



보도시점 2023. 9. 26.(화) 17:00
(행사 종료 시) 이후

배포 2023. 9. 26.(화) 10:00

보이스피싱, 이제 '112'로 신고하세요.

정부, 9. 26.(화) 관계부처 및 민간기업 관계자 참석 하에 「통합신고대응센터」 개소식 개최
- 부처별로 운영하던 신고창구를 전화는 '112', 인터넷은 '보이스피싱지킴이'로 통합
- 신종수법 대비, 범정부 대응 4단계 프로세스(예방-대비-대응-사후관리) 기반 총력대응
- 통합신고대응센터-범정부 TF 間 연계 강화로 즉각적이고 실효적 대책 수립

- 보이스피싱 신고절차 및 피해구제가 대폭 간소화된다. 이제 보이스피싱 신고는, 전화는 112, 인터넷은 '보이스피싱지킴이' 사이트로 일원화되어, 한 번의 신고로 사건처리부터 피해구제까지 원스톱으로 처리될 수 있게 된다.
- 정부는 9. 26.(화) 16:00, 방기선 국무조정실장, 윤희근 경찰청장 등 정부 관계자들과 통신·금융회사 관계자들이 참석*한 가운데 「전기통신금융사기(이하 '보이스피싱') 통합신고·대응센터」를 개소했다고 밝혔다.
 - * 국무조정실장, 경찰청장, 금융위 사무처장, 방통위 사무처장, 과기부 네트워크정책실장, 금감원 금융소비자보호처장, 한국인터넷진흥원장, 기업 관계자 등
- 그간 정부는 '보이스피싱 대응 범정부 TF*'를 중심으로 강력한 단속과 수사, 그리고 통신·금융 특별대책 등을 추진한 결과, '22년 발생건수 및 피해금액이 전년대비 30% 가량 대폭 감소하는 성과를 창출하였으나,
 - * 국무조정실장(단장), 과기정통부, 방통위, 금융위, 검·경 등 관계부처 참여('21.12월~)
 - 신고·상담 정보를 실시간 추적·분석하고 범정부 TF와 연계하여 정책에 반영하는 통합 대응기구가 없어 종합적·체계적 대응에 어려움을 겪었다.
 - 특히, 부처별로 신고·대응창구를 개별* 운영하고 있어, 신고 및 대응을 위해 국민이 직접 소관 부처를 찾아야 했고, 동일한 내용을 각 기관에 여러 번 반복 신고해야 하는 불편함이 있었다.
 - * 피해신고는 112(경찰), 지급정지는 1332(금감원), 범행수단 차단은 118(KISA)로 개별화
- 이와 같은 국민 불편을 해소하고 보다 체계적이고 유기적인 범정부적 통합 대응을 경찰청·방통위 등 관계부처와 금감원·한국인터넷진흥원 등 유관기관, 통신3사(통신사별 2명씩, 6명 통합근무 중) 등 민간기관이 참여하는 통합 대응기구를 설치하게 되었다.

