금융감독원	**보 도 참 고**	금융은 튼튼하게 소비자는 행복하게

보도	2022.5.13.(금) 조간	배포	2022.5.12.(목)

담당부서					
감독총괄국 검사분석팀	책임자	팀 장	유명신	(02-3145-8290)
	담당자	조사역	류영현	(02-3145-8294)
불법금융대응단 금융사기대응팀	책임자	팀 장	고병완	(02-3145-8521)
	담당자	선임조사역	박동현	(02-3145-8534)

금융꿀팁 200선 - ⑯ 개인정보노출자 사고예방시스템 안내

신분증 분실 혹은 피싱 의심시 개인정보노출자 사고예방시스템에 등록하세요

주요 내용

□ 금융감독원은 유출된 개인정보로 타인이 **금융거래**를 함으로써 발생할 수 있는 (명의도용) 피해를 예방하기 위하여 **「개인정보 노출자 사고예방 시스템*」**을 **운영중**('03.9월~)

* 금융이용자가 신분증 분실 등으로 개인정보 노출 우려시 금감원 소비자포털 '파인'에 등록하여 명의도용을 예방하는 시스템으로 개인업무 취급 전체 금융회사와 연결하여 개인정보 노출사실 및 해제 사실을 실시간(real-time) 전파

시스템 운영방식

◇ 개인정보 노출사실이 등록되면, 해당 정보가 금융협회를 통해 실시간 금융회사에 전달되어 **영업점 단말기**에 **'본인확인 주의'** 문구가 게시

○ 영업점 직원은 **통상 이상**의 주의를 기울여 **본인 확인**을 하고, 명의도용 의심시 **거래제한** 조치 등 실시



1 제도 소개

□ **(누구한테 필요한지)** 신분증 분실, 피싱 등에 의한 **개인정보 유출**로 **타인이 본인 명의로 금융거래를 할 가능성이 우려**되는 경우 **'개인정보노출자'로 등록**할 것을 권고*

* 성명, 주민등록번호 등 일부 개인정보만으로 대출, 카드발급 등은 어려우나 다른 경로를 통해 유출된 정보와 결합될 경우 악용될 가능성을 배제할 수 없음

□ **(등록시 효과)** **'개인정보노출자'로 등록**된 사람의 명의로 **대출, 계좌개설 등 금융거래가 진행** 될 경우 금융회사는 **강화된 본인 확인 절차**를 진행함으로써 명의도용을 예방

○ 상세 주소, 계좌 번호, 결제 계좌, 결제일 등 세부 정보를 **추가 확인***하고 철저한 신분대조를 통해 **명의자와 거래자를 비교**

* 다만, 상기와 같은 본인확인 절차가 강화됨에 따라 일부 금융거래가 제한되는 등 불편함이 발생할 수 있으나 언제든지 해제 가능

□ **(등록 방법)** **은행 방문, 인터넷 중** 편리한 방법으로 **'개인정보노출자' 등록**이 가능하며 등록 즉시 全 금융회사에 **자동 전파**

❶ **(은행 방문)** 영업점을 방문하여 **'개인정보노출자' 등록**을 요청

❷ **(인터넷)** 금융소비자포털 싸이트인 **'파인'**(fine.fss.or.kr)에 접속하여 소비자보호 > 개인정보노출등록·해제 메뉴를 이용

□ **(해제 방법)** 신분증 재발급, 기간 경과 등으로 **명의도용 우려가 해소되었다고 판단**되면 **등록시와 동일한 방법**(은행방문, 인터넷)으로 언제든지 해제 가능

2 제도 운영 현황

□ '21년중 금융감독원 금융소비자포털 「파인」에 개인정보 노출을 등록한 건수는 20.9만건으로 전년보다 188% 증가*

* '21년 금융소비자포털 파인(FINE) 항목 중 가장 많이 사용된 메뉴 (인기순위 1위)

○ 보이스피싱 등으로 인한 등록이 등록사유의 과반(51%)을 차지하는 등 명의도용으로 인한 금융사고 예방에 크게 기여

개인정보노출 등록사유별 현황

(단위 : 건, %)

