

공공기관 사칭 해킹메일을 통한 악성앱 유포 등 스미싱 주의

□ 개요

- 최근 공공기관, 금융기관 등을 사칭하여 개인정보를 탈취하거나 모바일 환경에서 악성앱 설치를 유도하는 해킹메일이 지속적으로 유포되고 있어 피해가 발생하지 않도록 주의 필요

□ 주요내용

- “범죄 연루”, “법규 위반”, “개인정보 유출 피해 보상” 등의 키워드를 활용한 해킹 메일을 유포하여 피싱사이트 접속 및 모바일 악성앱을 설치하도록 유도
 - (공공기관 사칭) “이용정지”, “출석 요구”, “소명 절차” 등의 내용으로 해킹메일 발송 후 악성 인터넷주소(URL) 클릭을 유도해 피싱사이트 접속 및 악성앱 설치 유도
 - (기업 사칭) “피해 보상” “보상금 지급” 등 관련 키워드를 악용해 피해 보상금 수령을 위한 개인정보 입력을 유도하는 피싱사이트 유포

[간급] 고객님의 회선 이용정지 예정 통보 고객님의 명의로 대량의 스팸 문자가 발송된 이력이 확인되어 타인 피해 방지를 위해 회선 이용정지가 진행될 예정입니다. 이용정지 유예 신청 및 본인확인을 원하시면 아래 링크에 접속하여 인증번호를 입력해주시기 바랍니다. [SP] 이용정지 유예 신청하기 URL	[국가수사기관] '금융사기 의심계좌 전면 지급정지 예고' 및 출석요구 귀하 명의의 계좌가 금융사기에 가담된 정황이 있어 계좌 지급정지가 예정되어 있습니다. 자세한 출석 요구 내용과 소명 절차는 아래 링크를 통해 확인하시기 바랍니다. [SP] 출석요구서 및 소명서 양식 다운로드 URL	[알림] 개인정보 유출 피해에 따른 보상금 지급 안내 귀하의 개인정보 유출에 대한 보상금 지급 대상으로 선정되었습니다. 보상금 수령을 위해 안내해 드리는 링크에서 신청해주시기 바랍니다. [SP] 보상금 수령하기 URL
--	--	---

해킹메일 유포(예상) 문구

□ 대응방안

○ URL 신고 및 확인 방법

- 보호나라(카카오톡 채널) 내 ‘스미싱·피싱 확인서비스’를 이용하여 신고 및 악성여부 판별



- 전기통신금융사기통합신고대응센터(<https://conterscam112.go.kr>) 내 ‘스미싱 문자 신고’
- 보호나라(카카오톡 채널) 내 ‘스미싱·피싱 확인서비스’를 이용하여 신고 및 악성여부 판별



o 해킹메일 예방 방법

- 이메일의 보낸 주소를 꼼꼼히 확인하고, 모르는 이메일 및 첨부파일 열람 금지
- 이메일 본문 내의 링크로 접속한 경우 서비스 제공업체의 정상 사이트와 일치 여부를 확인하고 일치하지 않을 시 계정정보 등 개인정보 입력 금지

o 시스템 및 소프트웨어 최신 업데이트

- 운영체제 및 문서 프로그램을 최신 버전으로 유지

o 백신 소프트웨어 관리

- 바이러스 백신을 최신 상태로 유지하고 정기적인 검사를 수행

o 악성 어플리케이션 설치 시 삭제

- 인터넷주소를 클릭한 것만으로는 악성 앱에 감염되지 않으나, 인터넷주소를 통해 어플리케이션을 설치했다면 아래와 같은 방법으로 스마트폰 점검
 - 모바일 백신으로 악성 앱 설치여부 검사 및 발견시 비행기모드 전환 후 112신고
 - ※ 악성 앱이 휴대폰을 원격제어할 수 있으므로 주변 사람의 전화기를 통해 신고
 - 악성 앱 수동 삭제하기
 - 가까운 휴대폰 서비스센터 방문

o 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

□ 스미싱 제보 및 상담 문의

- 전기통신금융사기 통합신고대응센터 : 국번없이 1394
- 한국인터넷진흥원 인터넷침해대응센터 : 국번없이 118

□ 작성 : 국민피해대응단 스미싱대응팀

□ 공공기관 사칭 해킹메일을 통한 사기 시도 사례

※ 출처 : 전기통신금융사기 통합대응단

- (검찰 사칭 피싱) 검찰을 사칭하여 사건에 연루되었다며 네이버 메일로 구속영장 전송 / 수사용 휴대폰을 개통하도록 유도한 후 원격제어 앱 설치를 유도하고, 은행앱을 설치하게 하여 대출 실행 / 대출금 보관 중 인입하여 피해 예방한 사례



검찰 사칭 피싱 - 피해예방 사례

검찰을 사칭한 사람이 '사건에 연루됐다'며 겁을 주고, 가짜 서류와 앱 설치를 유도해 대출까지 받게 하려 한 사례입니다. 상담과 신고가 접수되어 추가 피해를 막았습니다.



