보이스피싱 조심 또 조심하세요!

보이스피싱 예방 가이드북

신한은행 사랑의열매 사회복지공동모금회 굿네이버스 경찰청 금융감독원

CONTENTS

1. 전기통신 금융사기 정의

전기통신 금융사기란?

「전기통신기본법」 제2조 제1호에 따른 전기통신을 이용하여 타인을 기망·공갈함으로써 재산상의 이익을 취하거나 제3자에게 재산상의 이익을 취하게 하는 행위(개인정보를 알아내어 자금을 송금·이체하도록 하는 행위)를 말합니다.

피싱 사기 유형

피싱(Phishing)이란 개인정보(Private data)를 낚는다(Fishing)는 의미의 합성어로, 전화·문자·메신저·가짜사이트 등 전기통신 수단을 이용한 비대면 거래를 통해 피해자를 기망·공갈함으로써 이용자의 개인정보나 금융정보를 빼낸 후, 타인의 재산을 갈취하는 사기 수법을 의미합니다.
피싱 사기는 전화뿐만 아니라 문자, 메신저, 인터넷 사이트 등 다양한 전기통신 수단을 통해 이루어집니다.

❶

보이스피싱

전화를 통하여 신용카드 번호 등의 개인정보를 알아낸 뒤 이를 범죄에 이용하는 전화금융 사기 수법

❷

메신저피싱

카카오톡, 페이스북 등 메신저 아이디를 도용하여 로그인한 뒤 지인에게 메시지를 보내 금전을 탈취하는 신종 사기 수법

❸

스미싱

출처가 불분명한 문자 메시지에 포함된 인터넷 주소에 접속했을 때, 악성코드가 스마트폰에 설치되어 개인정보, 금융정보 유출, 소액결제 피해 등을 일으키는 사기 수법

❹

파밍

악성코드에 감염된 PC를 조작해 이용자가 정상적인 홈페이지 주소로 접속하여도 피싱(가짜) 사이트로 유도 되어 개인 금융정보 등을 유출하는 수법

❺

로맨스스캠

SNS 및 이메일 등 온라인으로 접근하여 호감을 표시하고 재력, 외모 등으로 신뢰를 형성한 후 각종 이유로 금전을 요구하는 방법의 사기

❻

몸캠피싱

채팅 과정에서 피해자를 속여 알몸 사진 등 '몸캠'을 확보하고 이를 가족이나 지인 등에게 유포하거나 SNS에 공개 하겠다고 협박하여 금전을 갈취하는 행위

❼

대포폰

신분을 감추거나 경찰 등의 추적을 피하기 위하여, 급히 돈이 필요한 사람에게 일정한 비용을 주고 그 사람의 명의를 빌려 불법적으로 개통해 실제 사용자와 이용약정 체결자가 다른 단말기를 개통해 사용

피싱 사기 과정

STEP 01 예금통장 매입, 대출 등 미끼로 편취

신용불량자, 노숙자 등을 이용하여 통장(대포통장)을 개설·매입, 대출 또는 취업을 미끼로 예금통장을 편취합니다.

STEP 02 해외(중국 등)콜센터에서 국내로 전화

해외(중국 등)에 본부를 둔 사기단이 금융기관 및 검찰, 경찰, 금융감독원 등 공공기관의 대표전화로 발신자 번호를 조작하여 무작위로 국내에 전화합니다.

STEP 03 개인정보 유출, 범죄 사건 연루 등으로 기망

금융기관 및 검찰, 경찰, 금융감독원 등 공공기관을 사칭하는 자가 개인정보 유출, 범죄사건 연루 등의 명목으로 기망하여 피해자의 개인정보 또는 금융 거래 정보를 탈취(최근에는 악성코드 유포를 통한 파밍으로 피싱사이트 접속을 유도하는 등 사기 기법이 첨단화되고 있음)합니다.

STEP 04 송금·이체 유도 또는 사기범이 직접 이체

계좌 보호 조치 또는 범죄 혐의 탈피 등 명분하에 사기계좌로 이체를 유도하거나 피해자로부터 편취한 정보로 공인인증서를 재발급 받아 사기범이 직접 이체합니다.

STEP 05 현금 인출책·송금책을 통해 해외 송금

점조직으로 이루어진 현금 인출책이 송금책의 계좌로 입금하면 송금책이 환치기 등의 방법으로 범죄 집단 본부로 송금(글로벌 체크카드 이용 시 해외에서 직접 출금)합니다.

