



보도시점 2023. 9. 21.(목) 12:00
(2023. 9. 22.(금) 조간) 배포 2023. 9. 21.(목) 09:00

추석 명절, 스마트폰 해킹(악성앱) 스미싱 문자 주의!

- 출처가 불분명한 문자(SMS)의 인터넷주소(URL)나 전화번호 클릭 금지
- 개인정보나 금융정보를 요구하는 메신저나 전화는 상대방을 정확히 확인
- 피해가 의심되면 국번 없이 112나 '보이스피싱지킴이'에 신고

과학기술정보통신부(장관 이종호, 이하 '과기정통부'), 방송통신위원회(위원장 이동관), 금융위원회(위원장 김주현), 경찰청(청장 윤희근), 한국인터넷진흥원(원장 이원태, 이하 'KISA'), 금융감독원(원장 이복현)은 추석 연휴를 앞두고,

택배 배송이나 교통법칙금 조회를 사칭한 문자사기(이하 스미싱*)나 지인 명절인사 등으로 위장한 메신저 피싱이 증가할 것으로 보고, 이로 인한 이용자의 피해 주의를 당부했다.

* 스미싱: 문자메시지(SMS)와 피싱(Phishing)의 합성어. 악성 앱 주소가 포함된 휴대전화 문자를 전송하여 이용자가 악성 앱 설치 또는 전화 통화 유도를 통해 금융정보·개인정보 등을 탈취하는 수법(보이스피싱, 전자상거래 사기 등에 악용)

최근 3년간 스미싱 피해 현황을 분석해 보면 택배 배송 사칭 유형이 28만여 건으로 전체의 약 65%를 차지하고 있는데, 이번 추석 명절에도 명절 기간을 전후하여 가족 친지, 지인 간 선물배송이 증가하는 상황을 악용하는 스미싱 문자가 다량 유포될 수 있어 국민들의 각별한 주의가 요구된다.

또한, 코로나 엔데믹으로 외부 활동이 늘어남에 따라 건강검진, 교통법칙금 등 공공기관 사칭('22년 17,726건→'23.8월 73,364건)이나 청첩장, 부고장 등 지인을 사칭하는 유형('22년 4건→'23.8월 73,364건)이 올해 급증하고, 추석을 앞두고 고향 방문 등 차량 이동 증가를 틈탄 교통위반 범칙금 조회나 안부인사 등을 사칭하는 악성 문자도 지속 유포될 것으로 보고 있다.

※ 주요 사례 <붙임 1 참조>

< 최근 3년간 스미싱 문자 신고·탐지 현황 >

(단위: 건)

구 분	2021년	2022년	2023. 8월	합 계
전 체	202,276	37,122	196,935	436,333
택배 사칭(%)	175,753	19,214	88,864	283,831(65.0%)
공공기관 사칭(%)	16,513	17,726	73,364	107,603(24.7%)
지인 사칭(%)	25	4	32,441	32,470(7.4%)
금융 사칭(%)	5,781	110	34	5,925(1.4%)
기타(%)	4,204	68	2,232	6,504(1.5%)

이와 함께, 메신저 앱을 통해 가족, 지인을 사칭하며 긴급한 상황*이라며 금전이나 상품권, 금융거래 정보 등을 요구하는 메신저 피싱 피해도 증가하는 추세로 주의가 필요하다. <붙임 2 참조>

* 휴대전화 고장, 신용카드 도난·분실, 사고 합의금, 상품권 대리 구매 등

특히, 공격자가 원격조종이 가능한 악성 앱이 설치되면 상당한 재산상 피해가 발생할 수 있으므로 국민들은 전화, 영상통화 등으로 상대방을 정확하게 확인하기 전에는 악성 앱 설치를 유도하는 상대방의 요구에 응하지 말아야 한다.

국민들이 위와 같은 문자사기 피해를 사전에 예방하기 위해서는 다음과 같은 보안 수칙 준수가 필요하다.

