

정부부처·유관기관 직원을 사칭한 스미싱 소비자 경보 발령!!!

■ 소비자경보 2024 - 2호

등급	주의	경고	위험
대상	금융소비자 일반		

소비자경보 내용

- ◆ 최근 정부부처·유관기관 임직원을 대상으로 부고·결혼 등을 빙자한 출처 미상의 스미싱* 문자가 확산되고 있어 각별한 주의를 당부

* 문자메시지(SMS)+피싱(Phishing)의 합성어로 악성앱 주소(url)이 포함된 휴대폰 문자(SMS)나 카카오톡 등 SNS 메시지를 대량 전송 후 이용자가 클릭하도록 유도하여 개인정보 등을 탈취하는 수법

1 사기 수법

- 정부부처 직원의 지인을 사칭한 사기범이 출처가 의심스러운 url 이 포함된 부고 문자(카카오톡 메시지)를 피해자에게 발송
 - 피해자가 해당 url을 클릭하면 피싱사이트로 연결되면서 피해자의 휴대전화에 저장된 개인정보 및 정부부처 관계자를 포함한 지인의 연락처를 탈취*

* 악성앱·불법프로그램이 사용되는 것으로 추정

- 탈취한 개인정보로 피해자가 근무중인 정부부처의 직원 등 지인에게 2차·3차 문자메시지를 송부하여 개인정보 탈취를 반복하고 메신저피싱 등에 악용

※ <별첨> 직장동료를 사칭한 스미싱 사례

2 소비자 행동 요령

□ 출처가 불분명한 모바일 부고장 · 청첩장 URL주소는 절대 클릭 금지!

- 사기범이 보낸 출처가 의심스러운 URL주소를 클릭할 경우 원격 조종 악성앱이 설치되고 개인정보가 모두 유출되어 피해가 발생*할 수 있으니 의심스러운 URL주소를 절대 클릭하지 않도록 당부

* 반드시 정식 앱마켓(구글플레이, 애플스토어 등)을 통해서만 앱을 다운로드하고, 수상한 사람이 보낸 앱 설치 요구는 절대로 응해서는 안됨

- 악성앱을 이미 설치했다면 ①모바일 백신앱(최신 버전 업데이트)으로 검사후 삭제, ②데이터 백업 후 휴대폰 초기화, ③지인이나 휴대폰 서비스센터 등에 도움을 요청해야 함

□ 보이스피싱 피해 발생시 신속히 지급정지 요청!

- 금융회사 콜센터 또는 금융감독원 콜센터(☎1332)에 전화하여 해당 계좌 지급정지를 요청하고 피해구제를 신청해야 하며,
- 개인정보 유출시 추가 피해 예방을 위해 금융감독원 금융소비자 정보포털 '파인'의 「개인정보 노출자 사고예방 시스템*」을 활용

* 신청인이 직접 개인정보를 등록하면 신규 계좌개설, 신용카드 발급 등이 제한됨

- 「계좌정보 통합관리서비스(www.payinfo.or.kr)」를 활용하여 본인 모르게 개설된 계좌 또는 대출을 한눈에 확인할 수 있음
- 본인 모르게 개통된 휴대폰을 조회하거나 추가 개통을 차단하기 위해서는 「명의도용 방지서비스(www.msafes.or.kr)」의 가입사실 현황조회 또는 가입제한 서비스 등을 이용할 수 있음

담당 부서 <총괄>	금융위원회 금융안전과	책임자	과 장	김수호 (02-2100-2976)
		담당자	사무관	남명호 (02-2100-2974)
<공동>	금융감독원 금융사기대응1팀	책임자	국 장	임정환 (02-3145-8150)
		담당자	팀 장	장종현 (02-3145-8140)