- 이제, 국민들은 보이스피싱 피해시, ‘112’에 신고하기만 하면 사건접수 뿐만 아니라 악성 앱 차단, 피해구제(지급정지) 등을 한 번에 처리 받을 수 있게 된다.
 - 또한, 범죄조직 검거 시, 신고되지 않은 사건까지 분석·추적하여 여죄의 단서로 활용하는 등 조직적 범죄에 대해 더욱 엄정한 처벌이 가능하고,
 - 최근 유행하고 있는 ‘악성앱 스미싱’ 등 신종수법에 효율적으로 대응하기 위해 센터를 중심으로, 예방-대비-대응-사후관리 등 범정부 대응 4단계 프로세스를 운영하여, 피싱 범죄에 대해 보다 효율적인 총력대응이 가능할 전망이다.
 - * 악성앱 문자 링크를 피해자가 클릭하면, 피해자 명의로 신규 폰을 개통하고 예금(대출) 탈취
 - 아울러, 신고·대응 과정에서 통합신고센터로 집적된 빅데이터를 체계적으로 관리·분석하고 범정부 TF와 공유하여 실효적 대책을 즉시 추진하는 등 보이스피싱 대응 및 예방에 상당한 효과가 있을 것으로 기대하고 있다.
- 참석자들은 개소식 직후 보이스피싱 범죄에 대한 민·관 공동 대응체계를 구축하기로 하는 내용의 업무협약(MOU)도 체결하였다.
- 향후, 정부는 삼성전자·이통3사·은행연합회와 통신·금융분야 협업사항을 공동 발굴·추진하고, 피해확산 방지를 위한 업무지원 및 정보공유를 통해 보이스피싱 관련 정책·제도 도입 및 대국민 홍보에 상호 협력하기로 하였다.
- 윤희근 경찰청장은 경과보고를 통해 “보이스피싱은 개인의 재산을 빼앗으며, 고통과 상처를 남기고, 사회적 불신까지 초래하는 악성 범죄 그 자체”라고 하면서, “통합신고대응센터가 보이스피싱 범죄 근절의 마중물이 될 수 있도록 최선을 다하겠다”고 각오를 밝혔다.
- 이어, 방기선 국무조정실장이 축사를 통해 “피싱 범죄는 경제적 살인으로 간주해 대응해야 하는 악질적 범죄”라고 하면서, “통합신고대응센터가 쏠 세계적으로 가장 우수한 범부처 합동 대응 기구의 표본이 될 수 있도록 비상한 각오로 근무해달라”고 주문하며, 정부차원의 지원을 아끼지 않겠다고 하였다.
- 또한, “보이스피싱 대응 범정부 TF는 통합신고대응센터와 유기적인 협력을 통해 즉각적이고 실효적인 대책이 현장에 즉시 반영될 수 있도록 범정부 총력 대응을 지속적으로 펼쳐나갈 것임”을 밝혔다.
 - 마지막으로, “상담원 등 센터 관계자들에게 국민의 안전한 일상을 지켜 내는 최전선 파수꾼이자, 최후의 보루라는 각별한 사명감과 자부심을 가지고 한치의 소홀함 없이 근무해줄 것”을 당부하였다.

※ 최근 신종수법 및 대처방법 (참고 4~6 참조)

담당 부서 <총괄>	국무조정실 일반행정정책관실	책임자	과 장	송헌규 (044-200-2082)
		담당자	경 위	최명현 (044-200-2094)
<공동>	경찰청 국가수사본부 경제범죄수사과	책임자	과 장	김종민 (02-3150-2037)
		담당자	팀 장	김혁진 (02-3150-3430)
<공동>	과학기술정보통신부 통신이용제도과	책임자	과 장	이정순 (044-202-6650)
		담당자	사무관	김주영 (044-202-6657)
<공동>	방송통신위원회 인터넷이용자정책과	책임자	과 장	박경주 (02-2110-1520)
		담당자	사무관	전혜정 (02-2110-1522)
<공동>	금융위원회 전자금융과	책임자	과 장	김수호 (02-2100-2970)
		담당자	전문관	남명호 (02-2100-2974)
<공동>	금융감독원 금융사기전담대응단, 정보화전략국	책임자	국 장	임정환 (02-3145-8150) 진태종 (02-3145-5370)
		담당자	팀 장	김세모 (02-3145-8130) 이우람 (02-3145-5420)
	한국인터넷진흥원 이용자보호단	책임자	단 장	정원기 (061-820-1840)
		담당자	팀 장	박해룡 (02-405-5245)



참고1**개소식 행사 개요**

□ 행사 개요

- 일시·장소 : '23. 9. 26.(화) 16:00, 통합신고대응센터 청사(효자로 9길 27)
- 참석자 : 국무조정실장, 경찰청장, 관계기관장, 기업대표(통신·금융·제조사) 등

< 주요 참석자 >

정부 공공기관	총리실	국무조정실장
	관계부처	경찰청장, 금융위(사무처장), 방통위(사무처장), 과기정통부(네트워크정책실장)
	공공기관	김미영 금융감독원 부원장, 이원태 한국인터넷진흥원장
민간기업	통신	주은기 삼성전자 부사장 손영규 SKT 부사장 박효일 KT 부사장 홍관희 LG+ 부사장
	금융	이태훈 은행연합회 전무이사