- ▲ 택배 조회, 명절 인사, 모바일 상품권·승차권·공연예매권 증정, 지인사칭 문자에 포함된 출처가 불분명한 인터넷주소(URL) 또는 전화번호를 클릭하지 않을 것
- ▲ 출처를 알 수 없는 앱은 함부로 설치되지 않도록 스마트폰 보안설정을 강화하고, 앱 다운로드를 받은 문자의 링크를 통해 받지 말고 공인된 오픈마켓(플레이스토퍼·앱스토어)을 통해 설치할 것
- ▲ 백신프로그램*을 설치하여 업데이트 및 실시간 감시 상태를 유지할 것
* 시티즌코난 등 모바일 백신 설치 후, 악성앱 설치여부 주기적 점검 및 삭제
- ▲ 본인인증, 정부지원금 등의 명목으로 신분증 등 개인정보·금융정보를 요구하는 경우, 절대 입력하거나 알려주지 않을 것
- ▲ 대화 상대방이 개인·금융정보나 금전을 요구하거나 앱 설치를 요구하는 경우 반드시 전화, 영상통화 등으로 상대방을 정확하게 확인할 것
- ▲ 신분증 사진 등이 유출되지 않도록 스마트폰 내에 저장된 주민등록증, 운전면허증, 여권 사진을 바로 삭제할 것
- ▲ 본인도 모르는 휴대전화 개통을 사전에 방지하기 위해 엠세이프 홈페이지(www.msafier.or.kr)에 방문하여, 명의도용방지 서비스를 신청할 것

정부는 국민들이 편안한 추석 명절을 보낼 수 있도록 관계부처들과 협력해 24시간 사이버 안전 대응체계를 마련하고, 문자사기 감시와 사이버 범죄 단속을 중점적으로 실시한다.

과기정통부와 KISA는 추석 연휴기간 동안 문자사기에 신속하게 대응할 수 있도록 24시간 탐지체계를 운영하고, 신고·접수된 문자사기 정보를 분석하여 피싱 사이트, 악성 앱 유포지 등에 대한 긴급 차단조치를 통해 국민들의 피해를 최소화할 계획이다.

또한, 전문적인 지식이 없어도 내 PC와 모바일 기기의 정보보안 수준 및 취약점을 점검할 수 있도록 ‘내PC·모바일 돌보미’ 서비스를 제공*하고, 고령층, 장애인, 아동 등 정보보호 실천이 어려운 디지털 취약계층을 지원하기 위해 노인·장애인 복지센터, 키움 아동센터 등에 보안 전문가가 직접 방문하는 보안점검 서비스도 진행한다.

* KISA 보호나라(www.boho.or.kr)→개인서비스→내PC·모바일 돌보미

더불어, 이통사와 공동으로 보이스피싱 신종 수법 피해 예방을 위해 전국 23,000개 휴대폰 판매 유통점과 인터넷 홈페이지 등을 통해 명의도용방지 서비스*(www.msafes.or.kr) 대국민 홍보를 진행한다.

* 조화일 기준으로 본인 명의의 회선 현황을 확인할 수 있는 서비스(가입현황조회 서비스), 본인 신청으로 이동전화 신규 가입, 명의변경 등을 제한하는 서비스(명의도용가입제한서비스)

방송통신위원회는 이동통신 3사(SKT, KT, LGU+), 한국정보통신진흥협회(KAIT)와 협력하여 9월 16일부터 각 통신사 명의로 가입자에게 『스미싱 문자 주의 안내』 문자 메시지를 순차 발송하고 있다. <붙임 3 참고>

금융위원회와 금융감독원은 금융권과 공동으로 문자사기와 보이스피싱 피해 예방을 위한 집중 홍보기간(9.4.~9.27.)을 운영한다. 피해 예방 방법과 피해 발생 시 대응 요령을 포스터, 리플렛, 만화 영상 등으로 제작하여 국민들에게 배포하고, <붙임 4 참고>

출처가 불분명한 인터넷주소(URL)를 잘못 클릭할 때 직면하게 되는 상황을

체험형 콘텐츠로 개발*하여 스미싱 문자에 대한 경각심을 제고한다.

* 보이스피싱 사이버체험관(www.fss.or.kr/fss/pk/index.html)에서 콘텐츠 이용 가능
- URL을 클릭하면 체험자가 어떤 선택을 하더라도 피해를 당하는 내용으로 구성

경찰청은 문자사기 피해 예방을 위해 경찰청 홈페이지와 모바일 앱인 ‘사이버캡’을 통해 예방 수칙·피해 정보 등을 제공하고,

추석 연휴 기간 전후로 발생하는 문자사기, 직거래 사기 등 서민 생활을 침해하는 사이버상 악성사기에 대해 단속을 강화할 계획이며, 사이버범죄 피해를 입은 경우 112나 사이버범죄 신고시스템(ECRM)을 이용해 신고를 접수해달라고 당부했다.

