

개인정보보호 교육의 공공성 (보이스 피싱 중점)

2024. 6. 5.(수)



개인정보보호 전문강사협회

목차

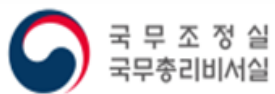
1. 개인정보보호 교육의 공공성(보이스 피싱 현황)
2. 아동·청소년 개인정보 보호 교육의 필요성
3. 보이스 피싱 사례 및 대응 방안

1. 보이스 피싱 현황

보이스피싱(Voice Phishing)이란 개인정보(Pprivate data)와 낚는다(Fishing)의 합성어로, 피해자를 기망 또는 협박하여 개인정보 및 금융거래 정보를 요구하거나 피해자의 금전을 이체하도록 하는 수법.

초기에는 보이스피싱 범죄가 수사당국 혹은 규제기관의 대응으로 통제 가능할 것으로 예상했지만 현재로서는 보이스 피싱 범죄의 근절은 요원할 것으로 인식되고 있으며, 오히려 보이스 피싱 시도 및 피해액은 지속해서 증가하고 있으며, 보이스피싱에 대한 정보가 부족한 20대 이하 취약계층 피해는 더욱 증가하고 있다. 아울러 인공지능을 활용한 대량의 피싱 메시지 등 간단하게 제작 가능할 수 있으며, 언어적 한계도 없어져서 더 교묘하고 치밀한 보이스 피싱 공격이 일반인을 대상으로 무차별적으로 발생하고 있다.

I. 보이스 피싱 현황



국무조정실
국무총리비서실

보도자료

다시, 대한민국!
새로운 국민의 나라

보도시점 배포 후 즉시 사용 배포 2024. 5. 1.(수) 12:00

“보이스피싱, 미리 알고 대비하면 막을 수있어요!”

-정부,「5월 가정의달」보이스피싱 집중 홍보기간 운영-

- ▶ 관계기관 ‘원팀’으로 홍보 분야 협력 강화, 피해 예방에 총력
- ▶ 국민 생활 접점·취약층 맞춤 홍보에 기관 간 상호 지원으로 시너지 제고
- ▶ 「단계별·상황별 대응을 위한 안내서(가칭)」 공동 제작 및 배포

□ 정부는 순간적인 실수로 피해가 발생하고, 피해회복이 어려운 보이스 피싱 범죄의 특성에 따라 「5월 가정의달」을 집중 홍보기간으로 정하고, 신종수법과 대응방안을 적극적으로 홍보하는데 관계 기관과 함께 범정부 차원의 역량을 집중한다.

○ 최근 학생 및 청년층에 대한 피해 증가와 중년층을 겨냥한 ‘자녀 사칭’ 수법의 메신저 피싱도 빈번하게 발생하고 있고

- 이러한 피싱 범죄가 개인적 피해를 넘어 한 가정 전체에 심각한 경제적·정신적 피해를 끼치고 있다는 점에 주목하여 ‘5월 가정의 달’을 맞아 피싱 피해 예방을 위해 집중홍보에 나서게 되었다.

< 취약층 맞춤형 홍보 >

□ 전 연령대 중 20대 이하의 피해가 가장 큰 비중*을 차지하는 만큼 학생·청년층 대상 맞춤형 홍보의 필요성이 높아진 것과 관련하여,


* (20대 이하 피해 비율) '23년 47%, '24년 1~3월 32%로 전 연령대 중 최다 / 경찰청 제공

○ 교육부는 전국 초·중·고등학교에 ‘보이스피싱 예방 교육’ 내용을 포함한 법교과 학습 안내자료를 5월 중 인쇄·보급하고 온라인 플랫폼*에 탑재하여, 학교에서 적극 활용하도록 안내할 예정이다.

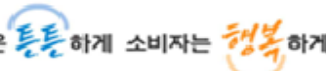
*가 교육정책·정보 제공 온라인 플랫폼인 에듀넷·티-클리어(www.edunet.net) 탑재

출처: 국무조정실 보도 자료(2024.05.01.)

I. 보이스 피싱 현황

 금융감독원

보도자료

금융은 

보도	2024.3.8.(금) 조간	배포	2024.3.7.(목)		
담당부서	금융사기대응단	책임자	팀장	장종현	(02-3145-8140)
	금융사기대응1팀	담당자	선임조사역	김대희	(02-3145-8149)

작년 보이스피싱 피해자 1인당 1,700만원 피해, 전년比 1.5배 ↑
- 2023년 보이스피싱 피해현황 분석 -

※ 본 통계는 '23년 중 「통신사기피해환급법」에 따라 금융감독원에 접수된 보이스피싱 피해구제 신청건을 기준으로 작성되었으며, 수사당국의 범죄사건통계와 차이가 있을 수 있음

주요 내용

□ (피해규모) '23년 보이스피싱 피해액은 1,965억원으로 전년(1,451억원) 보다 514억원(35.4%) 증가

○ 피해자 수는 감소(10.2%↓)하였으나, 1천만원 이상 고액 피해사례가 증가

□ (피해구제) 「통합신고대응센터(☎112)」 개소에 따른 보이스피싱 구제절차 일원화 등으로 신속한 지급정지가 가능해짐에 따라 환급률 개선*(7.1%p↑)

