관계부처합동 보도자료 다시 대한민국! 새로운 국민의 나라

보도시점 온라인 : 2025. 1. 19.(일) 12:00
지 면 : 2025. 1. 20.(월) 조간
배포 2025. 1. 17.(금) 18:00

# 설 명절을 겨냥한 문자사기(스미싱) 등 사이버사기 주의!

- 연말정산·설 선물 배송 사칭하는 스미싱 문자 증가, 출처가 불분명한 문자의 인터넷 주소(URL)·전화번호 클릭 주의
- 지나치게 저렴하게 판매하는 온라인 쇼핑몰 상품은 구매에 앞서 사업자 정보 등을 반드시 확인하고 거래 전 사기 피해 신고 여부를 먼저 확인

**과학기술정보통신부**(장관 유상임, 이하 '과기정통부'), **방송통신위원회**(위원장 직무대행 김태규, 이하 '방통위'), **금융위원회**(위원장 김병환, 이하 '금융위'), **경찰청**(청장직무대행 이호영), **한국인터넷진흥원**(원장 이상중, 이하 'KISA'), **금융감독원**(원장 이복현, 이하 금감원)은,

설 연휴 기간을 틈타 연말정산, 과태료·범칙금 조회 등 공공기관을 사칭하거나, 온라인 송금, 상품권 지급 등 명절 선물을 위장하여 금전 탈취를 시도하는 **문자사기(스미싱*)와**, 배송 지연, 물량 부족으로 가장한 비대면 직거래 사기·허위 쇼핑몰 등 각종 **사이버 사기** 피해가 우려되므로 각별한 주의를 당부했다.

* 문자메시지(SMS)와 피싱(Phishing)의 합성어. 악성 앱 주소가 포함된 휴대폰 문자를 전송하여 이용자가 악성 앱 설치 또는 통화를 유도하여 금융정보·개인정보 등을 탈취하는 수법(보이스피싱, 전자상거래 사기 등에 악용)

## < 스미싱 주의보>

악성앱 유포 문자 발송으로 인한 **피해액이 크게 증가**하고 있으며, 특히 악성앱 감염을 유도하기 위해 **정부·공공기관을 사칭**하거나 일상생활에서 주로 사용되는 **SNS 등 플랫폼 기업을 사칭**하여 계정정보를 탈취하려는 문자 발송의 비중이 매우 높다.

관계 당국에서 탐지한 문자사기 현황('22년 ~ '24년)을 살펴보면, **과태료·범칙금 등 정부·공공기관을 사칭하는 유형이 총 162만여 건(59.4%)으로 가장 많은 비율**을 차지하였고, SNS 기업을 사칭한 계정탈취 유형이 46만여 건(16.9%)으로 눈에 띄게 급증하였다. 이어 청첩장, 부고장 등 지인 사칭형도 42만여 건(15.5%)으로 증가하였다.

**< 문자사기(스미싱) 신고(접수)·차단 현황 >**

(단위: 건)

| 구 분 | 2022년 | 2023년 | 2024년 | 합 계 |
|---|---|---|---|---|
| 전 체 | 37,122 | 503,300 | 2,196,469 | 2,736,891 |
| 기관사칭유형 | 17,726 (47.8%) | 350,010 (69.5%) | 1,258,228 (57.3%) | 1,625,964 (59.4%) |
| 지인사칭유형 | 4 (0.0%) | 59,565 (11.8%) | 363,622 (16.6%) | 423,191 (15.5%) |
| 투자·상품권 유형 | 110 (0.3%) | 164 (0.1%) | 21,088 (1.0%) | 21,362 (0.8%) |
| 택배유형 | 19,214 (51.8%) | 91,159 (18.1%) | 29,299 (1.3%) | 139,672 (5.1%) |
| 계정탈취유형 | 0 (0.0%) | 2,315 (0.5%) | 459,707 (20.9%) | 462,022 (16.9%) |
| 기타 | 68 (0.2%) | 87 (0.0%) | 64,525 (2.9%) | 64,680 (4.0%) |

※ 자료출처 : 과기정통부·한국인터넷진흥원

정부는 이번 설 명절을 전후해 가족 친지 간 차량 이동량 증가를 틈타 **범칙금, 과태료 부과 조회 등을 유도하거나 연초 연말정산 기간 중 환급액 조회를 유도한 악성 문자**가 다량 유포될 수 있으며, 명절 선물, 세뱃돈 송금 등 국민들이 쉽게 속아 넘어갈 수 있는 상황을 악용해 악성앱 감염 유도 문자가 유포될 수 있어 국민들의 각별한 주의를 당부했다.

