
 관계부처 합동	보 도 자 료			
	보도	배포시점부터 보도	배포	
책 임 자	과기정통부 사이버침해대응과장 정 재 욱(044-202-6460)		담 당 자	김 남 승 사무관 (044-202-6461)
	방송통신위원회 이용자보호과장 이 소 라(02-2110-1540)			박 대 균 주무관 (02-2110-1547)
	금융위원회 전자금융과장 이 한 진(02-2100-2970)			이 영 우 사무관 (02-2100-2975)
	금감원 불법금융대응단 팀장 이 선 진(02-3145-8521)			문 성 훈 수석 (02-3145-8534)
	경찰청 사이버안전과장 이 재 훈(02-3150-2208)			진 우 경 경정 (02-3150-0252)

추석 명절기간 스미싱, 보이스피싱 피해 주의!!

- 이통3사와 협업하여 스미싱 피해예방을 위한 문자메시지 발송 -

- 과학기술정보통신부(장관 최기영), 방송통신위원회(위원장 한상혁), 금융위원회(위원장 은성수), 금융감독원(원장 윤석헌), 경찰청(청장 김창룡)은 추석 연휴를 앞두고 추석택배 배송 확인, 코로나19 관련 긴급재난 지원 및 결재 등을 사칭한 스미싱*이 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(보이스피싱, 전자상거래 사기, 기타 다양한 사기에 광범위하게 이용)

- 올해 8월까지 스미싱 탐지 건수는 전년 동기간 대비 378% 증가하였으며('19.1~8월 185,369건 → '20.1~8월 700,783건), 코로나19 관련 긴급재난지원금을 사칭한 스미싱도 등장('20.1~8월 10,753)하여 이용자의 각별한 주의가 요망된다.

□ 정부는 추석을 앞두고 관계부처 간 협업을 통해 스미싱, 보이스피싱 등 전기통신금융사기 피해 방지를 위해 예방 활동을 추진할 예정이다.

○ 과학기술정보통신부(한국인터넷진흥원)는 추석 연휴기간동안 스미싱 유포 등에 신속하게 대응할 수 있도록 24시간 모니터링을 실시하고,

- 유관기관과 스미싱 정보공유 등 신고·접수된 스미싱 정보를 분석하여 악성앱 유포지 차단 등 이용자 피해를 최소화할 계획이다.

※ 보호나라(<https://www.boho.or.kr>) 홈페이지 참조

○ 방송통신위원회는 한국정보통신진흥협회(KAIT), 이통3사(SKTEL, KT, LGU+)와 협력하여 9월 22일부터 각 통신사 명의로 「스미싱 피해 예방 문자」를 순차 발송하여 국민들의 주의를 당부할 계획이다.

※ 방송통신이용자정보포털(와이즈유저, <http://www.wiseuser.go.kr>) 참조

○ 금융위원회와 금융감독원은 최근 자녀사칭 및 허위 결제문자 스미싱 피해 증가에 대비하여 부모님들은 반드시 직접 확인*후 대응하고, 자녀들은 부모님께 자녀 사칭 스미싱 문자에 속지 않도록 미리 전화로 알려드릴 것을 당부하였고,

* 자녀가 문자를 발송한 것이 맞는지 직접 통화해서 확인, 카드사에 직접 결제내역을 확인

- 추석명절 보이스피싱 피해예방 안내장(붙임3)을 행정안전부 및 금감원 지원 등을 통해 대국민 홍보 자료로 배포할 예정이다.

※ 보이스피싱지킴이(<http://phishing-keeper.fss.or.kr>) 홈페이지 참조

○ 경찰청은 스미싱 피해 예방을 위해 경찰청 홈페이지와 사이버범죄 예방 앱인 '사이버캡'을 통해 피해 예방 수칙과 피해 경보 등을 제공하고,

- 추석 연휴 기간 전후로 주요 포털사와 중고물품거래기업 등과 협업하여 스미싱 등 사이버범죄 예방 홍보 활동을 전개할 계획이다.

※ 경찰청(<https://www.police.go.kr>) 홈페이지 참조

□ 이용자들은 스미싱 사기 피해를 예방하기 위해서는 아래 주의사항을 실천해야 한다.