- 행사 내용: ①현판식, ②축사, ③업무협약식(MOU), ④센터 참관

< 행사 식순 (案) >

시 간		행사 내용	비 고
15:50~16:00	10'	사전 환담	1층 현관(스탠딩)
16:00~16:03	3'	국민의례 및 참석자 소개	1층 중앙 현관 앞 1층 행사장(야외)
16:03~16:08	5'	현판식 및 기념촬영	
16:08~16:11	3'	경찰청장 경과보고	
16:11~16:14	3'	국무조정실장 축사	
16:17~16:23	6'	업무협약식(MOU)	
16:23~16:25	2'	이동	2층(중앙계단)
16:25~16:30	5'	센터 견학	2층 사무실
16:30~		행사 종료	

□ **설립 배경**

- (피해의 심각성) 보이스피싱은 112 신고건수 日 평균 1천 건, '21년 피해액 7,744억원을 기록한 대표적인 서민경제 침해 범죄
- (신고불편) 그러나 범행 과정에서 다양한 금융·통신수단이 활용된다는 이유로 부처·기관별 신고·조치 창구를 각각 운영해 왔음
 - 이에, 국민이 직접 신고처를 찾아 같은 내용을 반복하는 불편과 신고 포기 사례 발생, 통합 신고·처리체계 구축 필요성 지속 제기
- (통합 대응체계 부재) 외국*과 같이, 부처간 정보 공유·분석으로 보이스피싱 근절을 위한 범정부 합동 대응체계 구축 필요성 제기
 - * 외국의 경우 '사기정보분석원(영국)', '사기대응센터(싱가폴)' 등 전문기관 운영

□ **추진경과**

- '22. 1. 국조실 주관 관계부처 회의, 경찰청 내 범부처 통합신고·대응센터 설치 및 운영 협의(주무부처: 경찰청)
- '22. 4. 준비단 발족 및 통합신고대응센터 관련 인수위 브리핑

< 인수위 브리핑 주요 내용 >

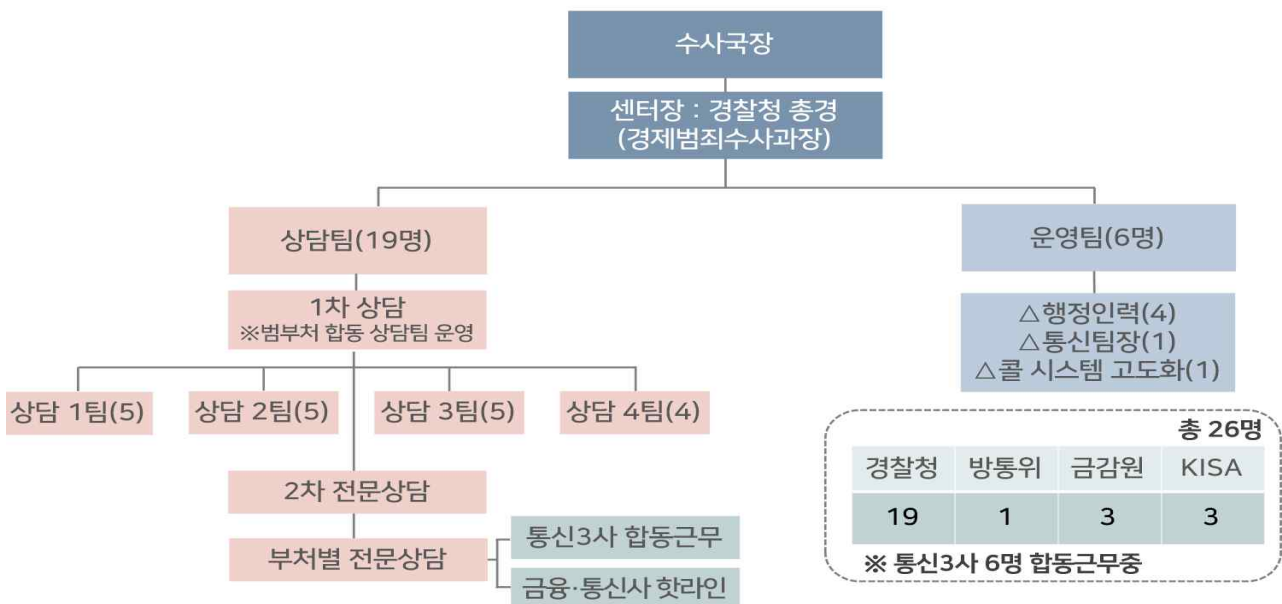
- ▶ 전기통신금융사기로 인한 피해가 심각해 범죄를 뿌리뽑기 위해 경찰청 내 유관기관이 참여하는 통합신고·대응센터 조기 설치
- ▶ 피해자들이 부처별·신고창구별로 같은 내용을 반복 신고해야 해서 신고를 포기하고 있는데, 이를 해소하기 위한 원스탑 처리체계 필요

