



보도시점 (온라인) 2025. 7. 10.(목) 12:00
(지면) 2025. 7. 11.(금) 조간

소비쿠폰 안내 문자에 URL 링크는 100% 사기입니다

- 정부 및 금융기관 등은 안내 메시지에 URL, 링크를 포함하지 않으니 절대 누르지 마세요
- 결제사기 등 의심 문자는 118 신고

- 정부는 ‘민생회복 소비쿠폰’ 신청·지급 시기와 맞물려 지급대상·금액 안내, 카드 사용 승인, 신청 등의 내용으로 정부·카드사·은행 등을 사칭한 문자 결제사기(스미싱)*가 증가할 것으로 예상되어 이용자들의 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
- 민생회복 소비쿠폰은 카드사 앱·누리집, 콜센터·ARS와 지역사랑상품권 앱·누리집 등에 접속해 비대면(온라인)으로 신청하거나, 카드와 연계된 은행 및 지방자치단체(주민센터)에서 대면(오프라인)으로 신청해야 한다.
- 정부는 민생회복 소비쿠폰 비대면 신청 시 신청페이지에 스미싱 ‘주의’ 안내문구를 포함하고, 어르신 등 디지털 취약계층을 위해 은행 및 지방자치단체(주민센터)를 통한 대면 신청 시 스미싱 ‘주의’ 안내도 같이 진행할 예정이다.
- 이용자는 스미싱 피해예방을 위해 국민비서 사전 알림서비스를 적극 활용하고, 국민비서·카드사·은행 외에 출처가 불분명한 SNS 안내 문자를 받은 경우, 또는 정부·카드사를 사칭한 의심스러운 인터넷 주소가 포함된 SNS 안내 문자를 받은 경우 한 번 더 유심히 살펴보아야 한다.

- 특히, 스미싱 피해를 사전 예방하기 위해 정부·카드사·지역화폐사는 민생회복 소비쿠폰과 관련하여 ‘인터넷 주소 바로가기(URL·링크)’가 포함된 문자 및 SNS는 일절 발송하지 않을 예정이다.
- 따라서, 공식 문자가 아닌 의심 문자로 판단될 경우 클릭하지 말고 바로 삭제하고, 문자를 열람했다면 문자 내 인터넷주소(URL)를 절대 클릭하지 않도록 신중해야 한다.
- 아울러, 스미싱 의심 문자를 받았거나 문자 내 인터넷 주소(URL)를 클릭한 이후 악성 앱 감염 등이 의심되는 경우 ‘스미싱 피해발생 시 행동요령[참고]’을 참고해 24시간 무료로 운영하는 한국인터넷진흥원 118상담센터(☎118)에서 상담받을 수 있다.

※ 민생회복 소비쿠폰 이용문의 : ☎110

- 정부는 민생회복 소비쿠폰 신청·지급 전 7월 14일(월)부터 각 통신사 명의로 ‘스미싱 피해예방 문자’를 순차 발송해 스미싱에 대한 이용자의 경각심을 높이고자 한다.
- 또한, 정부 및 지방자치단체 누리집 등에 민생회복 소비쿠폰 신청·지급 안내 시 주의사항을 게시하고,
- 국민비서 알림서비스(네이버, 카카오, 토스 등 17개사)를 활용해, 민생회복 소비쿠폰 신청·지급 안내 시 ‘스미싱 주의 메시지’를 같이 발송하는 등 다양한 창구를 통해 스미싱 주의 사항을 안내할 예정이다.
- 정부는 문자결제사기(스미싱)를 선제적으로 대응하기 위해 금융감독원·경찰청·한국인터넷진흥원을 통해 스미싱 발생 및 신고 현황 모니터링을 강화한다.
- 또한, 신고·접수된 문자결제사기(스미싱) 정보를 분석하고 관련 악성 누리집(링크) 등 유포지를 즉시 차단하는 체계를 구축하는 한편, 피해 신고 접수 시 신속하게 수사에 착수하는 등 이용자의 피해를 최소화하기 위해 총력을 다한다는 방침이다.

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



① 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)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://urrl.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

2 스미싱 피해발생 시 행동요령

8단계로 알아보는 스미싱 피해 대처법

스미싱 당했다면 이렇게!

KISA

'비행기 모드'로 전환 ✈

휴대전화 배터리가 평소보다 빨리 닳거나
발신한 적 없는 문자 또는 전화가 발생되어 있거나
작동 오류, 파일 손상 등의 증상이 나타나면
비행기 모드로 전환하고 와이파이 기능을 끄세요.

KISA

악성 앱 찾아 삭제 🚫

모바일 백신에서 '악성 앱 검사'를 이용하거나
가장 최근에 설치된 앱을 확인해 악성 앱을 찾아 삭제하세요.
확장자가 '.apk'인 파일도 삭제해야 안전합니다.

KISA

공인인증서는 폐기하고 재발급

공인인증서, 보안카드 등을 폐기하고 재발급받으세요.
금융거래에 필요한 정보를 사전협이나 메모장에
기록했다면 모두 폐기하고 재발급받아야 해요.

KISA

계좌 출금·지급 정지 🛑

'본인계좌 일괄지급정지 서비스'를 신청하세요.
금융사 영업점에 방문 또는 고객센터와 전화,
온라인의 경우, 금융감독원의 계정정보통합서비스를
이용할 수 있습니다.

KISA

명의도용 막기 🗑

금융감독원 '개인정보 노출사사고예방시스템'에 접속해
개인정보 노출 사실을 등록하세요.
한국신용정보원 응성 안내 서비스(☎1544-6640)를 이용하면
대출 여부를 확인해 지급 정지를 신청할 수 있어요.

KISA

금전 피해 없어도 신고 🚒

피해 신고 및 구제 절차는 경찰청(☎112),
계좌관리 등 금융 피해 예방 상담은 금융감독원(☎1332),
스캠 차단은 한국인터넷진흥원(☎118)으로 전화해 주세요.
전자금융사기 통합신고대응센터로 신고하시면
한 번에 도움을 받을 수 있습니다.

KISA

금전피해가 있다면 구제 신청

휴대전화 소액결제 방식으로 돈을 편취당했거나
휴대전화에 저장된 개인정보·금융정보를 탈취당했을 때
즉시신고(☎112)하고 구제 신청하세요.

KISA

스미싱 문자 재유포 차단하기

'엠세이퍼' 가입 및 이용 중인 통신사의
'번호도용차단서비스'를 가입해 내 번호로
스미싱 문자가 재유포 되는 것을 차단해 주세요.

KISA

2차 피해 최소화하자!

"스미싱 당했을 때
당황하지 말고 대처하세요~"

KISA

* 자료 : 과기정통부(한국인터넷진흥원)