△ 택배 조회, 명절 인사, 모바일 상품권·승차권·공연예매권 증정 등의 문자 속에 출처가 확인되지 않은 인터넷주소(URL)는 클릭하지 않을 것

※ 스미싱 문자 예시, 스미싱 피해예방 수칙 및 피해발생 시 행동요령 : 붙임 1, 2 참고

△ 알 수 없는 출처의 앱이 함부로 설치되지 않도록 스마트폰의 보안 설정을 강화하고, 앱 다운로드 시 출처가 불분명한 인터넷 주소 (URL)에서 다운로드 받지 않고 공인된 앱마켓을 통해 다운로드 및 앱을 설치할 것

△ 이통사 등에서 제공하는 백신프로그램을 설치하여 업데이트 및 실시간 감시상태를 유지할 것

※ 스미싱 피해예방 수칙 및 피해발생 시 행동요령 : 붙임 2 참고

△ 보안강화 및 업데이트 명목으로 개인정보·금융정보를 요구하는 경우 절대 입력하거나 알려주지 않을 것

△ 긴급재난지원금 안내 문자에는 인터넷주소(URL) 링크가 포함되지 않으므로 문자내용에 인터넷주소를 클릭하지 않고 즉시 삭제할 것

□ 명절 연휴 중 스미싱 의심 문자를 수신하였거나 악성앱 감염 등이 의심 되는 경우 국번없이 118상담센터로 문의하면 24시간 무료로 상담 받을 수 있다.

① 택배 관련 스미싱

<p>[배송 센터]{이름}주소정보가 맞지 않아 변경 후 상품 배송 new.so/xxx</p>	<p>{O*O택배} 주*문하신물품*미 배달사*유:도로*명불*일치.수 *정하세요:xx.ifxxxto.pro</p>
---	--

② 공공기관 사칭 스미싱

<p>민원조회 https://goo.gl/PRs7ft</p>	<p>2020 국민 건강검진 통*지*서 내용보기:k.gtyhn.ltd</p>
---	--

③ 지인 사칭·선물 관련 스미싱

<p>한가위이벤트에 당첨되어 선 물을 보내드립니다. 당첨된 선물 즉시 확인해보세요. http://falleynet/99ujh</p>	<p>추석연휴 소소하지만 가족과 함께 드실 수 있는 모바일 쿠폰 을 보내드렸습니다. http://HJK75/bkjkhg</p>
<p>추석명절 잘 보내시고 2020년 남은 시간 모두 모두 행복하세 요. ^.^~ http://hlino8/ny7089</p>	<p>추석명절 선물로 모바일 상 품권을 보내드립니다 지금 바로 확인 바랍니다. http://786hbuik/87</p>

④ 코로나19 사칭·긴급재난지원금 관련 스미싱

<p>전염병 발생 마스크 무료로 받아가세요. http://sxxxs.xyz/?qhogcd</p>	<p>코로나19확진자150명발생 환자이동경로는역학조사후 확인 http://mxxxt.xyz/ldxxdz</p>
<p>[긴급재난자금] 상품권이 도 착했습니다.확인해주세요. https://bit.ly/3xxxMel</p>	<p>7월추가 코로나19 재난지원금 www.coroona-19.net신청.</p>

* 자료 : 과기정통부(한국인터넷진흥원)

① 스미싱 피해예방 수칙



(링크 클릭주의) 출처가 미확인 문자메시지의
링크주소(숫자열 포함) 클릭 주의

※ 지인에게서 온 문자도 인터넷주소가 포함된 경우 클릭 前 확인



(스마트폰 보안설정 강화) 알 수 없는 출처의 앱 설치 제한

※ 설정방법 : 환경설정 > 보안 > 디바이스 관리 >

'알 수 없는 출처'에 V체크 해제



(백신프로그램 설치) 업데이트 및 실시간 감시상태 유지

※ (스미싱 방지앱 설치) 이통사 · 보안업체 제공



(소액결제 차단·제한)

자신의 스마트폰으로 114를 눌러 상담원과 연결



(금융정보 입력제한)

보안등급 명목으로 요구하는 보안카드번호 입력 금지

※ 스마트폰 등 정보저장장치에 보안카드 사진 · 비밀번호 등 저장 금지



(전자금융사기 예방서비스 가입) 공인인증서 PC지정,

SMS 사전인증 등 금융회사 제공 보안강화 서비스 적극 가입

② 스미싱 피해예방 대응요령 및 피해사례

출처 불명 파일 · 이메일 · 문자는 클릭하지 말고 삭제

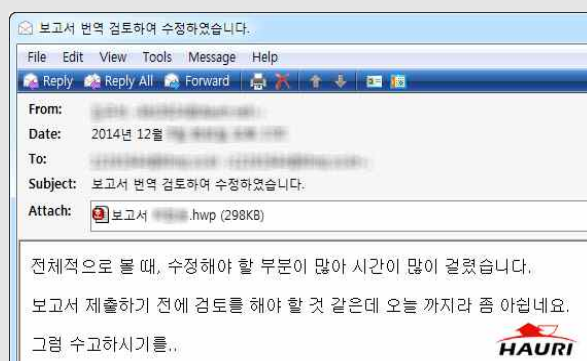
<대응요령>



<피해사례>

- 문서나 이미지 등을 가장한 파일, 정부기관이나 거래처 등을 사칭한 이메일 또는 문자를 통해 사용자의 PC나 휴대폰 등에 악성 코드를 설치하는 사례 증가

