

'나는 안 당해' 자만심 파고드는

남구청·남부경찰서 보이스피싱 예방 합동캠페인

‘명동’, 점심을 먹고 사무실로 돌아온 40대 A씨의 휴대전화로 문자 메시지 한 통이 왔다. ‘택배물품이 송장번호 미확인으로 반송됩니다’는 내용이였다. 평소 모바일로 쇼핑을 자주 하는 터라 별 의심 없이 해당 인터넷주소를 클릭했다. 이어 XX택배의 배송상세조회 화면이 떴고 이름과 주민번호 앞 6자리(생년월일), 휴대전화 번호를 통해 본인인증을 받았다. 그러자 ‘소액결제로 30만원이 출금되었다’는 문자메시지가 날아왔다.

어리둥절해진 A씨는 앞서 온 문자메시지를 꼼꼼히 살펴보고 나서야 자신이 ‘소액결제 보이스피싱’을 당했다는 것을 알아차렸다. 곧바로 가까운 경찰서에 사건을 접수하고, 이동통신회사를 방문해 보이스피싱 업체에 대한 결제액 지급 정지를 요청했지만 받아들여지지 않았다.

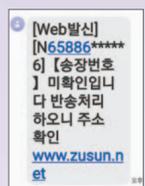
보이스피싱 수법이 갈수록 다양해지고 있고, 이에 보이스피싱 범죄를 예방하고 사고 발생 시 신속한 대처 방법을 2020년 보이스피싱 현황을 중심으로 소개한다.

#2020년 보이스피싱 현황

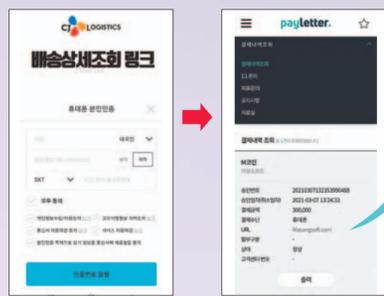
지난 2020년 전국 보이스피싱 피해 금액은 2353억원, 피해건수는 2만5859건으로 2019년 대비해 각각 65%, 64.3% 감소했다. 피해 환급률도 절반에 달해 보이스피싱 피해가 전반적으로 줄었다. 이는 지속적인 보이스피싱 예방노력에 기인한 것으로 보인다. 또 코로나19로 사기조직의 활동이 제한된 것도 일부 영향을 미친 것으로 분석된다.

하지만 보이스피싱 수법이 진화하면서 최근 들어 휴대전화 메시지피싱 피해가 크게 증가하고 있어 각별한 주의가 요구된다.

메신저피싱 피해가 전체 피해금액에서 차지하는 비중은 15.9%. 연령별로 50대(43.3%)와 60대(42.5%)가 전체 메시지피싱 피해의 85.8%를 차지했다. 대출형 사기 피해는 40~



A씨가 당한 택배를 위장한 보이스피싱 문자메시지 실제 사례. 본인 인증을 유도해 휴대전화 소액결제로 돈을 편취한다.



결제금액 300,000
결제수단 휴대폰

‘메신저 피싱’ 최근 급증

대출형 사기 40~50대 남성 취약

지인·가족 사칭 50~60대 여성 미끼

50대 남성이 65%로 가장 높았다. 지인이나 가족을 사칭하는 사기 피해자는 여성(64.5%)이 남성(35.5%)보다 크게 높았고 그중에서 50대와 60대 여성이 각각 28.4%와 27.1%로 가장 취약한 것으로 나타났다. 피해액의 이체 채널로는 모바일 인터넷뱅킹의 비중이 갈수록 증가해 지난해 75.2%를 차지했다. 창구,ATM의 비중은 줄어 지난해 13.5%, 텔레뱅킹 4.8%를 보였다.

■ 2020년 국내 보이스피싱 피해 현황

구분	2018년	2019년	2020년
피해액	4440억원	6720억원	2353억원
환급액	1011억원	1915억원	1141억원
환급률	22.8%	28.5%	48.5%
피해건수	7만218	7만2488	2만5859

■ 사칭형 범죄 피해 현황 (단위 : %)

연령	남성	여성	합계
10대 이하	0.0	0.0	0.0
20-30대	7.7	2.3	10.0
40-50대	10.2	31.4	41.7
60대 이상	17.5	30.8	48.3
합계	35.5	64.5	100.0

■ 대출빙자형 범죄 피해 현황 (단위 %)

연령	남성	여성	합계
10대 이하	0.0	0.0	0.0
20-30대	8.5	6.4	15.0
40-50대	38.7	26.3	65.0
60대 이상	14.0	6.0	20.0
합계	61.2	38.8	100.0

(자료 금융감독원)

#메신저피싱 급증 주의보

메신저피싱은 문자메시지나 카카오톡 메신저 등으로 가족이나 지인을 사칭해 긴급한 사정을 이유로 개인기밀정보 및 금전이체 등을 요구하는 사기 범죄를 말한다. 본인의 휴대전화 고장이나 신용카드 도난, 분실, 사고 합의금 명목으로 금전이 필요하다며 신분증, 계좌번호, 비밀번호, 신용카드번호, 비밀번호, 공인인증서 비밀번호 등을 요구한다.