* 피해금액 1,965억원 중 652억원이 피해자에게 환급

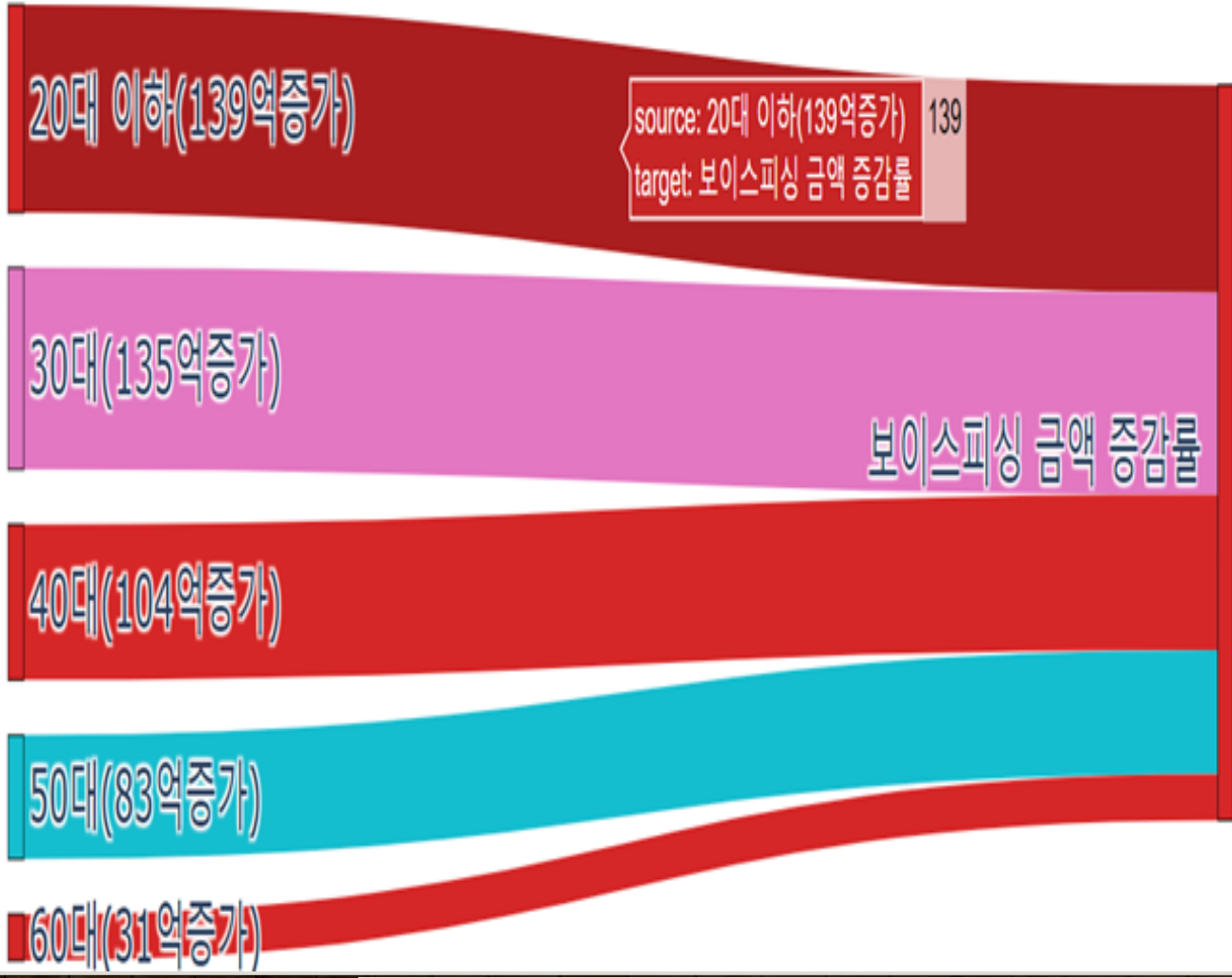
□ (유형별) 주요 사기유형별 비중은 대출빙자형(35.2%) - 가족·지인 사칭형 메신저피싱(33.7%) - 정부기관 사칭형(31.1%) 順*

* 메신저피싱 피해는 크게 감소하였으나, 정부기관 사칭형 및 대출빙자형 피해 증가

□ (연령별) 20대 이하(+139억원) 및 30대(+135억원) 피해 크게 증가

□ (권역별) 사기이용계좌 중 인터넷전문은행 비중은 감소한 반면, 상호금융조합 등 중소서민금융권 비중이 증가하는 등 풍선효과를 보임

연령대별 보이스 피싱에 대한 피해금액 증가율



출처: 금융감독원 보도 자료 (2024.03.08.)