또한, 악성문자 외에 공유형 킥보드 이용 및 행사정보 제공 등에 자주 이용되는 QR코드를 악용해 악성앱 설치를 유도하는 **‘큐싱(QR코드+피싱)*’ 피해가 우려되고 있어 이에 대한 주의가 요구**된다.

* QR코드에 악성앱 설치 인터넷주소(URL)을 삽입하여 QR코드 촬영시 악성앱이 설치되어 개인·금융정보 탈취, 스마트폰 원격 조종, 소액결제 유도 등 피해 발생

아울러, 명절을 앞두고 본인이 구매하지 않았거나, 미리 연락받지 않은 물건에 대한 배송안내, 결제요청, 환불 계좌 입력 등의 문자가 온 경우, **문자에 포함된 인터넷 주소(URL)를 누르지 말고 사실관계를 먼저 확인**할 필요가 있음을 강조했다. 유포된 악성 문자메시지를 통해 원격조종이 가능한 악성 앱이 설치되면 재산상 피해가 발생할 수 있으므로 전화, 영상통화 등으로 상대방을 정확하게 확인하기 전에는 악성 앱 설치를 유도하는 상대방의 요구에 응하지 말아야 한다.

**【 스미싱 피해 예방수칙 】**

① 범칙금・과태료 통보(또는 확인요청), 연말정산 환급액 조회 택배 조회, 명절 인사, 모바일 상품권・승차권・공연예매권 증정, 지인사칭 문자 등에 포함된 **출처가 불명확한 인터넷주소(URL) 또는 모르는 전화번호를 클릭하지 마세요.**

② 출처를 알 수 없는 앱은 함부로 설치되지 않도록 **스마트폰 보안설정을 강화**하고, 앱 다운로드는 받은 문자의 링크를 통해 받지 말고 **공인된 열린시장(오픈마켓)을 통해 설치하세요.**

③ 스마트폰 **백신프로그램을 설치**하여 업데이트 및 실시간 감시 상태를 유지하세요.

④ 본인인증, 재난지원금 및 백신예약 조회 등의 명목으로 **신분증 등 개인정보・금융정보를 요구하는 경우, 절대 입력하거나 알려주지 마세요.**

⑤ 대화 상대방이 개인・금융정보나 금전을 요구하거나 앱 설치를 요구하는 경우 반드시 전화, 영상통화 등으로 상대방을 정확하게 확인하세요.

⑥ 신분증 사진 등이 유출되지 않도록 **스마트폰 내에 저장된 주민등록증, 운전면허증, 여권 사진을 바로 삭제하세요.**

## < 허위쇼핑몰 등 사이버사기 주의보>

명절 선물 등을 **지나치게 저렴하게 판매하는 온라인 쇼핑몰** 발견 시, 상품 구매에 앞서 사업자 정보, 판매자 이력, 고객평가(리뷰), 온라인 내 고객불만 글 게시 여부를 확인하여야 한다. 또한, 구매시 가급적 취소가 가능한 신용카드를 이용하고, 추가 할인 등을 미끼로 현금거래를 유도하는 판매자와는 거래하지 않아야 한다.

**【 쇼핑몰사기 예방수칙 】**

웹사이트나 누리소통망 서비스(SNS)에서 이상하게 낮은 가격으로 고가의 상품을 판매하겠다고 홍보하는 경우, 아래 내용을 한 번 더 확인해보세요.