- '22. 8. 「전기통신금융사기 통합신고대응센터 설치 및 운영에 관한 규정(국무총리 훈령)」 제정 및 공포
- '23. 7. 20. 전기통신금융사기 통합신고대응센터 개소

□ 운영개요

- (시기·장소) '23. 7. 20.~, 통합신고대응센터 청사 (종로구 창성동)
- (운영인력) 센터장은 경찰청 총경(경제범죄수사과장 겸임), 파견인력 포함 총 26명*, 향후 추가상담원 및 데이터 분석·대응 인력 증원 추진
 - * △경찰관(11) △임기제공무원(8) △금감원(3) △KISA(3) △방통위(1)
- (운영시간) 신고·상담이 집중(전체 신고 80%)되는 평일 09:00~18:00
 - ※ 기존 시스템(112·182·118)과 유기적 협력(①112에서 일반 상담 ②평일 센터로 신고·제보 안내 ③피해자 대상 센터에서 콜백)으로 야간·휴일 대응

□ 조직도



□ 센터의 역할

- (신고접수) 전화는 '112', 온라인은 '보이스피싱 지킴이'(금감원)로 일원화
 - 피해신고는 112에서 경찰관 출동하여 초동조치* 후 센터에서 인계 받아 ①피해구제 ②범행수단 차단 ③추가 예방 등 상세 설명
 - * 계좌 지급정지 / 현장 CCTV 확보 / 정식 사건 접수 등
 - 비피해·단순 상담 건은 ① 피해구제 방법 안내(피해금 지급 등) ② 추가 예방 등 상담 안내하고, 신고자료는 D/B로 만들어 보관