1. 보이스 피싱 현황

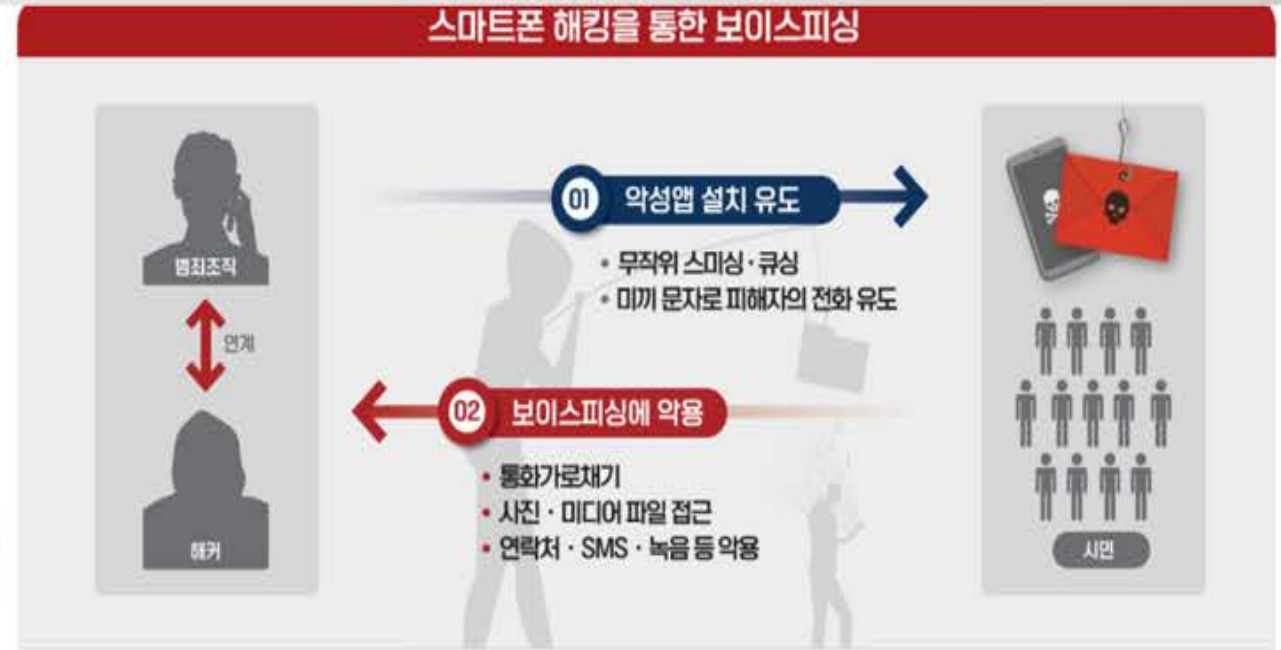




보이스피싱 예방수칙

보이스피싱, "스마트폰 보안" 강화로 막을 수 있습니다.

민생을 파괴하는 보이스피싱 현황



01 악성앱 설치 유도 유형 1 무작위 스미싱·큐싱

스미싱

문자·카톡으로 △택배 △청첩장 △부고 △금융기관 등을 사칭하여 악성앱 설치 유도

큐싱

악성행위가 포함된 QR코드를 이용하여 악성앱 설치를 유도하거나 개인정보를 탈취

부모님께서 소견하셨음을 삼가 알려드립니다. 장례식장 주소 <https://xxxxxxx.com/20Kz>

스미싱

모바일청첩장 결혼식일시 : 4/08(토) 많이와주세요.

<https://xt1ki/1cnh>

스미싱

[배송조회] 9/9 고객주소가 잘못되었습니다. 택배가 반송되었습니다. 배송주소 수정 <http://xxxjy/2Hh9vp9>

스미싱



00은행 특별대출 대상으로 안내. <http://xxxjy/2Hh9vp9>

스미싱



▶ **건당 평균 2.5천만원, 누적 4조원 초과**

▶ **사회초년생(20대) 비율이 예상외로 높음**

1. 보이스 피싱 현황

스미싱(미끼문자)>과태료(쓰레기 무단투기), 택배, 부고장, 청첩장 등 생활밀접 형태 증가

01 악성앱 설치 유도 유형 2 미끼 문자로 피해자의 전화 유도



[해외결제]확인코드:9**8
[KRW 959,000]결제가 완료되었
습니다. 결제 관련 고객센터
070-XXXX-3139

☎ (상담원_보이스피싱 조직)

"조회를 위해 확인코드가 필요합니다."
"확인코드는 보내드린 문자 링크 클릭..
"확인코드는 217.XXX.8.14(IP)로 접속하시면..
"안내대로 앱 설치 하셔야 처리가 가능합니다."



[Web발신](광고)OO은행
고객님 안녕하세요. [정부특례대출]
대상자이나 현재 미접수로..
-신청접수:☎02-XXXX-4247(1번)

☎ (상담원_보이스피싱 조직)

"한도소진 임박...서둘러 신청하셔야..
"비대면 대출을 위해 앱 설치 도와드리겠습니다."