① 공식 쇼핑몰과 유사하지만 서로 다른 인터넷주소(URL)을 사용하는 것은 아닌지 검색엔진 등을 통해 다시 한번 확인합니다.

② 쇼핑몰 웹페이지에서 사업자 정보, 고객 평 또는 불만 글 등록 여부 등을 확인합니다.

③ 거래는 될 수 있으면 신용카드를 이용, 추가 할인 등을 미끼로 현금거래를 유도하는 판매자와는 거래를 지양합니다.

④ 블로그나 누리소통망 서비스(SNS)를 통해 구입 시에는 **공정거래위원회 누리집**을 통해 해당 사업자가 통신판매 신고를 한 사업자인지 여부와, 청약 철회 가능 여부 등을 확인합니다.

(공정거래위원회「정보공개」–「사업자정보공개」–「통신판매 사업자」에서 확인 가능)

연휴 기간에는 택배가 운영되지 않는 기간이 길어서 사이버사기 피해를 입었는지 여부에 대한 확인이 늦을 수 있다. **긴 연휴를 앞두고는 가급적 비대면 거래를 지양**하고, 거래에 앞서 경찰청의 **「인터넷 사기 의심 전화·계좌번호 조회서비스」** 등을 통해 사기 피해 신고 여부를 먼저 확인할 것을 당부하였다.

※ **(경찰청 인터넷 사기 의심·계좌번호 조회서비스)** 경찰청(https://www.police.go.kr) 누리집 -「신고/지원」-「사이버안전지킴이」-「인터넷사기 의심 전화·계좌번호 조회」

아울러, 정상적인 문자 메시지인 것처럼 수신자를 속인 후, 다른 메신저 앱으로 유도해 금전이나 상품권, 금융거래 정보 등을 요구하는 **메신저 피싱*도 증가추세인 만큼 각별한 주의**가 필요하다.

* ▵물건배송·대금환불 가장 스미싱 문자 ▵지인을 사칭하며 메신저 등록을 요구하는 문자 ▵주식 리딩·코인투자·쇼핑몰 리뷰 아르바이트 등을 통해 고수익을 보장한다는 스팸 문자 등에 기재된 인터넷 주소(링크)를 클릭하지 말고, 문자를 보낸 상대방과 전화통화나 문자로 대화를 이어나가지 말 것을 당부

## < 사이버사기 예방 홍보 추진 >

**과학기술정보통신부와 한국인터넷진흥원은** 설 연휴기간 동안 **문자사기에 신속하게 대응**할 수 있도록 **24시간 탐지체계를 운영**하고, **문자결제사기(스미싱·큐싱)확인서비스*** 등을 통해 신고·접수된 문자사기 정보를 분석하여 금융사기 **사이트, 악성 앱 유포지 등에 대한 긴급 차단조치**를 지원하여 국민들의 피해를 최소화할 계획이다.

* **카카오톡앱에서 채널 친구로 '보호나라'를 추가**, '스미싱' 메뉴를 통해 의심되는 문자 메시지를 입력하거나 '큐싱' 메뉴를 통해 QR코드를 촬영하면 해당 내용을 분석 후 10분 이내 '주의', '악성', 또는 '정상' 답변 제공 <붙임 1 참고>

**방통위**는 이동통신 3사(SKT, KT, LGU+), 한국정보통신진흥협회(KAIT)와 협력하여 1월 15일부터 각 통신사 명의로 가입자에게 **『설 연휴 스미싱 문자 등 주의 안내』 문자 메시지를 순차 발송한다.** <붙임 2 참고>

**금융위원회**와 **금융감독원**은 최근 사기범들이 고령층을 대상으로 **카드 오발급** 등을 **빙자**하여 접근, 범죄 연루 여부 확인 등을 위해 필요하다며 금전 이체를 요구하거나 금융회사로부터 대출을 받도록 유인하여 금원을 편취하는 사례가 발생하고 있으므로 **각별한 주의**를 당부하였다. **본인이 신청하지 않은 신용카드가 배송 중**이라고 문자나 연락을 받으면 **"보이스피싱을 의심하고"**, **가족** 또는 **지인**의 **도움**을 받아 **카드사 공식 전화번호**로 연락하여 사실관계를 확인할 필요가 있다.

