기타 후속조치 및 피싱 예방 서비스

01 신분증 재발급
※ 온라인 신청 시 인증서 또는 휴대전화 인증 필요

주민등록증
정부24 홈페이지 (gov.kr) 또는 주민센터 방문
※ 6개월 이내 촬영한 증명사진, 이전 주민등록증 지참

운전면허증
도로교통공단 안전운전 통합민원 (safedriving.or.kr) 홈페이지 또는
전국 운전면허시험장 · 경찰서 민원실(강남경찰서 제외) 방문

02 공동 · 금융인증서 재발급
인증서 발급기관 홈페이지 또는 앱에서 재발급/폐기

03 개인정보 도용, 유출여부 확인
개인정보포털 (privacy.go.kr)에서
명의도용이 의심되거나 원치 않는 웹사이트 회원탈퇴 가능

'털린 내 정보 찾기 서비스' (kidc.eprivacy.go.kr)에서
계정정보 유출 여부 확인 및 비밀번호 변경 등 보안 강화

04 명의도용 계좌/카드/대출 조회
계좌정보통합관리서비스 (https://www.payinfo.or.kr/)
본인의 은행·보험·상품금융·대출·카드발급 정보 등을 조회할 수 있는 서비스
→ 어카운트인포 모바일 앱으로도 조회 가능

정부 24 | 도로교통공단 | 개인정보포털 | 털린내정보찾기 | 계좌정보통합관리서비스

피싱 예방 서비스

은행 신청

01 여신거래 안심차단서비스
개인정보 유출 등에 의하여 자기도 모르게 신용대출
카드론 등이 실행되는 것을 사전에 차단할 수 있는 서비스

02 비대면 계좌개설 안심차단서비스
개인정보 유출 등에 의하여 자기도 모르게 비대면으로
계좌가 개설되어 범죄에 이용되는 것을 사전에 차단할 수
있는 서비스

**03 지연이체 서비스, 입금계좌지정 서비스,
해외 IP 차단 서비스 등**

통신사 신청

01 번호도용 문자 차단 서비스
내 번호를 도용해 피싱 등 불법 문자를 Web에서 보낼 수
없도록 차단하는 통신사의 무료 부가서비스
→ **이용중인 통신사로 신청 가능**
(Web 발신에 일부 제한되는 부분도 있어 상담 후 신청)

**02 휴대전화 소액결제 차단 또는 한도조정,
콘텐츠 자동결제 차단 서비스**

피해지원 사업소개

01 기업 공익 사업 : '보이스피싱 제로' https://voicephisingzero.co.kr

지원대상 전기통신 금융사기(보이스피싱/메신저피싱/스미싱) 피해자 및 일반 시민

지원내용

생활비 지원
전기통신 금융사기 피해 회복을 위한 **긴급 생활비 300만원**
(※ 1인 최대 지원금 300만원)
※ 단, 피해금액이 1인 최대 지원금 300만원 이하인 경우 피해 금액만큼 지원

선정 기준
- 최근 3년 이내 전기통신 금융사기 피해자
- 중위소득 100% 이하인 자
- 전기통신 금융사기 수사 진행 중 또는 종결자

법률 상담 지원
전기통신 금융사기 관련 **법률 기본 상담**,
전기통신 금융사기 관련 **민사 소송** (소송 상담, 변호사 비용 등)
→ 대한법률구조공단 연계를 통한 지원

선정 기준
- **기본 상담** - 최근 3년 이내 전기통신 금융사기 피해자
  - 수사 진행 중 또는 종결자
- **민사 소송** - 기본 상담 진행자 중 민사 소송 지원 가능 대상
  - 중위소득 125% 이하인 자

심리상담 지원
전기통신 금융사기 피해 회복을 위한 **심리 상담비**
(심리 치료 및 검사, 진료비 및 약제비 등 1인 최대 200만원)

선정 기준
- 최근 3년 이내 전기통신 금융사기 피해자
- 수사 진행 중 또는 종결자
- 전문가 자문위원 심사를 통한 선정

신청 방법
사무국 메일 / 팩스를 통한 사업 신청 서류 제출
생활비 지원, 법률 상담 지원 → 개인 신청 및 기관 신청
심리 상담 지원 → 기관을 통한 신청
예방 교육 및 보험 지원 → 기관 및 단체 신청(사전 접수)

문의처
연 락 처 1811-0041
팩 스 02-6733-1067
이 메 일 sinhan-voice@gnkr.or.kr
상담 시간 월~목: 10:00 ~ 17:00
금: 10:00~12:00