→ 가짜 은행앱 설치 유도

02 보이스피싱에 악용

유형 1
통화가로채기



- 피해자가 금융사 · 수사기관 대표 번호에 확인하는 전화도 가로채 피해자를 안심시킨 후 금전 갈취
- 범죄조직이 직접 모바일 대출실행

유형 2
사진 · 미디어 파일 접근



- 스마트폰에 저장된 은행 보안카드 · 신분증사진 · 금융정보 등을 절취하여 대출실행에 악용

유형 3
연락처 · SMS · 녹음 등 악용



- 지인에게 피해자를 가장하여 피싱 문자 발송
- AI로 목소리를 복제(보이스 클로닝)하여 가족 · 친지에게 금전 요구

▶ 스마트폰 해킹시 이외 다양한 사기 · 협박 등 범죄로 연계 가능

I. 보이스 피싱 현황

사회 공학 기술의 활용(개인정보 활용, 특히 취약계층 타겟)

- 전화나 문자 메시지를 통해 타인을 가장하여 개인정보나 금융정보를 탈취하는 범죄
- 은행, 공공기관, 카드사 등을 사칭하여 피해자의 신뢰를 얻음(금융기관 신뢰 하락 및 사회불안 가중)
- 피해자에게 긴급성을 부여하여 신중하게 생각할 시간을 주지 않음
- 피해자가 정보를 제공하거나 금융거래를 하도록 유도

1천만원 이상 고액 피해자 증가

✓ 1억원 이상 고액 피해의 경우 정부/기관사칭형 사기 수법이 많음 (개인정보, 금융정보를 통한 명의도용 비대면 계좌생성, 휴대폰 개통 등)

보이스피싱은 기술적으로 발전하며, **사회공학적 기술을 활용**

✓ 20대 이하의 경우 기관 사칭, 30~40대 대출 빙자, 50~60대는 가족 및 지인 사칭

I. 보이스 피싱 현황

주요 피해 사례

- 공공기관 사칭하여 국세청, 국민연금관리공단 직원을 사칭하여 과·오납 세금이나 보험금 환급을 가장하여 피해자를 ‘피싱사이트’로 유도하고 주민등록번호, 공인인증서 비밀번호, 계좌번호, 계좌 비밀번호, 이체비밀번호, 카드번호, 카드비밀번호, CVC번호, 카드유효기간, 보안카드 번호 등을 입력하게 한 후 카드로 대출, 인터넷 뱅킹을 이용하여 피해금을 편취하는 수법임
- 이동통신회사 직원을 사칭하여 피해자의 휴대폰으로 전화를 하여 과납한 통신 요금을 설명하고 본인인증을 유도하고 소액 결제 등에 활용
- 가족이 납치 되었다고 협박하여 돈을 긴급하게 송금하도록 하여 편취하는 사례가 딥페이크 기술을 활용하여 확대되고 있음. 미성년 자녀를 납치하였다고 하며 해당 금일 수행평가 등 자녀 개인정보를 제시하며, 자녀의 절박한 목소리 등을 들려주며 지체없이 송금을 요구하는 수법으로 이성적인 판단을 내리기 어려워 피해가 확산되고 있음

I. 보이스 피싱 대응 현황

- 대국민 보이스피싱 예방 교육 및 홍보 활성화(특히 20대 이하 등 취약계층 중점)
- 금융기관 고객 보호 시스템 강화, 피해 최소화 노력(ATM 계좌 이체 시 보이스피싱 안내, 이체한도 제한)
- 전기통신사업자와 협력하여 발신번호 조작 등 기술적 방지 대책 마련

정부기관 사칭·대출빙자형 사기수법 대응 강화

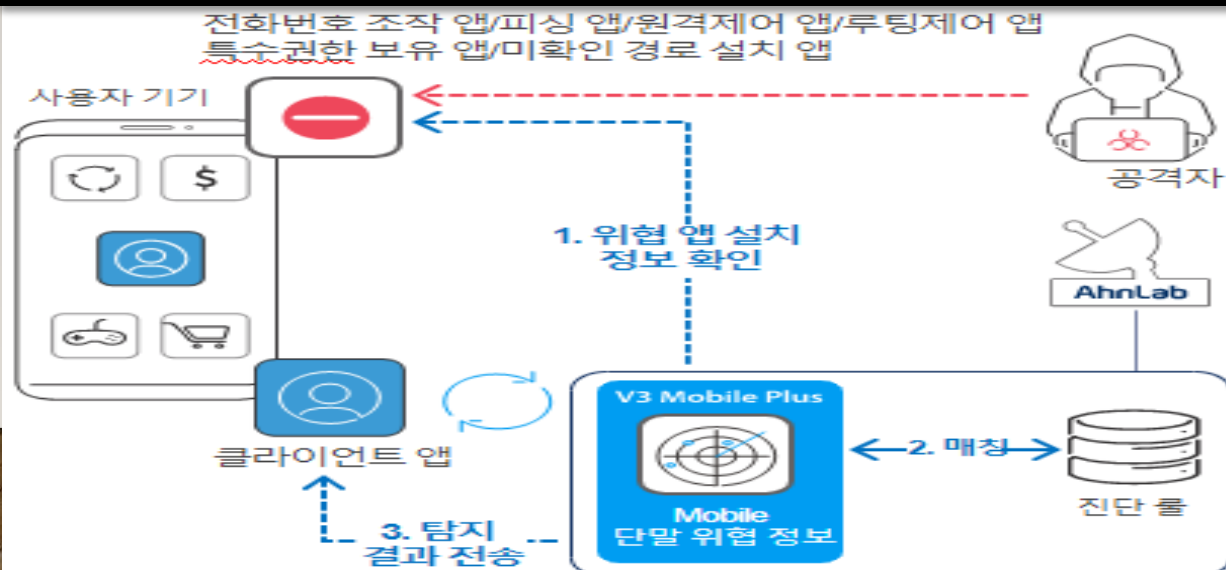
- ✓ 정부기관·금융회사를 사칭한 미끼문자 차단을 위해 관계부처와 협업하여 **안심마크(*) 표기**를 확대 추진
 - * 금융회사가 발송하는 문자에 안심마크를 표기하여 국민들이 안심하고 확인할 수 있도록 하는 서비스로, '24.2월 현재 23개 금융회사가 이용 중

