

민생회복 소비쿠폰 신청 문자에는 인터넷주소(URL)가 없습니다. 절대 클릭하지 마세요.

- 민생회복 소비쿠폰 조화·신청 사칭 스미싱 소비자경보 발령 -

■ 소비자경보 2025 - 17호

등급	주의	경고	위험
대상	금융소비자 일반		

소비자경보 내용

- 7월 21일부터 시작되는 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
 - 민생회복 소비쿠폰 안내를 위한 정부·은행·카드사 등의 공식 문자 메시지는 URL이 일절 포함되어 있지 않습니다.
- 민생회복 소비쿠폰 신청·지급 안내 등의 내용으로 정부·금융회사를 사칭한 문자메시지 URL 접속시 개인정보 노출 및 금융피해가 발생할 수 있어 절대 클릭하지 마시기 바랍니다.
 - 아울러 금융당국은 민생회복 소비쿠폰 사칭에 이용된 전화번호를 신속히 이용 중지하고, 피해 발생현황을 면밀히 점검할 예정입니다.

<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 발령 배경

- 7월 21일부터 전국민을 대상으로 개시되는 민생회복 소비쿠폰 신청·지급과 관련한 심각한 스미싱 피해 발생이 우려*되는 상황입니다.

* 과거 코로나19 재난지원금 신청·지급과 관련 스미싱이 성행

- 출처가 의심스러운 URL주소를 클릭할 경우 피싱사이트로 연결되거나, 악성앱이 설치되어 정보 노출 및 금융피해가 발생할 수 있습니다.

스미싱 사례



[Web발신]
[긴급재난지원금]
신용,체크카드 긴급재난지원금
모바일로 간단하게 신청하세요
<http://n.../covid-19>



[Web발신]
[재난지원]
코로나19 재난지원금
선별대상, 선별지급
지급대상 확인하기
<http://n.../corona>



[Web발신]
긴급생활비 지원사업이
접수되었습니다 다시한번 확인
부탁드립니다 www...

- 이에 금융당국은 민생회복 소비쿠폰과 관련한 소비자 피해 예방을 위해 소비자 유의사항을 안내하고 소비자경보(주의)를 발령합니다.

2. 금융당국의 대응

- 금융당국은 은행 및 카드업권에 소비자 대상 소비쿠폰 관련 안내시 URL 링크를 포함하지 않도록 지도하였으며,
- 금융회사 영업점·홈페이지·콜센터 등을 통해 소비자에게 민생회복 소비쿠폰 관련 스미싱 피해예방 및 피해발생시 행동요령 등을 안내토록 하였습니다.

[소비쿠폰 스미싱 예방 소비자 안내 강화조치]

- ① (영업점) 창구·대기 공간·ATM 등 영업점 내 홍보 포스터·리플렛 게시
- ② (홈페이지·모바일앱) 배너 또는 팝업, 게시판을 통해 유의사항 안내
- ③ (콜센터) ARS 연결 전 안내 멘트에 소비쿠폰 스미싱 주의 안내(카드사)
- ④ (문자메세지 등) 문자·알림톡 발송시 소비쿠폰 관련 URL 클릭 금지 홍보

- 또한, 금융당국은 앞으로 민생회복 소비쿠폰 조회·신청 사칭에 이용된 전화번호를 신속히 이용 중지할 예정이며,
- 은행·카드업권 FDS 모니터링을 강화하여 소비자 피해 발생현황을 면밀히 점검해 나갈 계획입니다.

3. 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, 수상한 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

□ 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 URL을 확인하세요

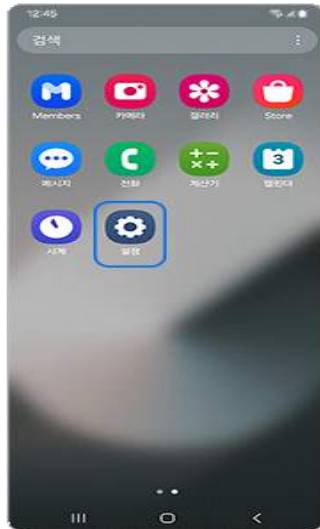
* 민생회복 소비쿠폰 관련 문의 : 정부민원안내센터 국민콜 110

가짜 웹페이지 사례

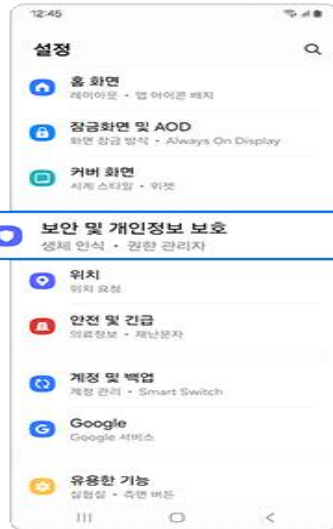
□ 휴대폰 보안 위험 자동 차단기능 설정(안드로이드)

- 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(www.counterscam112.go.kr)에 제보해 주세요

□ 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 유출시 추가 피해 예방을 위해 금융감독원 금융소비자 정보포털 “파인”의 『개인정보 노출자 사고예방 시스템*』을 활용하세요

* 신청인이 직접 개인정보를 등록하면 신규 계좌개설, 신용카드 발급 등이 제한됨

□ 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
- 비밀번호 및 외국인(재외국민) 인증서 발급 방법

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(SKT 이동통신)	1		1599-0999

2. 공동인증서를 통하여 로그인

가입을 제한한 이동통신사

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

[제한해제](#)

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

※ 명의방지도용 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://url.kr/25yp3q>)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)