02 '비대면 금융사고 책임분담기준'에 따른 은행권 자율배상 제도 안내

개 요 보이스피싱 등 비대면 금융사고의 소비자 피해구제를 위해 은행의 사고예방 노력과 이용자의 과실 정도를 함께 고려하여 자율적으로 손해를 배상하는 제도

대 상 보이스피싱 등을 당해 개인정보가 유출되어 제3자에 의해 본인 계좌에서 금액이 이체되는 등 비대면 금융사고로 금전적 피해 발생 시 (2024.1.1 이후 발생분)

신청방법 피해가 발생한 은행 영업점 또는 콜센터에 상담 및 배상신청

보이스피싱, 알면 예방이 가능합니다

보이스피싱 범정부 TF

과학기술정보통신부 | 방송통신위원회 | 경찰청 | 금융감독원 | KISA 인터넷진흥원

주요 피싱범죄 유형 및 예방법 안내

01 접근 방법

"카드 배송", "우체국" 등을 사칭하여 접근합니다. 일상 속 익숙한 명목으로 연락이 오더라도, 반드시 공식 기관에 연락해 확인하세요.

02 기관사칭

검사·경찰·금융감독원 등 공공기관은 절대 금전을 요구하지 않습니다. "범죄 연루", "구속", "약식 조사 전환"을 언급하며 금전을 요구하는 경우, 100% 피싱입니다.

03 대출빙자

은행 대출은 반드시 창구 방문 또는 공식 앱을 통해 신청하세요. 저금리 대출 광고, 무작위로 전송된 대출 안내 문자는 100% 피싱입니다.

04 자녀·납치빙자

최신 기술로 가족의 목소리와 얼굴까지 조작할 수 있습니다. 전화나 문자로 가족을 사칭하여 돈을 요구할 경우, 반드시 직접 확인하세요.

05 악성 앱

문자나 메신저로 전송된 인터넷 주소(URL)를 누르는 순간, 휴대전화의 모든 정보가 탈취될 수 있습니다.

06 고액 아르바이트

현금을 대신 받아 오거나 전달하는 아르바이트는 100% 피싱입니다. 보이스피싱 피해금을 운반하는 행위는 강력한 처벌을 받는 범죄입니다.

07 대포폰·대포통장

명의 제공 대가로 돈을 받는 것은 100% 피싱입니다. 대포폰과 대포통장은 자금 세탁에 이용되며, 형사 처벌을 받을 수 있습니다.

08 신분증

신분증이나 신용카드 사진 파일을 요구하는 경우, 100% 피싱입니다. 정상적인 기관은 신분증 사진을 요구하지 않습니다.

09 상품권

문자나 메신저로 상품권 핀 번호를 요구하는 것은 대표적인 피싱 수법입니다. 상품권 번호를 절대 타인에게 알려주지 마세요.

10 백신 검사

V3, 시티즌 코난 등 검증된 백신 프로그램을 설치하고 주기적으로 검사하세요. 사칭하는 악성 앱도 있으니, 앱스토어를 통해 공식 앱만 설치하세요.

악성앱이 설치되면 이렇게 위험합니다!

주의

악성 앱이 설치되면 어디에 전화하더라도 범죄조직에만 연결되므로 초기화 전까지 비행기 모드, 데이터 차단 및 와이파이 차단하고 모바일 백신점검 및 악성파일(.apk)을 삭제하세요.
도움이 필요한 경우 다른 휴대전화로 112 신고 또는 경찰서 방문하세요.

이런 경우 악성 앱이 설치!

① 출처를 알 수 없는 링크를 눌러 파일을 설치한 경우
② 모바일 대출신청서, 은행 앱을 가장한 파일을 받은 경우
③ 수사 협력 요청을 가장한 파일을 받은 경우
④ 휴대폰 보안검사가 필요하다며 파일을 받은 경우

악성 앱 주요 기능 및 현상

악성 앱 주요 기능	악성 앱 설치된 휴대전화에서 나타나는 현상
① 문자메시지 탈취	피해자에게 온 문자 인증코드 탈취해 피해자 명의 2차 본인인증
② 연락처 목록 탈취, 문자 발송	스마트폰의 지인 연락처를 수집, 그 폰으로 지인에게 스미싱(부고장, 청첩장 등) 문자 발송
③ 이미지 또는 파일 탈취	저장된 신분증·중요 서류를 빼앗아, 피해자 명의의 계좌·폰을 새로 개통하고 대출·계좌이체 등 2차 금융거래
④ 앱 설치 목록 확인, 삭제, 숨기기	스마트폰에 설치된 정상적인 금융·백신 앱 삭제하고, 악성 앱을 숨겨 흔적을 남기지 않음
⑤ 카메라·마이크·화면 스트리밍, 위치정보 탈취	악성 앱 설치된 스마트폰을 감시·감청
⑥ 전화 수·발신전화 가로채기	**발신전화** 피해자가 112에 전화 걸면, 그 전화를 끊고 준비해둔 음성과 화면을 송출, 동시에 피싱조직으로 연결 **수신전화** 범죄조직이 전화를 걸면, 피해자의 화면을 112로 위장하고 전화가 끝난 뒤 통화 기록을 조작