보이스피싱 대응 기술 고도화 추진

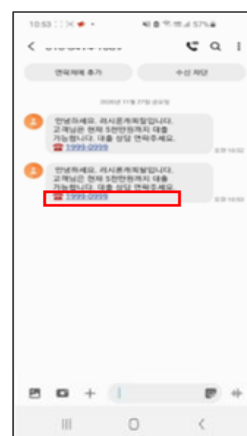
- ✓ 통신사 등 민간기업과 협력하여 AI기반 실시간 보이스피싱 탐지서비스 개발·보급을 추진

대량문자 전송자격인증제 사전 설명회 개최

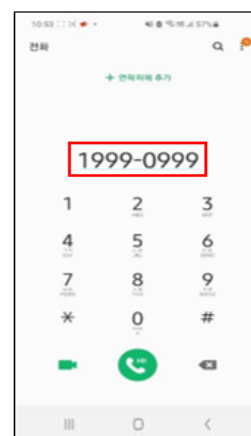
- 방통위 가이드라인에 따라 전송자격인증제 6월부터 본격 시행



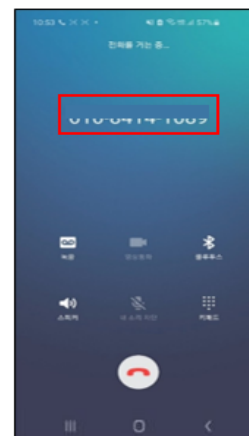
Mobile 단말 위협 정보 (연동형) - 전화 발신조작 탐지



문자 메시지 수신



통화 연결



전화 발신조작



발신조작 탐지 및 알림

3. 보이스 피싱 대응 현황

“보이스피싱, 미리 알고 대비하면 막을 수있어요!”

-정부,「5월 가정의달」보이스피싱 집중 홍보기간 운영-

- ▶ 관계기관 ‘원팀’으로 홍보 분야 협력 강화, 피해 예방에 총력
- ▶ 국민 생활 접점·취약층 맞춤 홍보에 기관 간 상호 지원으로 시너지 제고
- ▶ 「단계별·상황별 대응을 위한 안내서(가칭)」 공동 제작 및 배포

한편, 경찰청, 과기정통부, 금감원 등 관계기관 공동으로 「단계별·상황별 대응을 위한 안내서」를 제작하여 수사·통신·금융 분야에 대한 세부 대응 요령을 알기 쉽게 정리하고,

- 문체부는 카드뉴스·영상·정책기사 형태로 신종수법과 보이스피싱 주요 대책을 설명하는 콘텐츠를 제작하여 정책브리핑, 정부 SNS 채널 등을 활용하여 확산하고,

- 교육부는 전국 초·중·고등학교에 ‘보이스피싱 예방 교육’ 내용을 포함한 법교과 학습 안내자료를 5월 중 인쇄·보급하고 온라인 플랫폼*에 탑재하여, 학교에서 적극 활용하도록 안내할 예정이다.

- 또한, 과기정통부와 한국정보통신진흥협회(KAIT)는 본인 명의를 우회하여 신규로 부정개통하는 보이스피싱 수법을 차단할 수 있는 명의도용방지서비스(M-Safer)*를 통신사 홈페이지 등에 홍보할 계획이다.

* 명의도용 피해 예방을 위해 이용자에게 가입사실 안내서비스, 가입사실 현황조회서비스 및 가입제한서비스 등 제공

- 방통위와 한국인터넷진흥원(KISA)도 미끼문자로 활용되는 불법 스팸문자 사례와 신고방법을 SNS에 게시한다.

□ **민관 협업으로 공익광고 활용 계속**

영화관, 대중교통에서 보이스 피싱 예방 집중 홍보

◆ **공익광고 제작(案)**

- ▶ (나레이션) 하든~피싱! 다음 중 실제 은행 대출 전화는 무엇일까요?
(※ 1~3번은 실제 범인의 목소리로 구성)
1번, “정부지원대출 대상자로 선정되어 연락드렸습니다. 기존에 이용 중인 고금리 상품을 연이자 5%대 저금리 상품으로 대환대출 가능하세요.”
2번, “메신저로 보내드린 대출신청서 파일을 설치해서 작성하시고, 대출금을 받을 체크카드를 택배로 보내주세요.”
3번, “이중으로 대출 신청하셔서 대출약관 위반으로 금융감독원에 고발되었어요. 당장 기존 대출금을 상환하지 않으면 신용불량자가 됩니다.”
▶ (나레이션) 정답은 없습니다. 보이스피싱, 당신이 속지 않은 게 아닙니다. 아직 당신의 차레가 오지 않은 것입니다.

