복 소비쿠폰 신청이 접수되었습니다.
다시 한번 확인 부탁드립니다.
(<https://url.kr/25yp3q>)



1. 스미싱 문자가 아닌지 확인합니다.
문자 뒤에 인터넷주소가 있으면 정상 문자인지 의심해봐야 합니다.

2. 출처가 불분명한 문자 내 인터넷주소(URL)를 누르지 마세요!

* 스미싱이란? 악성 앱 주소가 포함된 휴대폰 문자를 전송 후 이용자가 앱 설치 또는 전화를 하도록 유도하여 금융정보·개인정보 등을 탈취하는 수법



신고전화 한국인터넷진흥원 118 상담센터

* 자료 : 과기정통부(한국인터넷진흥원)