<악성코드 이메일 사례>



- ① '19.3월, 디자인 분야에 재직하는 피해자는 유명 작가 명의로 저작권을 위반했다는 항의 메일과 원본이미지 파일이라는 첨부파일을 송부받음
- ② 첨부파일을 클릭한 순간 피해자 PC의 파일들은 랜섬웨어에 의하여 모두 해제할 수 없도록 암호화되었으며 암호화를 해제하려면 비트코인을 입금하라는 요구를 받음

③ 스미싱 피해발생 시 행동요령

⇒ 【행동요령】

- ① 금융기관 콜센터 전화 : 경찰서에서 발급받은 '**사건사고 사실 확인원**'을 이동통신사, 게임사, 결제대행사 등 관련 **사업자에 제출**
- ② 악성파일 삭제 : **스마트폰 내 '다운로드' 앱 실행** → 문자를 클릭한 시점 이후, 확장자명이 apk인 파일 저장여부 확인 → 해당 **apk파일 삭제**
※ 삭제되지 않는 경우, 휴대전화 서비스센터 방문 또는 스마트폰 초기화
- ③ 한국인터넷진흥원 118상담센터(**국번없이 118**) 상담
- ④ 금융 및 증권 등 **공인인증서 즉시 폐기** 및 **재발급받기**
- ⑤ 이동통신사에 **모바일 결제내역 여부 확인**
- ⑥ 사용 중인 **이동통신사에서** 제공하는 스미싱 **예방서비스(App 등)** 설치 및 활용
- ⑦ **주변 지인들에게** 스미싱 피해 사실을 즉시 알려 **2차 피해 발생 사전 방지**
- ⑧ 문자메시지 등으로 수신된 **금융회사 및 공공기관의 홈페이지**는 반드시 **인터넷 검색 등을 통해 정확한 주소인지 확인**

* 자료 : 과기정통부(한국인터넷진흥원), 금융위(금융감독원), 경찰청

추석 명절 보이스피싱 피해발생 주의!



가족사칭! 선물주문 악용! 추석 택배안내! 소액결제 안내!
명절인사 가장! 등 추석 명절을 노린 보이스피싱 주의!

주요 사례 및 소비자 행동 요령

☹️ 엄마 나 문화상품권 엄마 명의로 사게 엄마 신분증 좀 사진 찍어서 보내 줘. 네 각이 잘 나오게~ 부탁해요!

☹️ [Web 발신]
 <한국택배> 운송장 번호
 【3602****6796】 주소지 미확인
 반송처리 확인
<http://u6gg/atcFH>

☹️ ☺️ (〇〇) 추석 잘 보내시고 2020년 남은 시간 모두 모두 행복하십시오.
<http://wozkr/mhqd>

☹️ [Web 발신]
 <입금> 980,000 원 09/09 23:26
 301032-53-*****46
 잔액 13,938,938원

☹️ [Web 발신]
 주문하신 안마의자 57만 3000원
 결제되었습니다. 주문내역 확인
<https://googl/g6fkXn>

- ◎ **가족사칭 보이스피싱**
 ▷ 문자/SNS를 통한 신분증, 금전 요구 시
무조건 거절 후 가족여부 재확인 필요
- ◎ **선물주문 악용 보이스피싱**
 ▷ 선물주문 오류입금 차액 재이체 요청 시
실제 이체내역 확인 등 사실관계 재확인
- ◎ **추석 택배안내 보이스피싱**
 ▷ 확인되지 않은 택배안내 문자의
인터넷주소(Ur)는 절대 클릭 금지
- ◎ **소액결제 안내 보이스피싱**
 ▷ 결제내역 확인을 유도하는 전화번호나
인터넷주소(Ur)는 절대 클릭 금지
- ◎ **명절인사 가장 보이스피싱**
 ▷ 지인의 명절인사를 가정한
인터넷주소(Ur)는 절대 클릭 금지

보이스피싱 발생시에는 지체없이 금융회사 상담센터 및 금융감독원 콜센터 1332로 지급정지 요청!

보이스피싱 피해 예방법

보이스피싱 피해예방을 위한 금융서비스를 “꼭” 신청하세요! (고령층은 필수 가입필요)



자연이체서비스	- 수취인 계좌에 일정시간 경과 후 입금
입금계좌 지정 서비스	- 미리 지정한 계좌로는 자유롭게 송금 - 지정하지 않은 계좌로는 소액 송금만 가능
단말기 지정 서비스	- 미리 지정한 PC, 스마트폰 등에서만 이체 등 주요 거래 가능
해외 IP 차단 서비스	- 국내 사용 IP대역이 아닌 경우 이체거래가 불가능하게 차단 (정보유출 또는 해킹 등을 통한 해외 금전인출 방지)
개인정보노출자 사고예방시스템	- 개인정보 노출 혹은 명의도용 의심 시 정보등록을 통한 금융사고 예방 (Site 주소 ▶ http://fine.fss.or.kr)