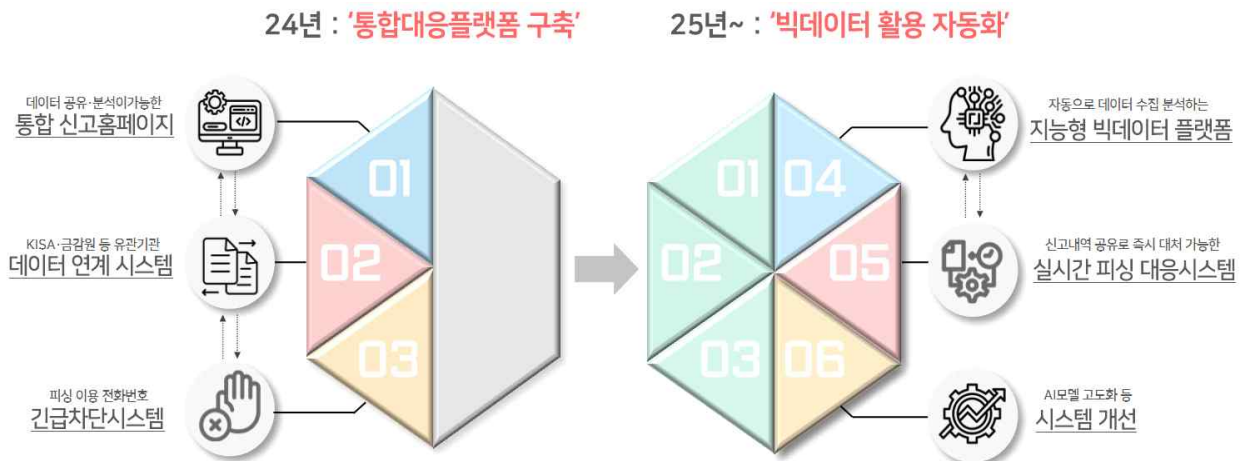
< 신고창구 일원화 >



- (대응·분석) 신고 내용을 근거로 ‘소관부처별’ 대응 및 후속조치, 신고 D/B는 기존 사건자료(KICS·112·182 신고내역)와 대조 등 심층 분석
- (예·경보 발령 등) 분기별 1회(필요시 수시로) 최신 유행 수법 및 신·변종 수법 분석, 보도자료 배포 등을 통해 예·경보 발령
 - 내부적으로 시도청·경찰서 수사팀에 범죄데이터 분석자료 제공, 대외 기관간 △범행동향 △제도개선 사항 등을 공유·대책 마련 병행

□ 향후 운영방향

- '23년 신고·상담창구 일원화, '24년은 통합대응플랫폼 구축을 통해 범정부 합동 실시간 대응체계 구축 목표



전기통신금융사기 근절 협업 강화를 위한 업무협약서

협약기관(이하 '각 기관')은 전기통신금융사기 근절을 위한 협업 강화를 위해 다음과 같이 업무협약을 체결한다.

제1조(목적) 본 협약은 전기통신금융사기 피해를 예방하고 범죄를 근절하기 위한 각 기관 간 협력과 지원을 강화하는 것을 목적으로 한다.

제2조(기본원칙) 협약기관은 관계 법령을 준수하고, 상대 기관의 규정을 존중하며, 본 협약서에 명시된 사항들을 신의와 성실의 원칙에 따라 이행한다.

제3조(협약내용) 협약기관은 다음 각호의 내용에 대해 상호 협력한다.

1. 범죄수법·피해사례 공유를 통한 전기통신금융사기 피해 예방 및 근절을 위한 협업 사항의 발굴 및 추진
2. 전기통신금융사기 피해확산방지를 위한 업무지원 및 정보공유
3. '전기통신금융사기 통합신고대응센터'의 운영 및 업무 수행을 위한 협력
4. 기타 전기통신금융사기 관련 정책·제도 도입 등 필요사항 지원

제4조(비밀유지 의무) 각 기관은 이 협약과 관련하여 상호 교류되는 자료 및 정보를 이 협약서에 명시된 목적 외에 이용할 수 없으며, 각 기관의 사전 동의없이 제3자에게 제공하거나 언론 등 대외에 발표하지 아니한다. 단, 상호협력 및 제공 이전부터 각 기관이 보유하고 있던 자료에 대하여는 그렇지 아니하다.

제5조(협약이행을 위한 세부사항) 구체적인 협력 사항과 본 협약서에 명시하지 않은 세부사항 및 시행 과정에서 보완이 필요한 사항에 대해서는 협약기관이 상호 협의하여 정한다.

제6조(효력 및 협약기간) 이 협약의 효력은 각 기관이 서명한 날부터 발생하며, 유효기간은 2년으로 하되, 상호 이의가 없는 경우 1년씩 자동 연장된다.

제7조(법적구속력 배제) 본 협약서의 내용은 제4조를 제외하고는 별도의 합의가 없는 한 협약기관을 법적으로 구속하지 않는다.

! 악성앱 스미싱(피싱) 주의 안내

최근 모바일 청첩장, 택배배송 조회, 건강검진 결과조회 등 악성앱 링크가 포함된 메시지를 보내 피해자가 링크를 클릭하면 개인정보를 탈취, 피해자 명의로 신규폰을 개통하여, 예금을 탈취하고 대출을 실행하는 사기수법이 확산되고 있어, 국민들이 꼭 알고 실천해야 할 4가지 사항을 다음과 같이 알려드립니다.