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

명절 연휴 중 문자사기 의심 문자를 수신하였거나, 악성 앱 감염 등이 의심되는 경우 112나 ‘보이스피싱지킴이**’에 신고하면 24시간 무료로 상담 받을 수 있다.

* 보이스피싱지킴이(www.fss.or.kr/fss/cvpl/vphisFncFrud/dclrGuide.do?menuNo=201134)

담당 부서	과학기술정보통신부 사이버침해대응과	책임자	과 장	허진우 (044-202-6460)
		담당자	사무관	김승열 (044-202-6461)
	방송통신위원회 이용자보호과	책임자	과 장	권희수 (02-2110-1540)
		담당자	주무관	김민지 (02-2110-1542)
	금융위원회 전자금융과	책임자	과 장	김수호 (02-2100-2970)
		담당자	사무관	남명호 (02-2100-2974)
	경찰청 사이버범죄수사과	책임자	과 장	이병귀 (02-3150-1605)
		담당자	경 정	이여정 (02-3150-1658)
	한국인터넷진흥원 침해대응단	책임자	단 장	임채태 (02-405-6610)
		담당자	팀 장	김은성 (02-405-5363)
	금융감독원 금융사기전담대응단	책임자	국 장	임정환 (02-3145-8150)
		담당자	팀 장	김세모 (02-3145-8130)

붙임1 문자사기(스미싱) 문자 사례 (KISA 제공)

[사례 1] 추석 명절 사칭

☎(^o^)*★ 추석 잘 보내시고
2023년 남은 시간 모두 모두 행
복한 시간 되시길 바랍니다
<http://woz.kr/mhgd>

- ① OO님 추석명절 선물로 모바일 상품권을 보내 드립니다. 확인 바랍니다. <URL>
- ② 추석선물 도착 전 상품 무료 배송! 할인쿠폰 지급완료! 즉시 사용가능! 확인 <URL>

[사례 2] 택배 사칭

[Web발신][OO택배]8월22일 택배, 미배달 도로명불일치 변경요망.
<http://napoa.rzhda.com>

[Web발신]로켓배송사전예약주문하신상품 8/12 도착예정,주소지재확인바람.
<http://x12.as1d.hair>

- ① 로켓배송사전에 예약 주문하신 상품 8/12 도착 예정, 주소지재확인바람 <URL>
- ② 반송처리 알림문자. 부재중으로 인해 반송처리됨 상세내용 <URL>
- ③ 송장번호 [xxxxxxx] 부재중 미수취 물품 확인 바랍니다. <URL>
- ④ 택배배송중 수령지를 선택해주세요. 1현관앞 2경비실 3본인수령 <URL>
- ⑤ 주문하신 물품 O/OO 배달예정, 주소재확인바람 <URL>

[사례 3] 지원금 사칭

[OO은행] 소득확인 가능자 최저 3.2%대금리,최대1억원까지 신청 가능
<http://nhsavingivi.com/>

[OO부 지원금 신청 안내]
귀하는 국민지원금 신청대상자에 해당되므로 온라인 센터 (<http://kr.center.com>)에서 지원하시기 바랍니다.

- ① [Web발신] “fOO은행」소득확인 가능자 최저 3.2%대 금리, 최대 1억원까지 신청 가능 상담 문의 : 02-000-0000
- ② 지원금 신청이 접수되었습니다. 다시 한번 확인 부탁드립니다. <URL>
- ③ 재난 지원금 신청 및 지급:<URL>
- ④ (광고)「OO희망론」『2023년 정부 특별지원금 대출 시행 안내』안녕하세요. 『OO새희망론』의 새로운 소식을 전합니다. [지원절차]- 상담 및 접수 (신청인) → 한도조회 → 가결시 대출약정체결 → 대출금 입금완료거부 080-000-0000
- ⑤ O월에 추가 보조금이 지급 되었으니 시간 내에 철회하십시오 <URL>

