



국가정보자원관리원 화재 상황을 악용한 보이스피싱·스미싱 주의

- 인터넷주소(URL)·링크가 포함된 문자메시지는 클릭하지 말고 112 신고
- 앱 재설치·재가입은 공식 앱 마켓을 이용하고, 출처가 불분명한 앱은 삭제

9월 30일, 경찰청 「전기통신금융사기 통합대응단」에 국가정보자원관리원 화재 상황을 악용한 피싱 범죄 시도에 대한 제보가 접수되었다.

범인은 특정 업체의 온라인 쇼핑몰에서 물품을 구매한 이력이 있는 소비자에게 전화를 걸어 환불을 안내한다는 명목으로 가짜 사이트 링크를 전달했다. 소비자가 링크에 접속하여 환불 정보 입력을 위해 개인정보를 입력하고 ‘환불 신청’ 버튼을 누르자, ‘국가정보자원관리원 화재로 인해 서비스가 중단되고 있다.’라는 안내 팝업 이미지가 나타났다.

범인은 서비스 중단 시에 사용되는 앱이라며 소비자에게 악성 앱 파일을 전송하고 설치를 유도했다. 다행히 소비자가 이상한 낌새를 느끼고 즉시 경찰에 신고하였기에, 범행 시도가 실제 피해로 이어지지는 않았다.

경찰청(청장직무대행 유재성)은 국가정보자원관리원 화재로 인한 행정 서비스 일시 중단과 관련하여 대체 사이트 접속이나 앱 재설치를 유도하는 수법의 보이스피싱·스미싱 범행에 대한 주의를 당부했다.

위 사건과 같이 범죄조직은 다양한 방식으로 화재 상황을 악용할 수 있다. 대표적으로 정부 부처 대체 사이트로 바로 접속할 수 있는 링크를 제공한다는 미끼문자를 발송하여 악성앱을 설치하게 하거나, 문자나 전화를 이용해 가짜 누리집 접속을 유인하는 등의 수법이 예상된다. ‘행정서비스 복구 과정에서 앱 재설치나 재가입 등이 필요하다.’라며 악성 앱 설치를 유도하는 범행 시도도 주의해야 한다.

< 보이스피싱·스미싱 예방 수법 >

【보이스피싱】 ①국가정보자원관리원 화재로 인한 행정 시스템 마비·오류로 금융 정보가 유출된 것처럼 속여 가짜 고객센터로 연락 유도 → ②범죄에 연루된 것처럼 기망 → ③자금을 이전할 것을 유도

【스미싱】 ①정부기관 앱 재설치·대체 사이트 안내를 빙자한 문자메시지 발송 → ②인터넷주소(URL) 클릭 시 악성 앱 설치 → ③개인정보 탈취·자금 이체 → ④탈취한 개인정보를 악용, 범죄 연루 기망 등 추가 범행

피해를 예방하기 위해서는 행정서비스를 제공하는 누리집 또는 주요 포털사이트 정부 공지 페이지에서 확인한 대체 사이트만 접속하고, 대체 사이트 인터넷주소(URL)·링크가 포함된 문자메시지는 클릭하지 말아야 한다. 특히, 금전 이체가 필요한 교통범칙금, 건강보험료, 국세 납부 등이 범죄에 활용될 가능성이 높으므로 각별히 주의해야 한다.

정부 부처 및 공공기관은 앱 재설치나 재가입 등을 문자·전화로 요구하지 않으며, 문자메시지·메신저 링크를 통해 앱 설치를 유도할 경우 사기 범행 수법이므로 유의해야 한다. 스마트폰에는 반드시 공식 앱 마켓을 통해서만 앱을 설치하고, 출처가 불분명한 앱은 삭제해야 한다. 또한 '알 수 없는 출처 앱 설치 허용'을 차단하고, 운영체제(OS) 앱은 항상 최신 버전으로 업데이트해야 한다.

경찰청에 설치된 「전기통신금융사기 통합대응단」은 112 또는 통합신고 누리집(www.counterscam112.go.kr) 등을 통해 보이스피싱·스미싱 범죄 관련 신고·제보를 24시간 접수하고 있다. 경찰청은 대체사이트 사칭 인터넷 주소(URL)가 확인되는 즉시 한국인터넷진흥원(KISA)을 통해 차단하고, 범죄 피해가 발생한 경우 전담 수사팀을 투입하여 적극 수사할 계획이다.

경찰 관계자는 “정부는 국민에게 인터넷주소(URL)나 링크가 포함된 문자메시지를 보내지 않는다.”라고 강조하면서, “대체 사이트나 앱 재설치·재가입을 안내한다는 문자에 인터넷주소(URL)나 링크가 포함되어 있는 경우, 클릭하지 말고 112로 신고해 주시길 바란다.”라고 당부하였다.

담당 부서	경찰청 수사국 경제범죄수사과	책임자	총경	박 찬 우	(02-3150-2037)
		담당자	경정	박 상 현	(02-3150-3438)