1. V3 모바일·알약M·후후·모바일가드 등 모바일 백신 설치하여 주기적으로 악성앱 설치여부 점검
2. 유사시 무조건 112로 신고
3. 본인도 모르는 휴대전화가 개통되어 금융범죄로 피해발생 사전 예방 방지
※ 휴대폰 명의도용방지서비스(엠세이퍼)에 등록
4. 주말·연휴 중에도 전화(112)로 본인계좌 일괄지급정지 가능

<p>악성앱 스미싱</p> 	<p>◇ 모바일 청첩장 등 링크(URL)는 절대 클릭하지 말고 발신자에게 반드시 확인</p> <ul style="list-style-type: none"> ▶ 택배 배송조회·건강검진 결과조회 등 문자로 수신된 링크(URL) 클릭 시, 악성코드가 설치되어 범인이 원격으로 피해자의 휴대폰을 조종하거나 피해자 명의로 신규 폰을 개통하여 예금 탈취
<p>진술서 피싱</p> 	<p>◇ 수사기관·금융기관을 사칭하여 특정 앱 설치 유도하면, 100% 보이스피싱</p> <ul style="list-style-type: none"> ▶ 범인은 진술서 작성에 필요하다며 '스마트 진술서' 악성 앱 설치를 요구하고, 앱을 설치하면 개인정보 탈취와 함께 모든 전화와 문자가 범인에게 연결(강수강발 : 강제수신·강제발신) ▶ 검찰·경찰·금감원 등 정부기관은 절대 특정 앱 설치를 요구하지 않음 ▶ 구글 플레이스토어 및 애플 앱스토어가 아닌 경로에서 앱 설치 자제
<p>AI 피싱</p> 	<p>◇ 가족·지인이라도 전화 통화로 금전을 요구할 경우, 서로만 아는 정보(암호)들을 질문하여 반드시 본인임을 확인할 것</p> <ul style="list-style-type: none"> ▶ 최근, AI 기술(딥러닝)을 활용, 부모·자녀·친구나 지인의 얼굴·목소리를 위조하여 전화(영상) 통화를 통해 금전을 요구하는 피싱 수법 등장
<p>투자유도</p> 	<p>◇ 주식(코인) 손실보상을 빌미로 개인정보를 요구하거나, 과도한 수익률을 보장한다며 접근하면, 100% 보이스피싱</p> <ul style="list-style-type: none"> ▶ 주식거래 손실을 보상해주는 회사로 속여, 손실금 1억원을 주겠다며 개인정보 요구 ▶ 피해자 개인정보로 1억원 대출, 마치 범인들이 송금한 것처럼 속여 ▶ 수익률 좋은 코인이 있다며, 1억원 재투자 요구 후, 입금받으면 잠적
<p>몸캠피싱</p> 	<p>◇ 채팅앱에서 음란 영상통화 제안 시, 피싱조직이므로 절대 응하지 말 것</p> <ul style="list-style-type: none"> ▶ 만남어플 채팅을 통해 여성행세를 하며 접근하여 음란 영상통화를 제안한 후, 녹화된 음란행위 장면을 유포하겠다고 협박하여 금품을 갈취하는 수법에 20~30대 남성 피해 심각



악성앱 스미싱 피해 흐름도 및 대응방법

- 최근 피해사례 -

- ① A씨는 문자로 수신된 모바일 링크를 클릭한 후, A씨 명의의 보험사와 은행 등에서 1억 4천만원 대출이 이루어져 특정 계좌로 입금되고, 입금된 돈은 다시 여러개의 대포통장으로 출금
- ② B씨는 문자로 수신된 모바일 링크를 클릭한 후, 익일 휴대전화가 정지되었으며, 예금통장 인출 및 각종 쇼핑물·게임사이트에서 결제대금으로 총 1억 2천만원 가량의 피해 발생