출처: 국무조정실 보도 자료(2024.05.01.)

I. 보이스 피싱 현황

🏠 ▶ 민원·신고 ▶ 보이스피싱지킴이

보이스피싱지킴이

피싱사기 피해, 예방만이 최선입니다.

📄 홈페이지 사용자
매뉴얼 다운로드

📞 보이스피싱
(전기통신금융사기)
제보

☎ 1332
서민금융
1332

📺 보이스피싱
그만

민원·신고

민원·신고 +

불공정 금융관행 신고센터 +

인허가 / 등록 · 신고 +

상속인 금융거래 조회

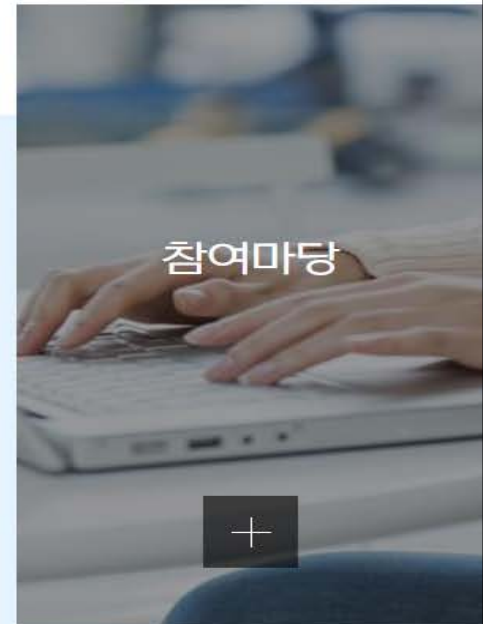
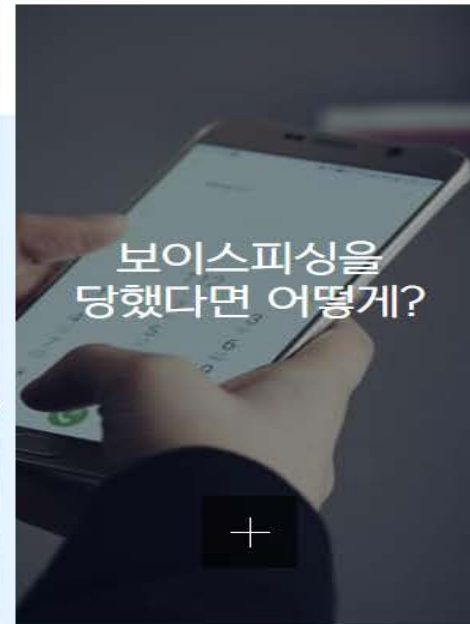
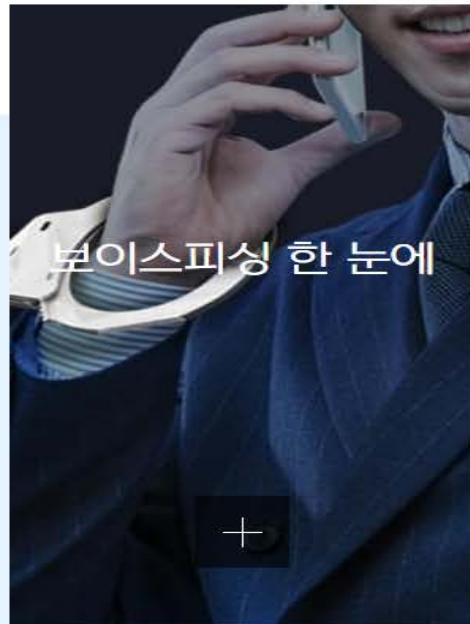
불법금융신고센터 +

보이스피싱지킴이

- 보이스피싱지킴이

- 보이스피싱 한 눈에
- 보이스피싱 사전예방
- 보이스피싱을 당했다면 어떻게?
- 참여마당
- 피해금 환급 등 보이스피싱 관련 조회

옴부즈만 고충민원 +



피싱피해 신고처 안내



보이스피싱 체험관



소비자 경보

1.보이스 피싱 현황

[전국민 보이스피싱 피해예방 캠페인]