1. 갑작스러운 메일

사건에 연루되었습니다. 첨부된 구속영장을 확인하세요.



검찰을 사칭한 메일로 불안감을 조성합니다.

2. 수사용 휴대폰 개통 유도

수사 협조를 위해 새 휴대폰을 개통하세요.



'수사 협조'라는 말로 새 휴대폰 개통을 요구합니다.

3. 원격제어 앱·은행앱 설치, 대출 유도

앱을 설치하고 시키는 대로 진행하세요.



원격제어 앱 설치 후 은행앱을 이용하게 해 대출까지 유도합니다.

4. 상담·신고로 추가 피해 예방

상담받길 잘했어요!

검찰은 메일·전화로 앱 설치나 대출을 요구하지 않습니다!



대출금을 넘기기 전 상담과 신고가 접수되어 추가 피해를 막았습니다.



예방 포인트

- 검찰·경찰은 전화나 메일로 앱 설치, 새 휴대폰 개통, 대출을 요구하지 않습니다.
- 원격제어 앱 설치 요구는 즉시 중단하세요.
- 의심되면 가족·지인과 상의하고 즉시 신고하세요.

※ 위 이미지는 생성형AI를 활용하여 제작하였습니다.

- (공공기관 사칭) '금융사기 의심계좌 전면 지급정지 예고통지', '출석요구서' 등 금감원·경찰청 사칭 메일 수신 / 휴대폰, PC를 통해 메일 내 링크 클릭 후 개인정보 입력 / 악성앱 점검 과정에서 불법 apk파일이 발견되어 삭제

금감원·경찰청 사칭 해킹 메일 사례

금융감독원과 경찰청을 사칭한 메일을 믿고 링크를 눌러 개인정보를 입력한 뒤, 휴대폰 점검 과정에서 여러 개의 악성 앱이 발견된 사례입니다.

1. 공문처럼 보이는 메일 수신



공공기관을 사칭한 메일로 긴장감을 유발합니다.

2. 링크 클릭 후 개인정보 입력



메일 속 링크를 누르면 가짜 사이트로 연결되어 개인정보 입력을 유도합니다.

3. 휴대폰 점검 과정에서 악성 앱 발견



점검 결과, 출처를 알 수 없는 APK 파일 23개가 발견되었습니다.

4. 삭제·조치 후 피해 확산 차단



악성 앱 삭제와 계정 점검 등 필요한 조치를 진행했습니다.



- ✓ 기관을 사칭한 메일의 링크는 바로 누르지 마세요.
- ✓ 개인정보·인증정보 입력 전 공식 홈페이지인지 확인하세요.
- ✓ 출처를 알 수 없는 앱(APK)은 설치하지 말고 즉시 점검받으세요.

※ 위 이미지는 생성형AI를 활용하여 제작하였습니다.

- (한국통신안전정보원 사칭 피싱메일)한국통신안전정보원(span-notice@kisop.com)을 사칭, 민원인의 휴대폰 번호로 대량의 스팸문자 발송 이력이 감지되어 회선 이용정지를 통보하는 내용의 메일 발송하고 이용정지 유예하는 링크 접속하여 인증번호 등을 입력하도록 유도

한국통신안전정보원 사칭 피싱메일 사례

‘휴대폰 번호로 대량 스팸문자가 발송됐다’며 회선 이용정지를 통보하고, 정지를 미루려면 링크에 접속해 인증번호를 입력하라고 속인 사례입니다.

1 이용정지 통보 메일



공공기관처럼 보이는 발신 주소와 문구로 불안감을 줍니다.

2 ‘정지 유예’ 링크 클릭 유도



급한 상황처럼 꾸며 링크 접속을 유도합니다.

3 인증번호·개인정보 입력 요구



가짜 인증 화면에서 인증번호와 개인정보 입력을 요구합니다.

4 의심 후 중단·상담



수상함을 느끼고 접속을 중단해 피해를 막았습니다.



예방 포인트

- ✓ ‘회선 정지’, ‘본인 확인’ 등 긴급 문구는 한 번 더 의심하세요.
- ✓ 메일 속 링크 대신 공식 홈페이지나 고객센터로 직접 확인하세요.
- ✓ 인증번호는 타인에게 알려주거나 입력하기 전 반드시 확인하세요.

※ 위 이미지는 생성형AI를 활용하여 제작하였습니다.