금융위원회 보도자료 금융감독원

보도시점 2025.9.22.(월) 조간 배포 2025.9.19.(금) 17:00

2차 소비쿠폰 신청 문자에는 URL이 없습니다. 절대 클릭하지 마세요

- 소비쿠폰 조회·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·지급**과 관련하여, 심각한 **스미싱*** **피해 발생**이 **우려**되는 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 **430건**의 **스미싱 문자**, 정부24 사칭 **악성앱 유포 사례** 등을 **확인**하였으며, 2차 소비쿠폰 지급기간에도 **다양한 스미싱 시도**가 **발생**할 것으로 **예상**됩니다.

□ 금융당국은 지난 '25.7월 소비자경보 발령(주의)에도 불구하고 스미싱 시도 사례가 지속 발생함에 따라 **소비자경보 등급**을 주의에서 **경고**로 **상향**하고, 금융소비자의 **각별한 주의**를 **당부**합니다.

○ 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 예방**을 위해 **소비자경보(주의)**를 **발령**한 바 있습니다.

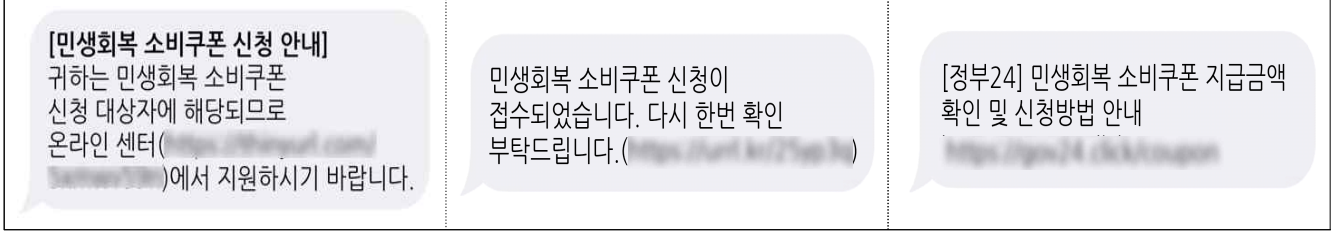
○ 소비자경보 발령 이후 **1차 소비쿠폰 지급기간**(7.21.~9.12.) 중 **430건**의 **스미싱 문자, 정부24 사칭 악성앱 유포 사례** 등이 **확인***되었습니다.

* 현재까지 소비쿠폰 관련 스미싱으로 인한 금융피해는 발생하지 않은 것으로 파악

□ 2차 소비쿠폰 지급기간(9.22.~10.31.) 중에도 **다양한 스미싱 시도**가 **발생**할 것으로 **예상**됨에 따라, **소비자경보 등급**을 **주의**에서 **경고**로 상향합니다.

○ 금융소비자께서는 금융회사가 발송하는 **2차 민생회복 소비쿠폰** 관련 **소비자 안내**에는 **URL**이 **포함되지 않는 점**을 **명심**하시어, 소비쿠폰 신청·지급 명목으로 전달받은 URL을 **절대 클릭하지 마시기 바랍니다.**

소비쿠폰 관련 스미싱 사례



소비쿠폰 관련 악성앱 유포 사례

<설치 유도 화면>

<악성앱 아이콘>

<악성앱 실행화면>

2. 소비자 유의사항

□ 문자메세지에 포함된 출처가 불분명한 URL주소는 절대 클릭 금지

○ 사기범이 보낸 **출처가 의심스러운 URL주소** 클릭시 **악성앱**이 설치되어 **개인정보 유출** 및 **금융피해**가 발생*할 수 있으니 **절대 클릭하지 마세요**

* 반드시 **정식 앱마켓(구글플레이, 애플스토어 등)**을 통해서만 앱을 다운로드하고, **신원이 확인되지 않은 사람**이 보낸 **앱 설치 요구**는 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 웹페이지**를 **제작**하여 **정보**를 **탈취**하므로 과도한 **개인·금융정보 요구시 즉시 진행**을 **중단**하고 **공식 홈페이지 주소**를 확인하세요

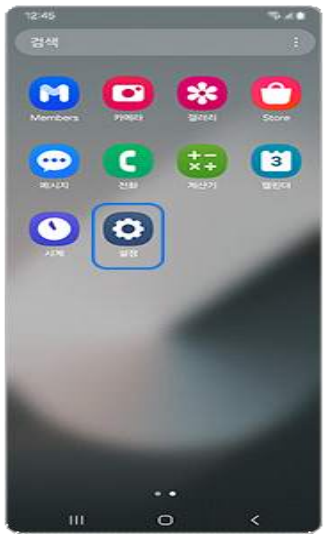
* 민생회복 소비쿠폰 관련 문의 : 정부민원안내센터 국민콜 110

가짜 웹페이지 사례

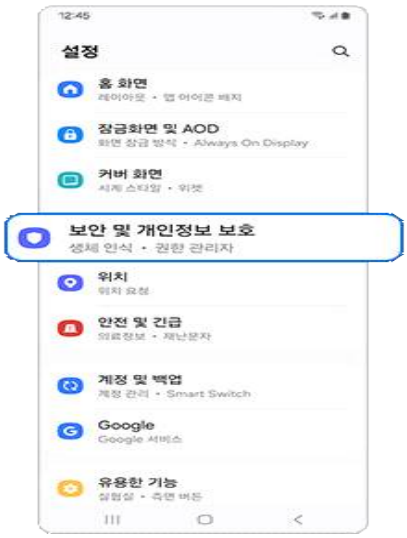
□ 휴대폰 보안 위험 자동 차단기능 설정(안드로이드)