2. 최근 피싱 피해 사례

지인 사칭

자녀를 사칭하며 접근하여 친구 추가 및 앱 설치

· 피해자 A씨는 "엄마 뭐해"라는 카톡을 받았습니다. 피해자는 지금 일하는 중이니 끝나고 통화하자고 하였습니다. 그러나 사기범은 '지금 핸드폰이 고장나서 통화가 어려워 PC카톡으로 연락한다'며 급하게 송금할 곳이 있어 지금 바로 송금해줄 것을 요청하였습니다.

· 급하다는 딸의 말을 믿은 A씨는 사기범이 지정한 계좌로 600만 원을 송금하였습니다.

공공기관 사칭

범죄 사건 연루 사례

· 사기범은 피해자 B씨에게 전화를 걸어 서울중앙지검 검사를 사칭한 후 범인이 B씨 명의의 계좌를 사용했는데 범죄에 가담 되지 않았다는 것을 입증하기 위해 B씨 명의의 계좌에서 일정 금액을 안전 계좌로 송금하고 상품권을 구매하여 전달해야 한다고 피해자를 속였습니다.

· B씨가 이를 의심하자 검찰청 로고가 프로필로 된 메신저를 통해 검찰총장 명의의 공문과 검사 신분증을 보여주어 피해자를 믿게 했습니다.

· 이에 속은 B씨는 피해자 명의의 계좌에서 1,000만 원을 송금하고 상품권 200만 원 상당을 구입하여 메신저로 전달하였습니다.

금융기관 사칭

저축은행 사칭 대출 권유

· 피해자 C씨는 OO저축은행으로 사칭한 곳으로부터 대출 권유 문자를 받고 사기범이 요구한 운전면허증을 송부하였습니다.

· 사기범은 C씨의 신분증을 이용해 C씨 명의의 대포폰을 만들었고, 신분증과 대포폰을 이용하여 C씨의 명의로 증권회사 비대면 계좌를 만들었습니다.

· 사기범은 이후 OO저축은행에서 C씨의 신분증과 대포폰, 그리고 C씨의 명의로 개설 된 증권회사 계좌를 통해 비대면 대출 500만 원을 받아서 탈취하였습니다.

카드사 사칭

문자 메시지 발송 사례

· D씨는 신용카드가 해외에서 발급 되었고 본인이 신청한 사실이 없으면 연락하라는 문자 메시지 확인 후 메시지에 기재된 전화번호로 연락하였습니다.

· 이후 검찰, 경찰, 금융감독원 직원을 사칭한 사기범들로부터 피해자 명의 대포통장이 중고거래 사이트 사기에 연루되었다며 구속 수사를 면하려면 공탁금을 이체해야 한다는 말에 기망 당하여 피해가 발생하였습니다.

모바일 URL

경조사 안내 문자

· 결혼, 돌잔치, 부고 등을 가장하여 피싱 사이트로 접속하도록 하는 URL이 포함된 문자를 불특정 다수에게 발송하여 피싱으로 인한 피해가 발생합니다.

3. 전기통신 금융사기 피해 시 대처 방법

1 경찰청 112 피해 신고 접수

보이스피싱 통합신고대응센터 원스톱 지원

2 신분증, 계좌번호 등 개인정보가 유출되거나, 의심스런 URL 접속으로 악성앱 설치가 의심되는 경우

❶ 휴대전화 초기화 또는 악성앱 삭제
(초기화 전까지 휴대전화 전원을 끄거나 비행기 모드 전환)

❷ 개인정보 노출 사실 등록(다른 휴대전화 및 PC 사용을 권장)

❸ 금융감독원 개인정보노출자 사고예방시스템(https://pd.fss.or.kr)에 개인정보 노출 사실을 등록하여 신규계좌 개설 및 신용카드 발급 등 제한

❹ 금융결제원 계좌정보통합관리서비스(www.payinfo.or.kr) 접속하여 계좌 지급 정지 신청
※ 영업점을 방문 또는 콜센터를 통해서도 지급 정지 신청 가능

❺ 한국정보통신진흥협회 명의 도용 방지 서비스(www.msafer.or.kr)접속 후 본인 명의 휴대전화 신규 개설 차단

3 경찰서에서 발급한 사건사고사실확인원 등 증빙 서류와 함께 지급 정지 신청한 영업점에 피해구제신청 서면 접수

필요 서류는 방문 전 금융회사 또는 경찰서 문의
※ 즉시 대응 조치를 시행한 이후, 금융회사 및 경찰 안내 등에 따라 인증서 폐지·재발급 신분증 분실 신고 등 필요한 추가 조치 실시

4 본인 신용 정보 열람 서비스(www.credit4u.or.kr) 확인

- 본인 신용 정보 열람 서비스를 통해 금융회사 등에서 받은 대출 내역 및 연체 정보 등 본인 명의의 대출, 연체, 보증정보 확인 가능
- 연체 정보 확인 등을 통해 대출 상환 관리에 활용할 수 있고, 소멸시효 완성 여부 등을 확인하여 부당한 채권 추심에 대응 가능

4. 전기통신 금융사기 예방 10가지 수칙

1

금융 거래 정보 요구에 일절 응대하지 않기

전화로 개인정보 유출, 범죄 사건 연루 등을 이유로 계좌 번호, 카드번호 등의 정보를 묻거나 인터넷 사이트에 입력을 요구하는 경우 절대 응하지 않습니다.