등록 사유	'18년	'19년	'20년	'21년	증가율	비중
신분증 분실	14,414	8,967	8,296	20,033	141	9.6
기타 방법	10,849	12,126	21,353	57,610	170	27.6
명의도용 금융사고 인지	3,015	3,514	7,727	20,065	160	9.6
보이스피싱 등	**9,516**	**15,447**	**33,496**	**107,023**	**220**	**51.2**
금융회사 고객정보 노출	530	846	1,643	4,319	163	2.1
합 계	**38,324**	**40,900**	**72,515**	**209,050**	**188**	**100.0**

<별첨> 금융꿀팁 200선 - ⑫⑥ 신분증 분실 혹은 피싱 의심시 개인정보노출자 사고예방시스템에 등록하세요

※ **(동영상 보도자료) '개인정보노출자 사고예방시스템'**을 쉽게 설명해주는 동영상은 금감원 SNS 채널에서 보실 수 있습니다.

❶ 유튜브 https://youtu.be/1HqsQoV-GEg
❷ 페이스북 https://fb.com/5126570904093187
❸ 네이버TV https://tv.naver.com/v/26715095

☞ 본 자료를 인용하여 보도할 경우에는 출처를 표기하여 주시기 바랍니다.(http://www.fss.or.kr)

별첨 **개인정보노출자 사고예방시스템 이용사례 및 꿀팁**

사 례

■ **(사례1)** 부산에 사는 이모 씨는 어느 날 **운전면허증**이 들은 **지갑을 분실**하였다는 것을 깨달음. 현금은 많이 들어있지 않았고, 평소 이용하던 카드사에 분실신고를 하여 카드 부정사용도 방지하였으나, **분실한 신분증으로 누군가 계좌를 개설한다거나 대출을 받는 등의 일**이 발생하지 않을까 걱정됨

그렇다고 **모든 금융회사에 면허증 분실 사실을 알릴 수도 없는 노릇**이라 불안해하던 차에, 얼마 전 라디오에서 **금감원이 개인정보노출시 사고를 예방하는 시스템**을 운영한다는 이야기를 기억하고, 금감원 소비자포털 파인(fine.fss.or.kr)을 통해 **개인정보노출자 사고예방시스템**에 접속

다른 복잡한 사이트와 달리 개인정보 노출사실 **「등록 및 해제 신청」**과 **「신청내역 조회」 두 가지 버튼**만 있는 것이 눈에 띄였고, 휴대폰 본인인증을 거쳐 **개인정보 노출사실을 등록*** 하여 **명의도용에 대한 걱정**은 한시름 덜음

* 개인업무를 취급하는 모든 금융회사에 개인정보 노출사실 전파, 금융거래 제한

일정기간 이후 신분증을 되찾기는 어렵겠다는 생각에 경찰서에서 **운전면허증을 재발급 받은 후,** 다시 금감원의 개인정보 노출자 사고예방사이트에 접속하여 **등록사실을 해제**한 후 금융거래을 재개할 수 있었음

개인정보 노출사실 등록 이후 일상생활을 하는 과정에서 **신규 카드발급 등 금융거래에 불편함을 느꼈으나 한편으로는 철저한 본인확인을 통해 사고가 예방될 것 같아 안심***

* 금융회사에 따라 카드발급 등 금융거래를 위해서는 금융이용자 본인이 개인정보 노출사실을 등록하였다는 등록증명서(화면) 등을 요구

	■ **(사례2)** 대전에 사는 한 모 씨는 모르는 번호로부터 아래와 같이 **"엄마, 나 휴대폰 액정이 깨져서 임시폰이야, 도와줘!"**라며 회사에 제출할 **백신접종 증명서 발급을 위한 앱을 설치**해 달라는 문자를 받음 당장 도와줄 사람이 엄마밖에 없다는 말에 '오죽하면 아빠를 두고 나에게 부탁했을까' 하는 마음에 급하게 주변의 도움을 받아 **문자상의 링크를 눌러가며 해당 앱을 설치**하였으나 이후 딸과의 통화를 통해 **해당 문자가 요즘 유행하는 메신저 피싱이었음을 인지** 황급히 **거래은행 창구로 달려가 사고접수를 통해** 입출금 및 신용카드 이용 등을 정지하고, **개인정보노출자 사고예방 시스템**에도 노출사실을 등록하는 것이 좋겠다는 안내에 따라 은행직원에게 등록해 줄 것을 요청 혹시 자신도 모르게 계좌가 개설되거나 대출이 실행되었는지를 확인하기 위해 **계좌정보통합관리서비스**(www.payinfo.or.kr)를 이용하여 확인* * 확인 결과 명의도용 계좌 개설 또는 비대면 대출 등이 실행된 경우 즉시 해당 금융회사에 피해사실 신고 및 지급정지를 신청해야 함 확인 결과, 다행히 명의도용 계좌 개설 등이 발견되지는 않았으나, 통신사 대리점의 도움을 받는 등 **악성앱 설치여부**를 확인 후 **핸드폰 초기화 등을 진행**
꿀 팁	**피싱이 의심될 때 행동 요령** **1. 가족 및 지인 여부를 반드시 확인** **2. 출처가 불분명한 앱설치 요구시 무조건 거절** **3. 개인정보노출자 사고예방시스템 및 계좌정보통합관리서비스 등 이용**