[사례 4] 공공기관 사칭

[Web발신]건강검사 통지서 발송완료. 상세보기 <https://b05.p5zd.hair>

[Web발신]도로교통위반벌금고지서 <https://me2.do/GZjvSndn>

- ① [Web발신] 도로교통위반 벌금고지서 <URL>
- ② [Web발신] 무료 건강검진 예약 알림 <URL>
- ③ 【사이버 검찰청】.사건 처리통지서입 니 다상세 내용확인 <URL>
- ④ [국민연금] OOOO년 O월 국민연금 지급정지 통지서 <URL>
- ⑤ 국민건강보험공단 환급금(지원금)안내<URL>

[사례 5] 지인 사칭

[모바일 초대] 결혼식 일시 : 08/19 (토) 11:00 많이많이와주세요
<skm.mediaquki.com/>

故 부친께서 별세하셨기에 아래와 같이 부고를 전해드립니다
<https://iplogger.com/2rzFg8>

- ① “엄마, 딸인데, 핸드폰 액정이 깨져서 대리점에서 임시 폰 받았어. 전화통화 안되니까 카톡 친구 추가해줘”
- ② “신분증과 계좌번호, 비밀번호 보내줘. 엄마 폰으로 할 게 있어. 보내주는 앱 깔아줘” <URL>
- ③ [부고] 18일 저녁 10시경 부친께서 별세하셨습니다. 안내 <URL>
- ④ [모바일 초대] 돌잔치 초대장을 보내드렸습니다 참석하여 주시기 바랍니다 <URL>

붙임2 메신저피싱 피해사례 (경찰청 제공)

- ☐ 피해자 A는 “엄마 내꺼 핸드폰 떨어트려서 화면이 깨져 수리 맡겼어. 이 번호로 톡친구 추가하고 톡쥬”라는 문자를 수신
- ☐ 문자 발송 전화번호를 메신저앱에 등록하고 메시지를 보내자 “가족명으로 핸드폰 액정 보험에 가입하면 수리비가 공짜라는데 가족명의 인증이 필요해, 엄마 주민등록증사진, 계좌번호랑 비밀번호 보내줘, 빗반사 없이 내면 잘보이게”라며 개인정보, 금융거래정보 요구
- ☐ 피해자가 개인·금융정보를 보내자 다시 “인증이 안되네, 내가 엄마폰 연결 해서 할게, 눌러서 설치하고 열면 귀하의 아이디 9자리라고 나오면 나한테 보내줘”라며 인터넷주소(URL)를 보내 원격제어앱* 설치를 유도
 - * 원격제어앱 이용은 휴대전화로 할 수 있는 비대면 계좌개설, 이체, 대출 등 모든 행위를 상대방이 할 수 있게 해준다는 의미로, 반드시 제어 상대방 신분 확인 필요
- ☐ 피해자 인터넷 주소(URL)를 클릭해 앱 설치 후 접속정보를 알려주자 “내가 폰 다 사용하고 얘기할게, 폰 그냥 가만히 놔둬”라고 하며 사기범이 피해자 휴대전화를 제어, 은행·증권앱 등을 이용해 수십 회에 걸쳐 약 1억 5천만 원을 다수의 대포계좌로 이체하고,
 - ※ 휴대전화로 신청 가능한 비대면 대출을 이용, 대출금까지 편취 해가는 사례 다수 발생
- ☐ 온라인 쇼핑몰, 게임앱 등에서 전자지급결제대행 (PG) 서비스를 이용해 약 1천만 원 상당의 상품권(기프트 카드), 게임 아이템 등을 구매함
- ☐ 범행 중간에 이상함을 느낀 피해자가 전화통화를 요청하거나 출신학교, 지인들의 이름 등을 물어봤지만 사기범은 “엄마 왜 그래, 아들이라니까, 지금 거의 다 했어 끝나고 전화할게, 컴퓨터 메신저라 전화 못해”라며 통화 및 답변을 회피, 시간을 끌며 계속 범행을 이어감

붙임3 스미싱 문자 주의 안내사항 (방통위 제공)

☐ 이동통신3사 (문자메시지 발송)

[악성앱 스미싱 문자 주의 안내]

최근 모바일 청첩장, 택배 조회, 건강검진 결과조회 등 악성앱 링크가 포함된 메시지를 보내 피해자가 링크를 클릭하면 개인정보를 탈취, 피해자 명의 신규 폰을 개통하여, 예금을 탈취하고 대출을 실행하는 사기수법이 확산되고 있어, 국민들이 꼭 알아야 할 4가지를 다음과 같이 알려드립니다.