2

현급지급기로 유인하면 100% 보이스피싱

현금지급기를 이용하여 세금, 보험료 등 환급을 명목으로 현금지급기로 유인하는 경우 절대 응하지 않습니다.

3

발신자 번호 확인하기

발신자 표시가 없거나 국제 전화번호의 경우 수신하지 않습니다.

4

개인·금융거래 정보를 미리 알고 접근하는 경우 내용의 진위 확인

개인·금융거래정보를 미리 알고 접근하는 경우가 많으므로 전화, 문자 메시지, 인터넷 메신저 내용의 진위를 반드시 확인합니다.

5

피해를 당한 경우 신속히 지급 정지 요청

보이스피싱을 당한 경우 경찰청 112콜센터 또는 금융회사 콜센터를 통해 사기계좌에 대해 지급 정지를 요청합니다.

6

유출된 금융 거래 정보 즉시 폐기하기

유출된 금융 거래 정보는 즉시 해지 또는 폐기합니다.

7

예금통장 및 현금(체크)카드 양도 금지

통장이나 현금(체크)카드를 타인에게 양도 시 범죄에 이용될 수 있으며, 통장이나 현금(체크)카드 양도는 전자금융거래법 위반으로 형사 처벌을 받을 수 있습니다. (5년 이하의 징역 또는 3천만 원 이하의 벌금)

8

발신(전화)번호는 조작이 가능함을 인지하며 사기범들의 말에 속지 않기

텔레뱅킹 '사전지정번호제'에 가입되었다 하더라도 인터넷 교환기를 통해 발신번호 조작이 가능하므로, 사기범들의 말에 현혹되지 않습니다.

9

금융회사 등의 정확한 홈페이지 여부 확인하기

피싱사이트의 경우 정상적인 주소가 아니므로 문자 메시지, 이메일 등으로 수신된 금융회사 및 공공기관의 홈페이지는 반드시 정확한 주소인지 확인합니다.

10

「전자금융사기 예방서비스」 적극 활용하기

타인에 의해 무단으로 공인인증서가 재발급 되는 것 등을 예방하기 위해 각 은행에서 시행하는 「전자금융사기 예방서비스」를 적극 활용합니다.

5. '보이스피싱제로' 사업 안내

'보이스피싱제로'는 전 국민 대상으로 전기통신 금융사기 피해 예방 및 인식 제고 캠페인을 진행하며, 전기통신 금융사기(보이스피싱/메신저피싱/스미싱) 피해자 대상으로 경제적 지원과 법률·심리 상담을 지원하여 무너진 일상을 회복시키고 재기할 수 있도록 돕는 사업입니다.

사업명 보이스피싱제로(전기통신 금융사기 피해 지원 및 예방 사업)

사업 기간 2023년 10월 ~ 2024년 6월

사업 내용

생활비 지원	전기통신 금융사기 피해자 대상으로 생활 안정을 위해 긴급 생활비를 지원해 드려요! * 1인 최대 지원금 300만 원
법률 상담 지원	전기통신 금융사기 피해자 대상으로 법률적 어려움을 해소하기 위해 법률 상담 및 소송을 지원해 드려요! * 대한법률구조공단 연계를 통한 지원
심리 상담 지원	전기통신 금융사기 피해자 대상으로 심리 정서 회복을 위해 심리 검사 및 치료비를 지원해 드려요! * 1인 최대 지원금 200만 원
예방 교육 및 보험 지원	청소년/사회 초년생/노년층 등 일반 시민 대상으로 전기통신 금융사기 피해 예방 교육 및 보험 가입을 지원해 드려요!

사업 문의

보이스피싱제로 사무국

연 락 처 1811-0041

홈페이지 voicephisingzero.co.kr

검색창에 '보이스피싱제로'를 입력하세요!

굿네이버스

발 행 일 2024년 3월
발 행 처 보이스피싱제로 사무국
홈 페 이 지 voicephisingzero.co.kr
연 락 처 **Tel** 1811-0041 **Fax** 02-6733-1067