- 피해 흐름도 -

STEP 01 STEP 02 STEP 03 STEP 04 STEP 05

<p>스미싱 문자 수신</p> <p>[Web발신] (링크)pf.kakao.com/_xnBjPK/freind 모바일정침장 저희 두사람 결혼합니다 무료거부 0808000442</p> <p>스미싱 문자는 청첩장, 건강 검진조회, 택배조회, 주식 추천 등 다양한 형태로 발송</p>	<p>URL(링크) 클릭 <악성앱 설치파일(APK) 저장></p> <p>다운로드가 완료되었습니다. (/storage/ emulated/0/Download/ 모바일초대장_V10(1)_2.1.22.apk)</p> <p>링크 클릭 시, 악성앱 설치파일 (APK)이 저장, 추가 팝업창에서 '확인'을 누르면 악성앱 설치</p>	<p>악성앱 설치 '확인' 클릭 <악성앱 자동 설치·실행></p> <p><input type="checkbox"/> 내용을 이해했으며 설치하겠습니다.</p> <p>계속 설치 확인</p> <p>악성앱이 설치되면, 범인이 피해자 휴대폰 내의 모든 정보를 탈취하고, 원격으로 조작·감시</p>	<p>휴대폰 해지 <번호이동 알뜰폰 개통></p>  <p>범인이 피해자 명의로 신규 알뜰폰을 개통하여 피해자 폰은 자동 해지(번호이동)</p>	<p>예금인출·대출실행</p>  <p>범인은 피해자 명의로 통장 개설, 대출실행, 카드발급 등을 통해 금전전취</p>
--	---	---	--	---

- 상황별 조치사항 -

< 단계별 피해 상황 >

< 피해자가 해야할 일(순서대로 진행) >

<p>< 문자나 카톡으로 받은 링크를 누른 경우 > - 악성앱 설치파일(APK) 저장 -</p>	<p>① 링크를 누른 경우, 악성앱 설치파일이 실행되지 않도록 설치 팝업창이 뜨면, '확인'을 누르지 말 것</p> <p>② 모바일 보안 앱을 실행하여 악성앱 삭제</p>
<p>< 링크를 누른 후, 설치 '확인'까지 누른 경우 > - 악성앱이 설치되어 실행 중인 상태 -</p>	<p>① 범인에 의한 휴대폰 원격조종 및 정보탈취를 차단하기 위해 비행기 모드로 전환 후, 보안앱으로 악성앱 삭제 및 공장 초기화 또는 전원 OFF ※ 반드시 비행기 모드로 전환 후에 전원을 꺼야 함</p> <p>② 내 계좌 일괄 지급정지(PC, 은행대리점, 콜센터)</p> <p>③ 공인인증서 폐기 후, 재발급하여 반드시 PC에 저장 ※ 범인에 의해 탈취된 인증서가 알뜰폰 가입 및 금융거래에 이용되는 것을 차단</p> <p>④ 신분증(주민등록증, 운전면허증) 및 신용카드 재발급 ※ 범인에 의해 탈취된 정보가 알뜰폰 가입에 이용되는 것을 차단</p> <p>⑤ 개인정보 노출자로 등록(pd.fss.or.kr) ※ 검색창에 '파인' 입력 후 서비스 이용 / 신규 계좌·카드발급 등 금융거래 차단</p> <p>⑥ 휴대폰 명의도용 서비스 가입(www.msafes.or.kr) ※ 인터넷에 '엠세이퍼' 검색 후 서비스 이용 / 신규 폰 개통 차단 신청</p> <p>⑦ 112 신고 → 통합신고대응센터 연계(수사, 피해구제, 링크 차단 등)</p>
<p>< 휴대폰이 갑자기 먹통이 된 경우 > - 범인이 피해자 명의로 신규 폰을 개통하여, 피해자 휴대전화는 자동해지(번호이동) 상태 -</p>	<p>① 타인의 휴대전화나 유선전화로 경찰청 보이스피싱 통합신고 대응센터(112)에 전화, 계좌 일괄 지급정지 신청 ※ 취약시간(야간, 주말)에는 콜센터 통해서만 신청 가능</p> <p>② 공인인증서·신분증·신용카드 재발급, 개인정보 노출자로 등록, 휴대폰 명의도용 서비스 가입</p> <p>③ 112 신고 → 통합신고대응센터 연계(수사, 악성앱 차단, 피해구제 등)</p> <p>④ 통신사 대리점 방문, 범인이 개통한 폰 해지 후 재가입</p>



보이스피싱 대응 범정부 TF

□ 휴대폰 명의도용 방지서비스(M-Safer) 개요

휴대폰 명의도용 방지

www.msafes.or.kr



명의도용 방지서비스를 이용하여 **본인 모르게**
 개통된 휴대폰을 조회하거나 추가개통을 차단

명의도용방지서비스(Msafer)란?