○ 악성앱 설치로 인한 **전화 강제 수·발신 등 통화 제어, SMS·연락처·사진 등 정보 탈취 방지**를 위해 **사전에 휴대폰 보안설정**을 **강화**하세요

휴대폰 보안설정 강화(안드로이드)



1. 스마트폰 '설정' 앱 클릭



2. '보안 및 개인정보 보호' 메뉴 접속

3. '보안 위험 자동 차단' 활성화

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

□ 스미싱 문자 발신 전화번호 신고

○ 스미싱 문자를 받은 경우 **발신 전화번호 이용 중지**를 위해 **보이스피싱 통합신고대응센터***에 **제보**해 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 ❶**본인 또는 사기범 계좌**의 **금융회사**나 ❷**보이스피싱 통합신고대응센터**(112)로 **지체없이 신고**하여 **지급 정지**를 **요청**하세요

○ 개인정보 유출로 인한 **추가 피해 예방**을 위해 **『개인정보 노출자 사고예방 시스템*』**, **『본인계좌 일괄지급정지 서비스**』를 **활용**하세요

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

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

□ 금융피해 예방을 위한 안심차단서비스, 명의도용 방지 서비스 적극 이용

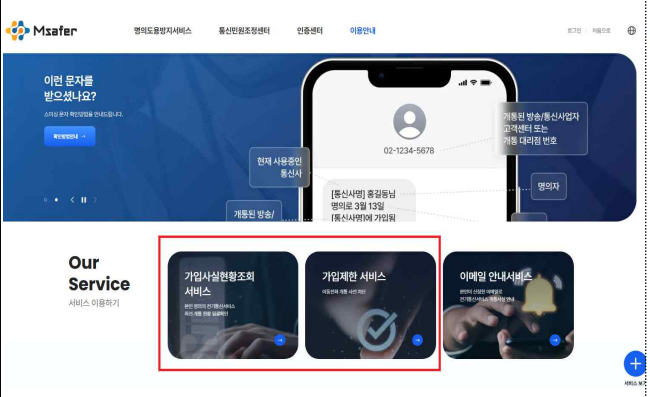
○ **개인정보 유출** 등으로 본인이 모르는 **무단 대출, 신규 계좌개설**을 **사전에 차단**할 수 있도록 **여신·비대면계좌개설 안심차단 서비스**를 **적극 이용**하세요

- 거래중인 금융회사 **영업점***을 **방문**하거나, **은행 모바일앱**을 통해 **간편하게 신청**할 수 있습니다.

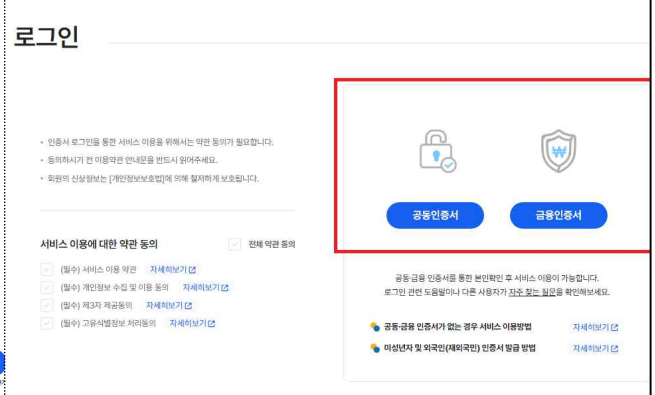
  * 은행, 저축은행, 농협, 수협, 신협, 새마을금고, 산림조합, 우체국

○ 또한 **본인 모르게 개통된 휴대폰을 조회**하거나 **추가 개통을 차단**하기 위해 **『명의도용 방지서비스**(www.msafer.or.kr)』를 **이용**해보세요

< 명의도용방지 서비스(Msafer) >



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



2. 공동인증서를 통하여 로그인

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

붙 임 **민생회복 소비쿠폰 관련 스미싱 피해예방 요령**

□ 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)을 클릭하거나, 전화를 할 경우 피해를 입을 수 있으니 각별히 주의하시기 바라며 아래 유의 사항을 반드시 숙지 하시기 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.

* 자료 : 과기정통부(한국인터넷진흥원)