금융위원회	보도참고자료	금융감독원

보도시점 배포 시 배포 2025.9.30.(화)

정부 행정정보시스템 장애와 관련한 금융회사 사칭 스미싱을 주의하세요!

- 국가정보자원관리원 화재 관련 스미싱 소비자경보 발령(주의) -

▣ 소비자경보 2025 - 24호			
등급	주의	경고	위험
대상	금융소비자 일반		

소비자경보 내용

□ 9월 26일(금) 발생한 **국가정보자원관리원**(이하 "국정자원") **화재**로 인한 **행정정보시스템**의 **장애**로 **일부 서비스 이용**이 **제한**되고 있습니다.

○ 이에, 동 상황을 악용하여 **금융 앱**을 **가장**한 **악성 앱 설치***, **신분증 사진** 등 **개인정보 요구 스미싱 발생**이 **우려**됨에 따라 **소비자경보(주의)**를 **발령**합니다.

* '22년 카카오 데이터센터 화재 발생 당시, 카카오톡 설치파일을 위장한 악성 앱 유포, 사용자 확인을 빌미로 피싱사이트를 통한 정보입력 요구 등의 스미싱 수법이 기승

□ 금융회사는 **문자메세지 URL**을 통해 **금융 앱 설치파일**을 **제공**하거나 **임시 홈페이지**를 통한 **정보입력**을 **요구하지 않습니다.**

○ 금융회사를 사칭한 문자메시지 **URL 접속**시 **개인정보 노출** 및 **금융피해**가 **발생**할 수 있으니, **절대 클릭하지 마시기 바랍니다.**

□ 금융당국은 국정자원 화재 관련 **신규 스미싱 시도**에 대한 **모니터링**을 **강화**하고 **피해사례 다수 발생시 소비자경보**를 **격상**하는 등 **신속히 대응**토록 하겠습니다.

<소비자 유의사항>

1. **문자메세지에 포함된 출처가 불분명한 인터넷주소(URL)는 절대 클릭 금지**
2. **정부 전산시스템 장애로 인한 임시 본인인증 명목으로 신분증 등 개인정보·금융정보 요구시 진행 중단**
3. **휴대폰 보안 위험 자동 차단기능 설정(안드로이드)**
4. **금융피해 예방을 위한 안심차단서비스, 명의도용 방지 서비스 적극 이용**

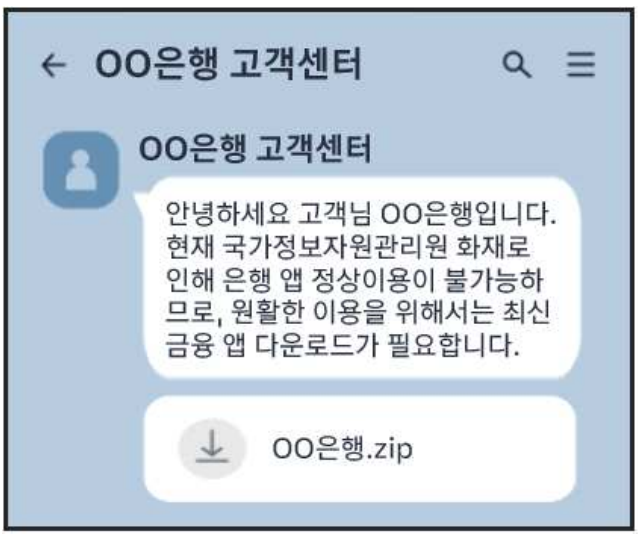
1. 소비자경보 발령 배경

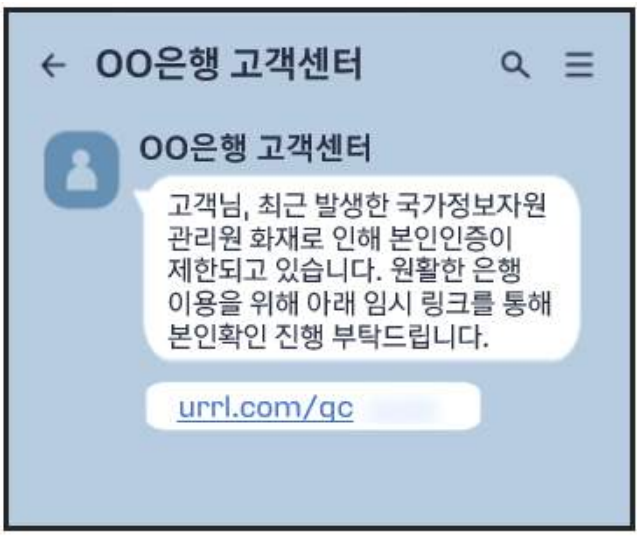
□ 9월 26일(금) 발생한 **국가정보자원관리원**(이하 "국정자원") **화재**를 악용해 **금융 앱**을 **가장**한 **악성 앱 설치*, 신분증 사진 요구** 등 **스미싱 발생**이 **우려**되는 상황입니다.

* '22년 카카오 데이터센터 화재 발생 당시, 카카오톡 설치파일을 위장한 악성 앱 유포, 사용자 확인을 빌미로 피싱사이트를 통한 정보입력 요구 등의 스미싱 수법이 기승 (출처 : 한국인터넷진흥원 보호나라)

□ 이에 금융당국은 국정자원 화재와 관련한 **스미싱 피해 예방**을 위해 **소비자 유의사항**을 **안내**하고 **소비자경보(주의)**를 **발령**합니다.