아울러, 금융소비자가 **「여신거래 안심차단 서비스」, 휴대폰 기기 내 보안강화 기능** 등을 이용하여 보이스피싱으로 인한 금전 피해를 미연에 방지할 수 있도록 **금융회사 영업점, 금융앱(알림톡), SNS 채널** 등을 통해 안심차단 및 보안강화 서비스 이용 방법을 금융소비자에게 전파하고 있다.

* 금융소비자가 본인이 원하지 않는 여신거래로 인한 피해를 입지 않도록 신용대출, 카드론 등 개인의 신규 여신거래를 사전에 차단할 수 있도록 하는 서비스
☞ **「여신거래 안심차단」 서비스 이용방법** <붙임 3 참고>

** 알 수 없는 출처의 앱이 휴대폰에 설치되는 것을 제한하여 악성앱 설치를 미연에 방지
☞ **알 수 없는 출처의 앱 설치 차단 방법** <붙임 4 참고>

**경찰청**은 설 연휴 기간 전후 발생하는 문자사기(스미싱) 등 사이버사기 범죄에 대한 **단속을 강화**하고 피해 예방을 위해 **누리집과 SNS 채널 등을 통해 예방수칙을 제공할 계획**이다. <붙임 5 참고>

또한, **명절 연휴 중에도 문자사기(스미싱) 등 사이버범죄 피해**를 입은 경우, **112로 신고**하거나 **『경찰청 사이버범죄 신고시스템(ECRM)』**을 통해 온라인으로 피해신고를 접수할 수 있음을 안내할 예정이다.

※ 경찰청(https://www.police.go.kr) 및 사이버범죄신고시스템(ecrm.police.go.kr) 누리집 참조

**【사이버사기 피해 또는 의심되는 경우 신고방법 등】**

| 사이버사기 사례(의심) | 조치방법 |
|---|---|
| o 사이버사기 범죄 피해를 입은 경우 | 경찰청(☎112)에 전화신고 또는 경찰청 홈페이지에서 '사이버범죄 신고시스템'를 통해 온라인 신고 |
| o 보이스피싱 사기범에게 속아 피해금을 계좌로 송금한 경우 | 경찰청(☎112) 신고 및 송금계좌에 대한 지급정지 요청<br>※ 돈이 출금되거나 입금된 금융회사 콜센터에 연락하여 지급정지 신청하는 것도 가능 |
| o 악성앱 설치 등으로 개인정보 유출이 의심되어 보이스피싱 우려 | 금융회사 영업점을 방문하거나 콜센터에 전화하여 본인 계좌에 대해 일괄 지급정치를 요청 |
| o 문자사기 의심문자 수신 또는 악성 앱 감염 의심 시 | ① 보호나라 스미싱·큐싱 확인서비스 이용 악성 확인<br>※ 카카오톡 채널에 '보호나라'를 검색하여 접속<br>② 한국인터넷진흥원(☎118) 상담센터에 상담<br>③ 금융감독원 '사기전화 지킴이'에 신고<br>※ 네이버에 '사기전화 지킴이'를 검색하여 접속 |

| | | | | | |
|---|---|---|---|---|---|
| 담당 부서 | 과학기술정보통신부<br>사이버침해대응과 | 책임자 | 과 장 | 최광기 | (044-202-6460) |
| | | 담당자 | 사무관 | 김성환 | (044-202-6461) |
| | 방송통신위원회<br>디지털이용자기반과 | 책임자 | 과 장 | 고남현 | (02-2110-1520) |
| | | 담당자 | 사무관 | 김상엽 | (02-2110-1527) |
| | 금융위원회<br>금융안전과 | 책임자 | 과 장 | 이진호 | (02-2100-2970) |
| | | 담당자 | 사무관 | 차영호 | (02-2100-2974) |
| | 경찰청<br>사이버범죄수사과 | 책임자 | 과 장 | 함영욱 | (02-3150-1605) |
| | | 담당자 | 경 정 | 이여정 | (02-3150-1658) |
| | 한국인터넷진흥원<br>국민피해대응단 | 책임자 | 단 장 | 이동연 | (02-405-6640) |
| | | 담당자 | 팀 장 | 김은성 | (02-405-5363) |
| | 금융감독원<br>금융사기대응단 | 책임자 | 국 장 | 정재승 | (02-3145-8150) |
| | | 담당자 | 팀 장 | 김태근 | (02-3145-8130) |