안내 사항	수법 분석
<p>[KT안내(예시)] 전국민 보이스피싱 피해예방 캠페인</p> <p>고객님의 피해가 우려되는 ‘무조건 피해야할’ 보이스피싱 전화, 문자, SNS 사례들을 안내 드립니다.</p> <p>다음과 같은 내용의 문자에 대해서는 ① 즉시 진행을 중단하시고, ② 출처를 알 수 없는 링크는 절대 누르지 마시기 바라며, ③ 혹시 ‘링크’를 누르신 경우에는 ‘악성 앱’ 이 개인정보를 탈취하거나, 고객님의 통화를 가로챌 수 있으니 대응요령을 참고하여 조치하시기 바랍니다.</p>	<ul style="list-style-type: none">■ (스미싱 문자 발송) 모바일 청첩장·부고장·범칙금 안내 등 악성앱 설치 링크가 포함된 문자나 카카오톡 발송■ (개인정보 탈취) 범인은 피해자가 위의 링크를 클릭하여 설치된 악성앱을 통해, 피해자의 개인정보를 탈취■ (신규폰 개통) 범인은 탈취한 피해자의 개인정보를 활용, 피해자 명의로 신규 휴대폰 (주로 알뜰폰) 개통■ (금융피해) 범인은 피해자 명의로 개통한 휴대폰을 이용, 예금탈취·대출 실행·카드 발급 등 비대면 금융거래 실행
사례	대응요령
<p>[사례]</p> <ul style="list-style-type: none">■ [청첩장] 모바일 청첩장 결혼식 일시 : 4/08(토) 많이 와주세요 https://123.456.789(예시)■ [부고장] 아버님께서 금일 아침에 별세하셨기에 삼가 알려드립니다. 장례식장주소 https://123.456.789(예시)■ [과태료] 쓰레기 무단투기로 단속되어 과태료 부과되었습니다. https://123.456.789(예시)	<ul style="list-style-type: none">▶ 의심이 되는 문자가 있으면 단말 내 스팸신고를 통해 신고하시거나, 아래 신고처로 연락 바랍니다.☎ 신고처 : 경찰서(☎112), 검찰(☎ 1301), 금융감독원(☎1332), 각 금융사▶ KT에서는 내 번호를 도용하여 문자를 발송할 수 없도록 ‘번호도용문자 차단서비스’를 무료로 제공하고 있습니다. 많은 이용 바랍니다.☎ https://kt.com/v8sw▶ 썬티즌코난 등 모바일 보안앱 설치를 통한 악성앱 검사를 권장합니다.▶ 금융 피해가 의심되면 계좌통합관리서비스(www.accountinfo.or.kr) 및 금융소비자 포털 파인 (fine.fss.or.kr)을 통해 ‘내계좌 지급정지’서비스를 이용할 수 있습니다. 보이스피싱 등 금융사기 피해가 우려되는 경우 신속하게 지급정지를 신청하여, 계좌 잔액 편취 등 금전적 피해를 사전에 방지할 수 있습니다.

출처: KT,SKT,LG+ 스미싱 안내 문자

2. 아동·청소년 개인정보 보호 교육의 필요성



2. 아동·청소년 개인정보 보호 교육의 필요성

피해사례 01

친구가 공짜로 기프트콘 받는 방법을 알려줬어요.
SNS로 휴대폰 번호를 알려주고 인증번호를 보내주면
기프트콘을 바로 보내주더라고요.
아이스크림 기프트콘을 바로바로 보내주니까 몇 번 했었는데
어느 날부터 스팸전화가 오기 시작했어요.



피해사례 02

인터넷 강의 사이트에서 특별회원을 모집한다고 했어요.
가입하면 태블릿 PC를 경품으로 준다고 해서
회원가입을 하면서 전화번호, 메일주소를 입력했는데
그 후로 인터넷 강의 연결은 되지 않고
수능 교재를 판매하는 스팸문자와 메일이 왔어요.



피해사례 03

온라인에서 중고거래 물품을 구매하기 위해 댓글에 연락처를
남겼어요. 문자로 상세 이미지 확인이 가능한 URL이 왔고,
클릭하여 확인해보니 별다른 내용은 없었는데
그 후 핸드폰 소액결제로 사용하지 않은 금액이
결제되었어요.



피해사례 04

시험이 끝나고 친구들과 학교 근처 맛집에 다녀왔어요.
SNS에 전체공개로 친구들과 그 날 찍은 사진과 동영상을
위치, 날짜, 이름 등을 태그해서 올렸는데,
얼마 뒤 누군가 나를 사칭해서
내 사진으로 우리집 근처에서 게임 아이템을 팔겠다고
계시금을 올렸어요.



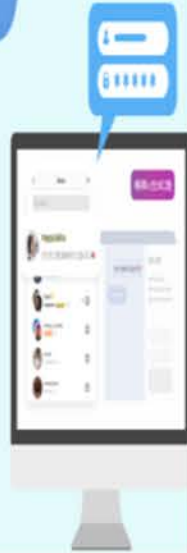
피해사례 05

요즘 개인 유튜브에 브이로그를 올리고 있어요.
촬영하다가 실수로 택배박스 운송장을 가리지 않았었는데
'ㅎ' 스팸 문자와 광고 전화가 자꾸 와서 힘들었어요.



피해사례 06

모르는 사람으로부터 비공개 사이트에
제 신상정보가 돌아다닌다는 DM메시지를 받았어요.
링크를 클릭하니 SNS 로그인 창이 뜨길래
아이디와 비밀번호를 입력했는데 알고 보니 그 사람들이
저의 정보를 알아내기 위해 만든 피싱 사이트였어요.



피해사례 07

인터넷 쇼핑물 모델을 하고싶어서
SNS 게시물에 사진과 함께
#쇼핑물모델 #피팅모델 해시태그를 올렸어요.
얼마 후, 모델을 찾고 있다는 DM이 와서
학교, 이름, 연락처를 보냈는데
몸 사진을 찍어 보내라고 했어요.
이를 거부하면 제 얼굴과 다른 사진을 합성해서
SNS에 올리겠다고 협박했어요.