신규로 각종 통신서비스(이동전화, 무선인터넷[WiBro], 유선전화, 초고속인터넷, 인터넷전화[VoIP], 유료방송 등)에 가입하거나 명의변경을 통해 양도받을 경우 그 사실을 본인 명의로 사용하고 있는 이동전화 회선을 통해 SMS로 알려주는 서비스를 말합니다. 또한, 홈페이지(www.msafes.or.kr)에서는 **명의도용가입제한 서비스, 가입현황조회 서비스, 이메일 안내 서비스** 등의 부가 서비스를 제공하고 있으며, 본 서비스는 명의도용 피해를 예방하고자 제공하는 대국민 무료 서비스입니다.



명의도용방지서비스

- (가입제한 서비스) 타인이 내 명의로 휴대폰 신규가입(번호이동 포함) 및 명의변경을 할 수 없도록 사전 차단(또는 해지)하는 서비스
 - (이용 가능 통신사) 이통3사(SKT·KT·LGU+)뿐만 아니라, 알뜰폰 전체 대상으로 휴대폰 가입제한 서비스 등록 가능
 - (서비스 이용방법) 포털 검색창에 '엠세이퍼' 검색 → 명의도용 방지서비스 → 가입제한서비스 → 인증서 로그인* → 서비스 등록
 - ※ 로그인은 공동인증서, 네이버인증서, 카카오페이인증서만 이용 가능

- (가입사실현황조회 서비스) 본인 명의로 등록된 통신 서비스(휴대 전화, 인터넷, 방송서비스 등) 가입현황 확인 가능
 - ※ 본인인증 후 명의자의 '이름과 주민등록번호'로 가입 회선 일괄 조회 가능

참고6

「본인계좌 일괄지급정지 제도」 설명자료

보이스피싱으로 다수 계좌에서 자금이 한 번에 편취당하는 피해를 방지하기 위하여 피해자가 선제적으로 본인 명의 모든 계좌를 일괄하여 지급정지할 수 있는 제도

< 본인계좌 일괄지급정지 제도 주요내용 >

- 이용대상** : 만 19세 이상 내국인
* 미성년자, 외국인은 이용이 불가
- 대상계좌** : 수시입출금계좌(은행, 저축은행, 농협·수협·신협·산림조합, 새마을금고, 우정사업본부*) 및 금융투자회사계좌(증권)
* 현재 인터넷 및 모바일을 통한 우체국 계좌 지급정지는 가능하나, 영업점 및 고객센터를 통한 우체국 계좌 지급정지 등은 '23.10월 중 가능할 예정
- 이용채널** : (온라인) 어카운트인포 홈페이지(payinfo.or.kr) 및 모바일 앱, (오프라인) 거래하는 금융회사 영업점 및 고객센터*
* 2개 증권사(SK·하이투자)의 야간·주말 고객센터를 통한 지급정지 접수는 '23.10월 중 가능할 예정
- 이용시간** : **연중무휴 매일 00:30 ~ 23:30**
- 지급정지 신청** : 고객 본인 소유 계좌 조회* 및 일괄지급정지**
* 금융회사명, 관리점, 개설일, 계좌번호 등 상세정보 제공
** 정지 대상 거래 : 영업점 및 비대면 채널, 자동이체, 오픈뱅킹 등을 포함한 모든 출금거래
- 지급정지 해제** : 거래하는 금융회사 영업점 방문을 통한 해제

본인계좌 일괄지급정지 서비스 개요

		서비스 개요		
지급 정지	신청	거래 금융사 <u>영업점(방문신청)</u> ※ 영업시간 중	거래 금융사 <u>콜센터(전화로 신청)</u> ※ 연중무휴	'어카운트인포' 홈페이지 또는 모바일앱
		▶ 악성앱 스미싱으로 범인이 내 명의의 신규폰을 개통하여, 더 이상 내 폰을 사용할 수 없는 경우에는, <u>영업점 방문</u> 이나 <u>타인 전화로 콜센터</u> 에 지급정지 신청 가능		
해제	신청	<u>거래 금융사 영업점</u>		
	단위	<u>전체 금융사 계좌</u>		