방송통신위원회

보 도 자 료

다시, 대한민국! 새로운 국민의 나라

보도 일시	2022. 5. 12.(목) 14:00	배포 일시	2022. 5. 12.(목) 10:00
담당 부처	방송통신위원회 이용자보호과	책임자	과 장 이소라 (02-2110-1540)
		담당자	주무관 김효나 (02-2110-1542)
	금융위원회 민생침해금융범죄대응반	책임자	부이사관 김기한 (02-2100-2575)
		담당자	사무관 허 성 (02-2100-2632)
	경찰청 사이버범죄수사과	책임자	과 장 이병귀 (02-3150-1605)
		담당자	경정 이성일 (02-3150-1658)
	금융감독원 불법금융대응단	책임자	국 장 박중수 (02-3145-8150)
		담당자	팀 장 고병완 (02-3145-8521)

가족, 지인 사칭 「메신저피싱」 주의 당부

- 이동통신3사 전가입자 대상 피해예방 문자메시지 발송 -

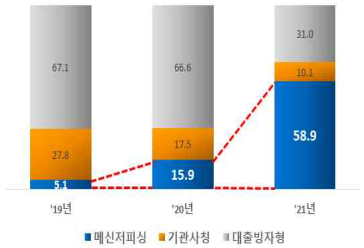
방송통신위원회,금융위원회,경찰청,금융감독원은 코로나19 이후 비대면 매체 이용이 증가하면서 메신저피싱(messenger phishing)* 사기가 급증하고 있어 이로 인한 국민의 피해가 예상되고 있다며 각별한 주의를 당부했다.

* 카카오톡, 네이트온, 페이스북 등 타인의 메신저 아이디를 도용하여 로그인한 뒤 등록된 지인에게 메시지를 보내 금전을 편취하는 범죄수법

최근 몇 년간 보이스피싱 관련 사기피해는 전반적으로 감소하는 추세이나, 신종 범죄수법인 메신저피싱으로 인한 피해는 오히려 매년 증가하고 있다. 특히 '21년도 메신저피싱 피해액은 전년대비 165.7%(+618억원) 급증한 991억원으로 보이스피싱 피해 유형 중 58.9%를 차지하고 있다.

보이스피싱 유형별 피해 현황

(사기유형별 피해금액 비중)



(단위 : 억원, %, %p)

구 분		'19년	'20년	'21년	전년대비 증감(률)	
사칭형	메신저피싱 (비중)	342 (5.1)	373 (15.9)	991 (58.9)	+618 (+43.0)	(+165.7) -
	기관사칭 (비중)	1,872 (27.9)	414 (17.6)	170 (10.1)	△244 (△7.5)	(△58.9) -
대출빙자형 (비중)		4,506 (67.0)	1,566 (66.6)	521 (31.0)	△1,045 (△35.6)	(△66.7) -
합계		6,720	2,353	1,682	△671	(△28.5)

* 비중은 전체 피해액 중 비중

<출처: 금융감독원 자료>

이에, 방송통신위원회는 이동통신사업자, 한국정보통신진흥협회(KAIT)와 협력하여 5월 13일부터 이동통신 3사 명의로 가입자에게 「메신저피싱 주의 안내」 문자메시지를 순차 발송하고, 알뜰폰 가입자에게는 요금고지서로 피해예방 정보를 안내할 예정이다.

메신저피싱은 '가족, 지인을 사칭한 범죄자가 피해자에게 휴대폰 파손 등 불가피한 상황을 알리며 악성링크에 연결하도록 유도한 후 개인정보를 탈취하여 자금을 편취하는' 사기수법이다.

메신저피싱은 아래의 '메신저피싱 예방수칙' 을 준수하면 피해를 줄일 수 있다.