# 붙임 1 스미싱 · 큐싱 확인서비스 이용방법

## 1. 카카오톡 채널 검색 후, '보호나라' 채널추가

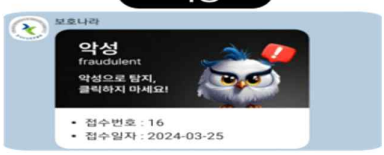
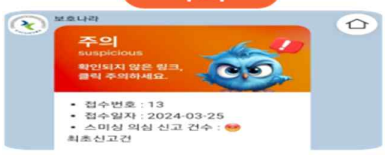
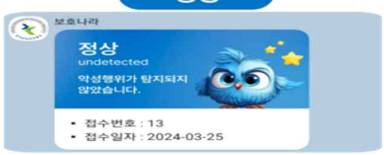

## 2-1. (스미싱 확인) 채널 창내 '스미싱' 클릭 후 메시지 복사 및 붙여넣기


스미싱 문자 복사 | 스미싱 확인서비스 열기 | 스미싱 확인서비스 붙여넣기

## 2-2. (큐싱 확인) 채널 창내 '큐싱' 클릭 후 QR코드 촬영


큐싱으로 의심되는 QR코드 | 큐싱 확인서비스 열기 | QR코드 촬영

## 3. 결과 확인

| 악성 | 주의 | 정상 |
|---|---|---|
|  |  |  |
| ☑ 해당 메시지 삭제・차단 | ☑ 악성/정상 불분명, 약 10분 후 '접수결과확인' 클릭하여 재확인 | ☑ 정상링크 확인 |

## 붙임 2 설 연휴 스미싱 문자 등 주의 안내사항(방통위)

### □ 이동통신3사 (문자메시지 발송)

**[설 연휴 스미싱 문자 등 주의 안내]**

설 명절을 앞서 연말정산 조회, 신용카드 배송조회 등을 사칭한 스미싱 문자 및 해킹메일 등이 예상되오니 피해예방을 위해 다음 유의사항을 안내 드립니다.

1. 출처가 불분명한 문자를 받은 경우 인터넷주소(URL)나 전화번호는 절대 누르지 마시고 '스팸으로 신고' 또는 카카오톡 「보호나라」 채널 '스미싱확인서비스'에 의심문자의 '정상' 여부를 확인하시기 바랍니다.
2. 본인이 신청하지 않은 신용카드가 배송 중이라고 문자나 연락을 받으면 '일단 보이스피싱을 의심하고', 가족 또는 지인의 도움을 받아 카드사 공식 전화번호로 연락하시기 바랍니다.
3. 개인정보 유출로 인해 본인이 원하지 않는 여신거래가 발생하여 피해를 입지 않도록 금융회사를 방문하여 '여신거래 안심차단 서비스'를 신청하시기 바랍니다.
4. 사이버사기 범죄피해를 입은 경우 ☎112 또는 경찰청 홈페이지 신고창구로 즉시 신고하여 주시기 바랍니다.
5. 아무리 급해도 불법사채, 불법사금융은 NO! 불법사금융 신고·상담은 금융감독원 「불법사금융 지킴이」(포털 검색) 또는 ☎1332로 신고하여 주시기 바랍니다.

※ 1월 15일(수)부터 순차적으로 이통3사를 통해 문자발송 예정

# 붙임 3 「여신거래 안심차단」 이용방법

## ① 여신거래 안심차단 신청(은행, 저축은행, 농·수협, 새마을금고, 신협, 산림조합, 우체국)


▶ 이용자는 **현재 거래 중**인 **금융회사 영업점**을 **방문**하여 본인확인 후 **여신거래 안심차단**을 **신청**

▶ **안심차단 신청 즉시,**
**금융권**의 **신규 여신거래**가 **차단**됩니다.