메신저피싱 피해는 주로 고령층에서 발생하는데, 이는 사기범이 자녀를 사칭해 부모의 이성적 판단이 와해되는 취약점을 공략하기 때문이다. 사기범은 탈취한 신분증, 인증번호 등으로 피해자 몰래 계좌잔액 인출, 신규계좌 개설·신규대출신청, 오픈뱅킹 가입 후 피해자의 다른 금융계좌 잔액을 편취한다. 올해 2월, 딸을 사칭한 문자메시지를 받은 A씨가 자신의 신분증과 신용카드 사진, 계좌비밀번호를 전송했는데 사

기범은 이를 이용해 A씨의 은행 계좌에서 1억6900만원을 인출한 사례가 대표적이다.

#사고 발생시 신속 대응 필수

금융이용자는 일상생활 속에서 누구나 보이스피싱에 당할 수 있다는 점을 명심하고, 피해가 발생하지 않도록 주의해야 한다. 보이스피싱 피해예방 5계명(표 참조)을 숙지해 상황별 행동원칙을 파악하는 것이 도움이 된다. 사기범에 속아 현금이체 등 피해를 당한 경우에는 지체없이 경찰청(☎112)이나 부산 남부경찰서(☎610-8367), 해당 금융회사 등에 신고해 지급정지를 신청해야 피해 회복이 가능하다.

* 위의 보이스피싱 통계는 금융감독원 자료를 기초로 작성했습니다. 금융감독원은 사기에 의한 자금의 송금, 이체를 보이스피싱 피해로 집계하며, 통신사기피해원금법의 적용 대상이 아닌 '대면편취형 및 재화·용역을 가장한 사기'는 포함하지 않아 경찰청 통계와는 차이가 있습니다.

검은 속삭임



보이스피싱 예방에 앞장서는 남부경찰서 관계자들. 왼쪽부터 지능범죄수사팀 김희성 팀장, 김민수 서장, 오영환 수사과장, 김남경 수사관.

보이스피싱 피해예방 5계명

- 1 경찰·금융원이라며 금전을 요구하면 무조건 거절
- 2 메신저·문자 통해 금전을 요구하면 유선 확인 전까지 무조건 거절
- 3 등급 상향, 저금리 전환, 대출 수수료 명목 금전 요구는 무조건 거절
- 4 출처 불분명 앱, URL 주소는 무조건 클릭 금지
- 5 사용하지 않은 결제 문자는 업체가 아닌 해당 카드사에 확인

※ 보이스피싱·스미싱 신고·문의

경찰청 ☎112, 부산남부경찰서 ☎610-8367, 금융감독원 ☎1332
한국인터넷진흥원 118센터 ☎118

고 객념을 위한
앞선 초저금리
대출상품이 ...

저금리 대환대출 미끼로 3억2000만원 탈취

■ 남구 주민 피해 사례

▷남구 거주 A씨는 '2~3% 저금리 대환대출을 해 주겠다는 OO은행'을 사칭하는 문자메시지를 받았다. 대출신청용 앱을 설치하도록 한 후 기존 대출금 상환 명목으로 직원을 보낼 테니 돈을 직접 전달해 상환토록 하고 이후 OO은행 직원이 아꼈으니 이후 모든 은행거래가 중지된다고 공탁금 명목으로 돈을 맡기라고 해 3억2000만원 상당의 피해를 당했다.

▷남구 거주 B씨는 '서울 중앙지검 000검사'로 사칭하는 사람'으로부터 수사 중인 사건에서 "당신의 계좌가 부정하게 범죄에 이용된

사실이 발견되었다'라며 '계좌에서 사용된 자금을 대해 가담여부를 확인해야 하니, 4000만원을 맡기면 범죄에 연루되지 않았다'는 사실이 확인되면 반환하겠다고 속여 4000만원 상당의 피해를 입었다. 기존 금융기관을 사칭해서 저금리 대환대출을 해 주겠다고 하거나, 정부 햇살론 자금을 저리로 대출해 준다는 전화 또는 문자메시지는 대부분 보이스피싱 범죄를 의심해야 한다. 이밖에 경찰, 검찰 등 수사기관을 사칭해 계좌가 범죄에 연루되었다거나 '해외에서 신용카드가 결제되었다'라는 문자메시지를 받으면 100% 보이스피싱 범죄를 의심해야 한다. 사례 제공 남부경찰서 지능범죄수사팀



그랜드자연요양병원



이 사진은 실제 병원 전경입니다.

보건복지부 의료기관 2주기 인증
유효기간 : 2018.7.24. ~ 2022.7.23



◆ 병원장 이재일(내과 전문의 / 중앙대학교 의과대학부)
◆ 치매, 뇌졸중, 파킨슨, 노인성질환, 물리치료, 의학 한의학 협진
부산 남구 대연동 황령대로 355-14 | 대남교차로에서 황령터널 방향 우측



상담문의 051-612-0075
www.grandnature.kr

유료광고