



보도시점 (온라인) 2025. 9. 14.(일) 12:00  
(지 면) 2025. 9. 15.(월) 조간

## URL 링크가 제공되는 2차 소비쿠폰 문자와 알림은 100% 사기입니다

- 정부 및 금융기관 등은 안내 메시지에 URL을 절대 포함하지 않음
- 배너 링크, 앱푸쉬 기능도 제공하지 않으니 절대 누르지 말 것을 당부

- 정부는 ‘2차 민생회복 소비쿠폰’ 신청·지급 시기와 맞물려 정부·카드사·은행 등을 사칭해 지급대상·금액 안내, 카드 사용 승인, 신청 등의 다양한 스미싱\* 공격이 예상됨에 따라 특별한 주의를 당부했다.

\* 스미싱(smishing) : 문자메시지(SMS)와 피싱(Phishing)의 합성어로 악성 앱 주소가 포함된 휴대폰 문자(SMS)를 대량 전송 후 이용자가 악성 앱을 설치하거나 전화를 하도록 유도하여 금융정보·개인정보 등을 탈취하는 수법

- 1차 민생회복 소비쿠폰과 관련해 현재까지 탐지·대응한 스미싱 건수는 총 430건이며 스미싱 유포에 따른 피해사실은 없었다.
- 1차 소비쿠폰 관련 스미싱 유형 분석결과, 대부분 불법 도박사이트 광고 및 접속유도였으나, 개인정보 탈취형 스미싱 악성 앱 유형도 탐지됐다.
  - 개인정보 탈취형 스미싱 악성 앱은 감염 후 주변인들에게 스미싱 문자를 재유포하는 기능이 탑재되어 이용자들의 더욱 특별한 주의가 요구된다.
- 한편, 스미싱 피해를 사전 예방하기 위해 정부·카드사·지역화폐사는 2차 민생회복 소비쿠폰과 관련해 ‘인터넷 주소 바로가기(URL)’가 포함된 문자 및 SNS 안내문자를 일절 발송하지 않을 예정이다.
- 또한, 정부·카드사·지역화폐사는 인터넷 주소 바로가기(URL)뿐만 아니라, 이와 유사한 기능을 하는 배너 링크 및 앱푸쉬 기능도 절대 제공하지 않을 방침이다.

□ 만약 스미싱 의심 문자를 받았거나 문자 내 인터넷 주소 바로가기(URL)를 클릭한 이후 악성 앱 감염 등이 의심되는 경우, ‘스미싱 피해예방 대응 요령’을 참고해 24시간 무료로 운영하는 한국인터넷진흥원 118상담센터 (☎118)로 신고하고 상담받을 수 있다.

※ 민생회복 소비쿠폰 이용 일반문의 : ☎110

□ 정부는 2차 민생회복 소비쿠폰 신청·지급 전 9월 12일(금)부터 각 통신사 명의로 ‘스미싱 피해예방 문자’를 순차 발송해 스미싱에 대한 이용자의 경각심을 높인다.

○ 민생회복 소비쿠폰 비대면 신청 시 신청페이지에 스미싱 ‘주의’ 안내 문구를 포함하고, 어르신 등 디지털 취약계층을 위해 은행과 지방자치단체 (주민센터)를 통한 대면 신청 시 스미싱 ‘주의’ 안내도 병행할 예정이다.

○ 또한, 금융감독원·경찰청·한국인터넷진흥원 등을 통해 스미싱 공격에 대한 모니터링을 강화하고, 피해신고 시 즉시 수사에 착수하는 등 신속 대응 체계도 지속 운영할 계획이다.

|       |                           |     |     |                    |
|-------|---------------------------|-----|-----|--------------------|
| 담당 부서 | 행정안전부<br>디지털보안정책과         | 책임자 | 과 장 | 조원갑 (044-205-2741) |
|       |                           | 담당자 | 사무관 | 박병호 (044-205-2747) |
|       | 과학기술정보통신부<br>사이버침해대응과     | 책임자 | 과 장 | 최광기 (044-202-6460) |
|       |                           | 담당자 | 사무관 | 김성환 (044-202-6461) |
|       | 방송통신위원회<br>디지털이용자기반과      | 책임자 | 과 장 | 최충호 (02-2110-1520) |
|       |                           | 담당자 | 사무관 | 이명심 (02-2110-1522) |
|       | 금융위원회<br>금융안전과            | 책임자 | 서기관 | 김태훈 (02-2100-2970) |
|       |                           | 담당자 | 사무관 | 유은지 (02-2100-2974) |
|       | 경찰청<br>사이버범죄수사과           | 책임자 | 총 경 | 임욱성 (02-3150-1605) |
|       |                           | 담당자 | 경 정 | 조성실 (02-3150-1658) |
|       | 금융감독원<br>금융사기대응단          | 책임자 | 국 장 | 정재승 (02-3145-8150) |
|       |                           | 담당자 | 팀 장 | 김태근 (02-3145-8130) |
|       | 한국인터넷진흥원(KISA)<br>국민피해대응단 | 책임자 | 단 장 | 이동연 (02-405-4900)  |
|       |                           | 담당자 | 팀 장 | 김은성 (02-405-4940)  |



## 참고

## 소비쿠폰 관련 스미싱 유형 및 피해예방 대응요령

### ① 스미싱 유형 예시

#### 인터넷주소(URL) 연결 링크 유형

지원금 신청이 접수되었습니다. 다시 한번 확인 부탁드립니다.  
<https://url.kr/25yp3q>

#### 배너 링크 유형(클릭 시 앱으로 이동)

알림톡 도착

**민생회복 소비쿠폰  
지금 대상자 알림**

민생회복  
소비쿠폰 지금 대상자로 확인되어  
안내드려요.

55만원

✓ 지원금액 : 1인당 15~55만원,  
소득별 맞춤형 지원 및 단계적 지급

✓ 신청 및 지급 기간:  
- 1차: 2025.07.21.(월) ~ 09.12.(금)  
- 2차: 2025.09.22.(월) ~ 10.31.  
(금)

자세한 사항은 버튼을 통해  
확인해주세요.

자세히 보기

#### 앱푸시 유형(클릭 시 앱으로 이동)

LG U+

7월 21일 월요일

8:30

[공지] 1차 민생회복 소비쿠폰  
잠시후 오전 9시부터 신청가능합니다.  
※ 본 푸시는 서비스 운영 관련 공지사항으로  
마케팅수신동의 여부와 관계없이 발송됩니다.

지금

## ② 스미싱 피해예방 대응요령

- 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]

2차 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 클릭 하지 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**