국정자원 화재 관련 발생 가능 스미싱(예시)





2. 금융당국의 대응

□ 9.29(월) 금융당국은 국정자원 화재 관련 금융권 **신속 대응체계**를 **가동**하여 **스미싱 피해 관련 유의사항 전파** 및 **피해사례 발생시 즉시보고**토록 **당부**하였습니다.

○ 금융회사는 문자메세지 **URL**을 통해 **금융 앱 설치**를 **권유하지 않는 점, 임시 홈페이지**를 통한 **정보입력**을 **요구하지 않는 점**을 **적극 안내***할 예정입니다.

* 금융회사 모바일 앱, 홈페이지, 콜센터 등을 활용

□ 앞으로 금융당국은 국정자원 화재 관련 **새로운 스미싱 시도**에 대한 **모니터링**을 **강화**하고 **실제 피해사례 발생**시 **신속히 전파**하는 등 **적극 대응**토록 하겠습니다.

3. 소비자 유의사항

□ 문자메세지에 포함된 출처가 불분명한 URL주소는 절대 클릭 금지

○ 사기범이 보낸 **출처가 의심스러운 URL주소** 클릭시 **악성앱**이 설치되어 **개인정보 유출** 및 **금융피해**가 발생*할 수 있으니 **절대 클릭하지 마세요.**

* 반드시 **정식 앱마켓(구글플레이, 애플스토어 등)**을 통해서만 앱을 다운로드하고, **신원이 확인되지 않은 사람**이 보낸 **앱 설치 요구**는 절대로 **응해서는 안됨**

악성앱의 주요 기능

◆ **발신번호 조작** : 피해자 휴대폰에 표시되는 발신 전화번호를 112 등 임의의 번호로 조작
◆ **전화 가로채기** : 피해자 휴대폰의 통화 기능을 제어(강제수신·강제발신)
◆ **개인정보 탈취** : 휴대폰에 저장된 신분증, SMS, 연락처 등 모든 개인정보를 탈취
◆ **원격제어** : 사기범이 피해자 휴대폰의 모든 기능을 통제

□ 정부 전산시스템 장애로 인한 임시 본인인증 명목으로 신분증 등 개인정보 · 금융정보 요구시 진행 중단

○ 사기범은 금융기관 등을 사칭해 **가짜 웹페이지**를 **제작**하여 **정보**를 **탈취**하므로 **개인·금융정보 요구시 즉시 진행**을 **중단**하고 **공식 홈페이지 주소**를 확인하세요.

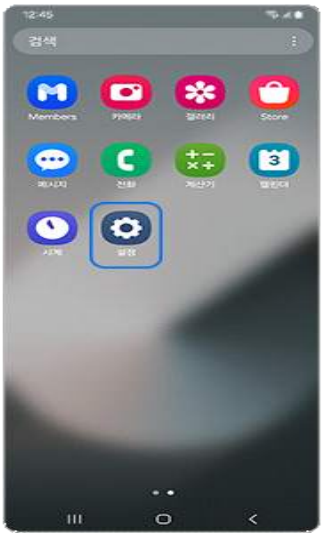
가짜 웹페이지 사례

□ 휴대폰 보안 위험 자동 차단기능 설정(안드로이드)

○ 악성앱 설치로 인한 **정보 탈취 방지***를 위해 **사전에 휴대폰 보안설정**을 **강화**하세요.

* SMS·연락처·사진 탈취, 전화 강제 수·발신 등

휴대폰 보안설정 강화(안드로이드)



1. 스마트폰 '설정' 앱 클릭

2. '보안 및 개인정보 보호' 메뉴 접속

3. '보안 위험 자동 차단' 활성화

○ 악성앱을 **이미 설치**했다면 ①**모바일 백신앱**(V3, 시티즌코난 등)으로 **검사 후 삭제**, ②**휴대폰 초기화**, ③**한국인터넷진흥원 상담센터**(☎118)에 **도움을 요청하세요.**

□ 금융피해 예방을 위한 안심차단서비스, 명의도용 방지 서비스 적극 이용

○ **개인정보 유출** 등으로 **본인이 모르게 대출, 신규계좌개설**이 무단으로 이루어지는 것을 **사전에 차단**할 수 있도록 **안심차단 서비스**를 **적극 이용**하세요.

- 거래중인 금융회사 **영업점***을 **방문**하거나, **은행 모바일앱**을 통해 **간편하게 신청**할 수 있습니다.

  * 은행, 저축은행, 농협, 수협, 신협, 새마을금고, 산림조합, 우체국

○ 또한 **본인 모르게 개통된 휴대폰을 조회**하거나 **추가 개통을 차단**하기 위해 『**명의도용 방지서비스**(www.msafer.or.kr)』를 **이용**해보세요.

담당 부서	금융위원회	책임자	서기관	김태훈 (02-2100-2970)
<총괄>	금융안전과	담당자	사무관	유은지 (02-2100-2974)
<공동>	금융감독원	책임자	국 장	정재승 (02-3145-8150)
	금융사기대응총괄팀	담당자	팀 장	김태근 (02-3145-8130)