▸메신저피싱 예방 수칙◂

○ 실제 가족·지인이 맞는지 반드시 직접 전화통화로 확인
○ 긴급한 상황을 연출하더라도, 전화로 확인 전에는 절대 송금 금지
○ 가족·지인 본인이 아닌 타인의 계좌로 송금요청시 일단 의심

금융당국은 원격조종앱에 의한 메신저피싱 사기피해 사례가 많은 점을 감안하여 금융회사가 원격조정앱 구동을 차단하는 금융앱 기술을 도입하도록 유도하고, 언론에 신분증 및 금융거래정보를 탈취하여 자금을 편취하는 사기수법을 집중 홍보할 것이라고 밝혔다

또한 경찰청은 전국 시도청에 설치된 사이버경제범죄수사팀을 중심으로 3월 1일부터 10월 31일까지 8개월간 메신저피싱 등 사이버금융범죄 집중단속을 실시하고, 단속 뿐 아니라 범죄수익 동결·환수에도 만전을 기하는 등 관련 범죄에 엄정 대응하고 있다고 밝혔다.

메신저피싱 등 보이스피싱으로 의심될 경우에는 해당 금융회사에 연락하여 지급정지 요청을 하여야 하며, ☎112(경찰청),☎1332(금융감독원)으로 연락하면 피해신고 및 피해금 환급 관련 상담을 받을 수 있다.

한상혁 방송통신위원회 위원장은 "피해 예방을 위해서는 누리 소통망(SNS) 등으로 개인정보나 금품 등을 요구받으면 상대가 누구든지 확인하고 또 확인해 보는 습관이 필요하다." 고 강조하고, "앞으로도 관계기관과의 협력을 강화하여 통신 금융사기 피해예방을 위해 실효성 있는 해결방안을 지속적으로 추진하겠다." 고 밝혔다.

붙임1 메신저피싱 주의 안내사항

□ 이동통신3사 (문자메시지 발송)

[메신저피싱 주의 안내]

최근 가족 또는 지인의 프로필을 사칭하여 문자메시지 또는 누리 소통망(카카오톡, 페이스북 메신저 등)로 말을 걸어 돈을 갈취하는 '메신저피싱' 피해가 빈번하게 발생하고 있으니 피해 예방을 위해 다음 행동 요령에 따라주시기 바랍니다.

1. 이용자 행동 요령
   - o (문자로 금전·개인정보 요구시) 핸드폰 고장, 분실 등의 사유로 연락이 어렵다고 하면 보이스피싱이 의심되므로 더욱 더 주의하여 메시지 대화를 중단
   - o (출처가 불분명한 앱 설치 요구시) 자녀 등 지인을 사칭하여 원격조종 앱 등 악성앱 설치를 유도할 수 있으므로 출처가 불분명한 앱 설치 요구시 무조건 거절

2. 메신저피싱 후 대응방법
   송금·입금 금융회사 콜센터에 전화 → 계좌 지급정지 요청 및 피해구제신청 접수
   경찰청(☎112) 또는 금감원 콜센터(☎1332)에 전화 → 피해신고 및 피해금 환급 관련 상담

□ 알뜰폰사업자 (요금고지서 안내사항)

가족, 친구 등 지인 사칭 메신저피싱 주의 하세요!

붙임2 보이스피싱(메신저 피싱) 피해사례

□ **문자메시지, 카톡** 등으로 **가족·지인**을 **사칭**하며 **긴급한 사정***을 이유로 **개인정보**** 및 **금전이체** 등을 요구

* 본인의 휴대폰 고장, 신용카드 도난·분실, 사고 합의금 명목의 급전 필요 등

** 신분증, 계좌번호 및 비밀번호, 신용카드번호 및 비밀번호, 공인인증서 비밀번호 등

○ 메신저피싱 피해는 주로 **고령층**에서 발생하는데, 이는 사기범이 **자녀를 사칭함**으로써 **부모의 이성적 판단**이 **와해**되는 취약점을 공략

○ 사기범이 **탈취한 신분증, 인증번호** 등으로 피해자 몰래 **계좌잔액 인출, 신규계좌 개설 및 신규대출신청, 오픈뱅킹 가입 후 피해자의 다른 금융계좌 잔액을 편취**하는 등 **추가 피해 위험**에 노출

① '21.12월 사기범은 피해자 A씨(62세, 주부)의 딸을 사칭하며, '엄마 나 휴대폰이 파손되어서 급하게 휴대전화 보험 신청해야 해. 엄마 명의로 대신 진행하게 도와줘'라며 메신저톡을 전송함