1. 시티즌코난 등 모바일 보안앱 설치
2. 유사시 무조건 112로 신고
3. 본인도 모르는 휴대전화 개통을 사전에 방지
 - ※ 엠세이퍼 홈페이지(www.msafes.or.kr)에 방문하여, 명의도용방지 서비스를 신청
4. 주말·연휴 중에도 전화(112)로 본인계좌 일괄지급정지 가능

보이스피싱 피해 발생 시 즉시 대응조치



**경찰(112), 금감원(1332),
금융회사에 계좌 지급 정지 신청**

금융감독원 | 한국정보통신진흥협회 | 한국소비자원 | 한국인터넷진흥원 | 한국전자거래진흥원 | 한국금융정보보호협회 | 한국금융정보보호협회

보이스피싱 전화 또는 문자를 받고,
피싱 사기범에게 이체·송금, 개인정보 제공
또는 악성앱이 설치된 경우 다음과 같이 대응

- 1** 입금 금융회사 또는 송금 금융회사 콜센터에 즉시 전화하여 피해신고 및 계좌 지급정지* 신청
(경찰청 112 및 금감원 1332에서도 연결 가능)
*본인 거래 금융회사에서 본인의 모든 계좌 일괄 지급정지 가능
- 2** 신분증, 계좌번호 등 개인정보가 유출되거나, 의심스런 URL 접속으로 악성앱 설치가 의심되는 경우 다음 절차대로 신속 조치

초기화 전까지 휴대전화 전원을 끄거나 비행기모드 전환

악성앱 삭제

- (악성앱 설치 시) 휴대전화 초기화나 악성앱 삭제

다른 휴대전화 및 PC 사용을 권장

개인정보 노출사실 등록

- 금감원 개인정보 노출자 사고예방시스템 (pd.fsc.or.kr) 접속
- 이용약관, 개인정보제공 등 동의 후 휴대전화 인증으로 본인 확인
- 개인정보 노출사실을 등록하여 신규계좌 개설, 신용카드 발급 등 제한

다른 휴대전화 및 PC 사용을 권장

본인 계좌 지급정지(일괄 또는 부분) 신청

- 금융감독원 계좌정보통합관리서비스(www.payinfo.or.kr) 접속
- 본인 계좌 지급정지 메뉴에서 은행권, 제2금융권, 증권사 클릭
- 공동인증서 및 휴대전화 인증(2중 인증)으로 본인 확인
- 지급정지를 신청할 계좌를 선택 후 지급정지 신청

1. 영입점을 방문하거나 콜센터(전화)를 통해서도 지급정지 신청 가능

명의도용된 휴대전화 개설 여부 조회

- 한국정보통신진흥협회 명의도용방지 서비스 (www.msafar.or.kr) 접속
- 공동인증서 등으로 로그인
- 가입사실현황조회 서비스 메뉴 클릭하여, 본인명의로 개설된 휴대전화 개설 사건여부를 확인
- 명의도용 휴대전화가 등록된 경우, 즉시 해당 이동통신사 등에 확산해지 신청 및 명의도용 신고
- 가입제한 서비스 메뉴 클릭하여, 본인명의 휴대전화 신규개설 차단

필요서류는 방문 전 금융회사 또는 경찰서 문의

3 경찰서(사이버 수사대)에서 발급한 사건사고사실확인원 등 증빙서류와 함께 지급정지 신청한 영업점에 피해구제신청 서면접수(신청일 3일 이내)

※ 즉시 대응조치를 시행한 이후, 금융회사 및 경찰 안내 등에 따라 인증서 폐지·재발급, 신분증 분실신고 등 **필요한 추가조치**를 실시

만화를 통해 복습하는 보이스피싱 대응요령



휴대전화 초기화 및 악성앱 삭제



개인정보 노출사실 등록
[pd.fss.or.kr]



내 계좌 지급정지(일괄 또는 부분) 신청
[www.payinfo.or.kr]



명의 도용된 휴대전화 개설 여부 조회
[www.msafar.or.kr]