

 > 알림마당 > 보안공지

청첩장 등 지인 사칭 스미싱 주의 권고

2025-03-11

 250311_청첩장_등_지인_사칭_스미싱_주의_권고_v1.2.pdf

□ 개요

- 최근, 온라인 청첩장을 사칭해 스미싱 악성앱을 유포하는 사례가 증가됨에 따라 악성앱 감염에 의한 개인정보 등 민감정보 탈취, 금전피해로 연계되지 않도록 사용자 주의 필요
 - 특히, 악성앱에 감염된 휴대전화의 연락처를 통해 지인 명의로 재유포되므로 온라인 청첩장 수신 시 메시지 내 포함된 인터넷 주소(URL) 클릭 주의

□ 주요내용

- “결혼”, “결혼식”, “청첩장” 등의 키워드를 활용, 결혼식 정보 확인을 위한 악성앱 설치를 유도하는 스미싱 유포 사례 증가
 - 특히, 스미싱 문자 발신번호를 수신자 스마트폰에 저장된 연락처나 일반 휴대전화번호로 표기됨에 따라 실제 지인이 보낸 문자로 오인하도록 유도
 - 또한, 악성앱이 정상앱과 동일한 아이콘을 사용함에 따라 육안 판별 불가
- 악성 앱은 설치 후 실행 시 아래와 같은 행위를 수행하여 2차 피해로 연계될 수 있으므로 사용자 주의 필요
 - ① 설치 후 아이콘 은닉을 통해 사용자가 설치 사실을 인지 못 하도록 함
 - ② 스마트폰 내 저장된 연락처, 문자 메시지, 사진 등 개인정보 유출
 - ③ 공동인증서 수집 등을 한 금융정보 탈취
 - ④ 피해자 폰을 통한 문자 메시지 발송, 삭제 등의 원격제어 수행
 - 특히 피해자 폰에 저장된 연락처 대상 스미싱을 발송하여 수신자가 의심없이 악성앱을 설치하는 피해 발생

□ 대응방안

- 스미싱 문자 신고 및 확인 방법
 - 스마트폰 내 문자 수신 화면에서 확인가능한 ‘스팸으로 신고’
 - 보이스피싱통합신고대응센터 내 ‘스미싱 문자메세지 차단 신고하기’
 - 보호나라(카카오톡 채널) 내 ‘스미싱 확인서비스’를 이용하여 신고 및 악성여부 판별
- 스미싱 문자 예방 방법
 - 문자 수신 시 출처가 불분명한 사이트 주소는 클릭을 자제하고 바로 삭제
 - 의심되는 사이트 주소의 경우 정상 사이트와의 일치여부를 확인하여 피해 예방

- 정부기관 및 금융회사인 경우, 전화나 문자 등을 통해 원격제어앱 설치를 요구하지 않음
- ※ 정상스토어에 등록된 앱인 경우도 포함

○ 번호 도용 문자 발송 차단

- 악성앱 감염 및 피싱 사이트를 통한 정보 유출이 의심되는 경우, 스미싱 문자 재발송을 위해 피해자 번호가 도용될 수 있으므로 “번호도용문자차단서비스*”를 신청하여 번호 도용 차단
- ※ 이동통신사별 부가서비스 항목에서 무료로 신청 가능

○ 모바일 결제 확인 및 취소

- 스미싱 악성앱 감염 및 피싱사이트 개인 정보 입력 시 모바일 결제 피해가 발생할 수 있으므로 모바일 결제 내역 확인
 - ① 통신사 고객센터를 통하여 모바일 결제 내역 확인
 - ② 모바일 결제 피해가 확인되면 피해가 의심되는 스미싱 문자 캡처
 - ③ 통신사 고객센터를 통해 스미싱 피해 신고 및 소액결제확인서 발급
 - ④ 소액결제확인서를 지참하여 관할 경찰서 사이버수사대 또는 민원실을 방문하여 사고 내역 신고
 - ⑤ 사고 내역을 확인받고 사건사고 사실 확인서 발급
 - ⑥ 사건사고 사실 확인서 등 필요서류를 지참하여 통신사 고객센터 방문 또는 팩스나 전자우편 발송
 - ⑦ 통신사나 결제대행 업체에 사실 및 피해 내역 확인 후 피해보상 요구

○ 악성어플리케이션 삭제

- 문자메시지에 포함된 인터넷주소를 클릭한 것만으로는 악성 앱에 감염되지 않으나 인터넷주소를 통해 어플리케이션을 설치했다면 아래와 같은 방법으로 스마트폰 점검
 - ① 모바일 백신으로 악성 앱 삭제하기
 - ② 악성앱 수동 삭제하기
 - ③ 서비스센터 방문

○ 공인인증서 폐기 및 재발급하기

- 악성 앱에 감염되었던 스마트폰으로 금융서비스를 이용했다면 공인인증서, 보안카드 등 금융거래에 필요한 정보가 유출될 가능성이 있으므로 해당 정보를 폐기하고 재발급

○ 2차 피해 예방하기

- 스마트폰에 설치된 악성앱이 주소록을 조회하여 다른 사람에게 유사한 내용의 스미싱을 발송하는 등 2차 피해가 발생할 수 있으므로 주변 지인에게 스미싱 피해 사실을 알려야 함

□ 기타 문의

한국인터넷진흥원 인터넷침해대응센터 : 국번없이 118

□ 작성 : 국민피해대응단 스미싱대응팀

[개인정보처리방침](#)[FAQ](#)[RFC 2350](#)[KISA 대국민서비스 바로가기](#)

해킹·스팸개인정보침해 상담은 118

나주본원) 58324 전라남도 나주시 진흥길 9 한국인터넷진흥원
서울청사) 05717 서울시 송파구 중대로 135 (가락동) IT벤처타워
대표번호 : 1433-25(수신자 요금 부담) [해킹·스팸개인정보침해 상담 118]

Copyright(C) 2023 KISA. All rights reserved.