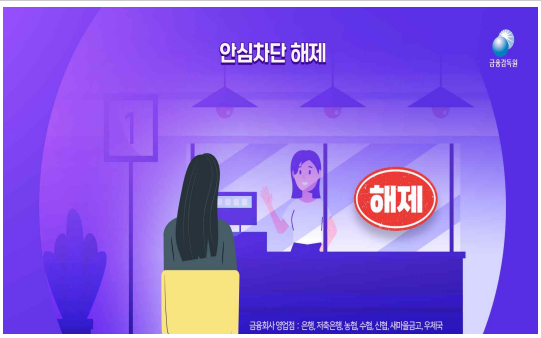
▼

## ② 차단되는 여신거래


▶ **안심차단 신청시,** 금융회사의 **신용대출, 카드론, 신용카드 발급, 할부금융, 예·적금 담보대출 등 개인의 여신거래**가 **실시간 차단**됩니다.

▼

## ③ 여신거래 안심차단 해제(은행, 저축은행, 농·수협, 새마을금고, 신협, 산림조합, 우체국)




▶ **기존 거래여부와 무관**하게 가까운 금융회사 영업점을 방문하여 본인확인 후 **손쉽게 해제 가능**

▶ 이용자는 **필요한 여신 실행 이후, 안심차단**의 **재신청**도 **가능**합니다.

▼

## ④ 여신거래 안심차단 신청여부 조회 및 통지


▶ 이용자는 본인의 안심차단 신청여부에 대해 **한국신용정보원 홈페이지***를 통해 **직접 조회 가능(신청 및 해제 상태 확인가능)**

* www.credit4u.or.kr

▶ **안심차단을 신청한 금융회사**에서 **반기 1회 안심차단 신청사실**을 이용자에게 **통지**합니다.

# 붙임 4 알 수 없는 출처의 앱 설치 차단 방법

< 차단 기능 설정 방법(안드로이드) >

1. 스마트폰 '설정' 앱 클릭


2. '보안 및 개인정보 보호' 메뉴 접속


3. '보안 위험 자동 차단' 활성화

※ 차단 방법은 스마트폰에 탑재된 안드로이드 OS 버전에 따라 다를 수 있음

**붙임 5** **설 연휴 사이버사기 및 스미싱 예방수칙(경찰청)**

# 설 명절 기간
# 사이버사기·스미싱 주의보

**<비대면 사이버사기 주의 !>**

QR로 조회해보기

거래에 앞서 경찰청에서 제공하는
「인터넷 사기 의심 전화·계좌번호 조회」에서
거래 상대방의 전화번호나 계좌번호를 조회해보세요.

※ 경찰청에 신고가 접수된 사기 의심 전화번호, 계좌번호 등과 비교해볼 수 있습니다.

**<허위 쇼핑몰 주의 !>**

구매에 앞서 공식 쇼핑몰의 URL이 정확하게 맞는지 확인하고
사업자 정보, 불만글 등록 여부 등을 먼저 검색해봅니다.
할인 등을 미끼로 현금 거래를 유도하는 판매자와는 거래를 피합니다.

**<스미싱 주의 !>**

개인정보나 금융정보의 입력을 요구하거나
신분증 사진을 찍어 보내달라는 문자에는 대응하지 말고,
출처를 모르는 URL 링크를 누르지 않습니다.

※ 실수로 클릭하여 파일이 다운로드 된 경우에는 즉시 삭제하고,
모바일 백신 등을 사용하여 보안상태를 점검합니다.

고수익을 보장한다며 투자 · 아르바이트를 유도하거나
지인을 사칭하여 메신저 친구추가를 요청하는
스팸문자는 개인정보 · 금전을 탈취하거나
선결제를 유도하는 사기이니 대응하지 않습니다.

경찰청 국가수사본부 수사국