② 이에 속은 피해자는 사기범으로부터 받은 메신저톡의 악성링크를 클릭하여 원격조종앱이 휴대폰에 설치되었고, 또한 사기범에게 본인의 신분증 촬영본, 은행계좌번호 및 비밀번호 등 개인정보를 전달함

③ 사기범은 원격제어를 통해 피해자 휴대폰에 설치된 금융앱에 접속하여 해당 계좌 잔액 및 오픈뱅킹서비스를 통한 타행계좌 잔액을 모두 사기이용계좌로 송금하여 총 26,700만원의 자금을 편취

붙임3 **보이스피싱 예방요령**

1. 금융거래정보 요구는 일절 응대하지 말 것

▸ 전화로 개인정보 유출, 범죄사건 연루 등을 이유로 계좌번호, 카드번호, 인터넷뱅킹 정보를 묻거나 인터넷 사이트에 입력을 요구하는 경우 절대 응하지 말아야 하며,특히 텔레뱅킹의 경우 인터넷뱅킹과 달리 공인인증서 재발급 등의 절차가 필요치 않아 타인이 취득 시 사기피해에 취약

2. 현금지급기로 유인하면 100% 보이스피싱

▸ 현금지급기를 이용하여 세금, 보험료 등을 환급해 준다거나 계좌안전조치를 취해주겠다면서 현금지급기로 유인하는 경우 절대로 응하지 말 것

3. 자녀납치 보이스피싱에 미리 대비

▸ 자녀납치 보이스피싱 대비를 위해 평소 자녀의 친구, 선생님, 인척 등의 연락처를 미리 확보할 것

4. 개인·금융 거래정보를 미리 알고 접근하는 경우에도 내용의 진위를 확인

▸ 최근 개인·금융거래정보를 미리 알고 접근하는 경우가 많으므로 전화, 문자메시지, 인터넷메신저 내용의 진위를 반드시 확인할 것

5. 피해를 당한 경우 신속히 지급정지를 요청

▸ 보이스피싱을 당한 경우 경찰청 112콜센터 또는 금융회사 콜센터를 통해 신속히 사기계좌에 대해 지급정지를 요청할 것

6. 유출된 금융거래정보는 즉시 폐기

▸ 유출된 금융거래정보는 즉시 해지하거나 폐기할 것

7. 예금 통장 및 현금(체크)카드 양도 금지

▸ 통장이나 현금(체크)카드 양도 시 범죄에 이용되므로 어떠한 경우에도 타인에게 양도하지 말아야 하며, 통장이나 현금(체크)카드 양도는 전자금융거래법 위반으로 형사처벌을 받을 수 있는 범죄임(3년 이하의 징역 또는 2천만원 이하의 벌금)

8. 발신(전화번호)는 조작이 가능함에 유의

▸ 텔레뱅킹 사전지정번호제*에 가입되었다 하더라도 인터넷 교환기를 통해 발신번호 조작이 가능하므로, 사기범들이 피해자들에게 "사전지정번호제에 가입한 본인 외에는 어느 누구도 텔레뱅킹을 이용하지 못하니 안심하라"고 하는 말에 현혹되지 말 것

* 사전에 등록된 특정 전화번호로만 텔레뱅킹을 할 수 있는 제도

9. 금융회사 등의 정확한 홈페이지 여부 확인

▸ 피싱사이트의 경우 정상적인 주소가 아니므로 문자메시지, 이메일 등으로 수신된 금융회사 및 공공기관의 홈페이지는 반드시 인터넷 검색 등을 통해 정확한 주소인지를 확인할 것

10. 「전자금융사기 예방서비스」 적극 활용

▸ 타인에 의해 무단으로 공인인증서가 재발급되는 것 등을 예방하기 위해 '12.9.25일부터 각 은행에서 시범 시행하는 「전자금융사기 예방서비스」 적극 활용할 것

붙임4 | **보이스피싱 피해 발생시 참고 사이트**

<금융소비자 정보포털(파인) : ①개인정보노출등록 및 ②계좌정보통합조회>

<한국정보통신진흥협회 Msafer 사이트 : 명의도용방지서비스>