※ 악성앱(원격제어 포함) 설치가 된 경우에는 피싱범과의 통화기록, 문자내용, 카카오톡 대화내용 등을 캡쳐하여 별도 보관 후 휴대폰 전체 초기화를 진행하세요.

이렇게 대응하세요!

01 112에 피해신고 및 계좌 지급정지 신청하세요 (24시간)

① 피해금을 계좌로 보낸 경우 경찰청(112)에 피해사실을 신고하고 범인이 돈을 옮기지 못하도록 즉시 지급정지 신청
(지급정지 신청일로부터 3일 내 경찰서에서 '사건 사고사실확인원'을 받아 지급정지된 은행에 제출(※ 은행에 방문해 피해구제 신청 접수)
※ 돈이 출금되거나 입금된 은행 콜센터에도 지급정지 신청 가능
② 악성 앱 설치 등으로 개인·금융정보 유출이 의심되는 경우 '본인 계좌 일괄 지급정지'로 피해를 예방할 수 있음

본인계좌 일괄 지급정지란?

개 요 개인·금융정보 유출이 의심되는 경우 본인 명의의 모든 계좌를 조회하여 **피해가 우려되는 계좌의 지급정지를 신청하는 서비스**

신청방법
① **인증서가 없는 경우:** 은행 콜센터 전화 또는 방문 신청
② **인증서가 있는 경우:** 각 은행 홈페이지 및 앱, PC 또는 휴대전화로 신청 가능

PC 신청
① 금융결제원 계좌정보통합관리서비스(payinfo.or.kr) 접속
② 본인 계좌 일괄지급정지 메뉴에서 은행권, 제2금융권, 증권사 中 선택
③ 2중(인증서+휴대전화) 본인확인
④ 지급정지 신청할 계좌 선택

휴대전화 신청
① 금융결제원 "어카운트인포-계좌정보통합관리" 설치
② 2중(인증서+휴대전화) 본인확인
③ 본인 계좌 지급정지 메뉴에서 은행권, 제2금융권, 증권사 中 선택
④ 지급정지 신청할 계좌 선택

02 휴대전화 신규가입 등 차단하세요 (홈페이지 평일·주말 공통 09:00~22:00)

개 요 명의도용으로 인한 이동전화 신규가입·번호이동·명의변경 등을 사전에 차단할 수 있는 서비스

신청방법
① **PC 신청:** 엠세이퍼(www.msafer.or.kr) 접속 → '가입제한서비스' 클릭 → 공동·금융인증서 로그인
② **통신사 방문:** 신분증을 가지고 통신사 지점·직영점에 방문하여 신청
③ **휴대전화 신청:** 엠세이퍼(모바일) · PASS앱 · 카카오뱅크앱에서 확인 가능
** 가입제한서비스 하단 통신사별 요금조회 기능 추가*

03 명의도용을 확인하세요 (홈페이지 평일·주말 09:00~22:00 / 고객센터 평일 09:00~18:00)

개 요 이동전화, 무선인터넷, 인터넷전화의 가입현황을 실시간으로 열람할 수 있는 서비스

신청방법
① **PC 신청:** 엠세이퍼(www.msafer.or.kr) 접속 → '가입사실현황조회 서비스'클릭 → 공동·금융인증서 로그인
② **통신사 방문:** 신분증을 가지고 통신사 지점·직영점에 방문하여 신청
③ **휴대전화 신청:** 엠세이퍼(모바일) · PASS앱&카카오뱅크앱(이동전화 조회)에서 확인 가능

04 보이스피싱 피해사례 안내 (www.msafer.or.kr)

개 요 대표적인 보이스피싱 피해사례 및 전용 영상자료실 게시판 운영

112로 전화하면 '전기통신금융사기 통합신고대응센터'로 연결, 전문 상담사를 통해 통신·금융 대응 방안을 순차적으로 안내받으실 수 있습니다.
* 경찰청·금감원·한국인터넷진흥원·이통사 합동 대응 / 운영시간 : 평일 09:00~22:00