1. 가족 및 지인 여부를 반드시 확인

□ 가족 및 지인 등이 문자 또는 메신저로 금전 및 개인(신용) 정보를 요구하는 경우 가족 및 지인 여부를 **직접 만나 반드시 확인**하고,

○ **휴대폰 고장, 분실 등의 사유로 만남이나 통화가 어렵다고 하면 보이스피싱이 의심**되므로 더욱더 주의하여 메시지 대화를 중단

※ 자녀여부가 불확실한 경우, 반려동물 이름, 부모님 직업 등 자녀가 쉽게 알 수 있는 질문을 하는 방안도 고려

2. 앱설치 요구 시 무조건 거절

□ 자녀 등 지인을 사칭하여 원격조종 앱 등 악성앱 설치를 유도할 수 있으므로 링크 등을 통해 **출처가 불분명한 앱 설치 요구시 무조건 거절***

* 제도권 금융회사는 전화·문자를 통한 자금요구, 뱅킹앱 설치 등을 절대로 요구하지 않음

○ 요구대로 새로 앱을 설치한 경우 **스마트폰 보안 상태 검사**를 통해 악성앱 설치 여부를 확인한 후 악성앱을 삭제하거나 휴대폰 포맷 및 초기화를 진행

3. 개인정보노출자 사고예방시스템 및 계좌정보통합관리시스템 등 이용

□ 피싱 피해가 의심될 때에는 송금 또는 입금 금융회사 콜센터 및 금융감독원 콜센터(☎1332)에 전화하여 해당 계좌에 대한 지급정지 요청 및 피해구제신청을 접수

○ 개인정보 유출에 따른 추가 피해를 막기 위해 금융감독원 금융소비자 정보포털, '파인'의 **『개인정보노출자 사고예방 시스템』**을 적극 활용

○ 아울러 **"계좌정보통합관리서비스*"**(www.payinfo.or.kr)를 활용하여 본인도 모르게 개설된 계좌 또는 대출을 확인

* '내계좌한눈에', '내카드한눈에', '금융정보조회' 코너를 활용

○ 또한 본인이 모르는 휴대폰 개통 여부는 한국정보통신진흥협회에서 운영하는 **명의도용방지서비스(www.msafer.or.kr)**에 접속하여 **가입사실현황***을 조회

* 피해자 명의로 가입된 휴대전화 등의 통신서비스 가입현황을 조회일자 기준으로 확인

[참고 : 개인정보노출자 사고예방시스템이란]

■ 금융이용자가 신분증 분실 등으로 개인정보 노출 우려 시 금융감독원 금융소비자포털 '파인(FINE)'에 등록하여 명의도용을 예방하는 시스템으로 개인업무를 취급하는 전체 금융회사와 연결 ('03.9월부터 운영)

- '21년중 「파인」에 개인정보 노출사실이 등록된 건수는 20.9만건으로 전년(7.3만건)보다 188% 증가

■ 개인정보 노출사실이 등록되면, 해당 정보가 실시간 금융회사에 전달되어 금융회사 **영업점 단말기**에 '**본인확인 주의**' 문구가 게시되고,

- 금융회사 영업점 직원은 **통상 이상**의 주의를 기울여 **본인 확인**을 하고, 명의도용 의심 시 **거래제한** 조치 등 실시

■ 금융이용자는 PC 또는 휴대폰을 이용해 해당 시스템에 온라인으로 접속해 자신의 개인정보 노출사실을 한 번에 등록(또는 해제)할 수 있으며, 온라인 이용이 어려울 경우 은행 등 영업점을 통해서도 등록(또는 해제) 가능