피해사례 08

게임을 열심히 해서 고레벨을 만들었던 계정을
모르는 사람에게 판매했는데, 그 사람이 저의 게임ID와
그 게임에 연결되어 있는 친구목록에 있는 친구들에게
저를 사칭해서 돈을 빌려 달라고 했어요.



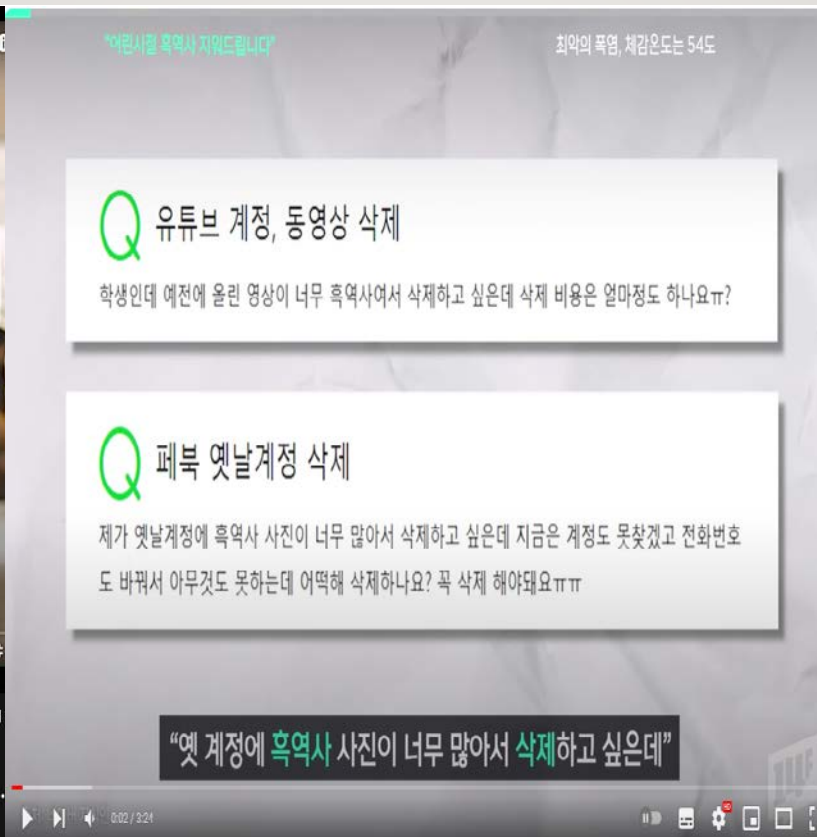
2. 아동·청소년 개인정보 보호 교육의 필요성

디지털 네이티브 세대인 아동·청소년이 자신의 개인정보에 대한 권리를 행사하고 안전하게 보호받을 수 있도록 **희망하는 초·중·고 교육기관에 개인정보위가 위촉한 전문강사를 파견하여 대면교육을 실시함** 현재 보이스 피싱 범죄스미싱, 큐싱(QR코드+피싱) 등으로 교묘해지고 **“20대 이하 피해가 크게 증가”** 하고 있어 **개인정보보호 교육에 대한 필요성이 더욱 부각**되고 있다. 법정 의무교육인 개인정보보호 교육은 아동·청소년기 적시에 이루어져야 하며 전문가를 통한 실효성 있는 교육은 개인정보 범죄 예방에 기여할 수 있다.

출처: 국무조정실 보도 자료(2024.05.01.)

2. 아동·청소년 개인정보 보호 교육의 필요성

개인정보보호 단계별 차등교육(초·중·고) - 모바일 앱의 권한 제공 동의에 대해 스스로 결정하기, 개인정보 유출 시 이를 이용한 악용 사례, 대응방안 및 구제절차 안내



이름	수정한 날짜
24_KISA_정보주체대상교재_글꼴	2024-03-19 오후 2:35
교보재_날말 맞추기	2024-03-19 오후 2:35
[공문]교육협조요청_한국인터넷진흥원(6개교육기관)	2024-03-26 오전 8:43
2024년 개인정보 보호 교육 강사 파견 요청(4.29,청주용암중학교)	2024-04-29 오후 2:07
2024년 개인정보 보호 교육 강사 파견요청(4.2.도담중학교)	2024-04-02 오후 1:17
2024년 개인정보 보호 교육 강사 파견요청(5.28.경산초등학교)	2024-04-29 오후 2:15
개인정보 보호 교육 강사 파견요청(5.31.,화천중학교)	2024-04-12 오후 7:21
개인정보 유출 피해 사례 분석을 통한 중학생 대상 정보보호 교육 콘텐츠 개발	2024-02-24 오전 9:35
개인정보보호 교육 교재_2_초등 저학년	2024-03-19 오후 2:34
개인정보보호 교육 교재_3_초등 고학년	2024-03-19 오후 2:34
개인정보보호 교육 교재_4_중학생	2024-03-19 오후 2:34
개인정보보호 교육 교재_5_고등학생	2024-03-19 오후 2:34
개인정보보호 교육 일정표	2024-04-30 오후 12:49
고학년 동영상	2024-03-19 오후 2:34
아동·청소년 및 힐 권리 지원...내년엔 부모까지 확대	2024-03-19 오후 2:34
어린이를위한개인정보보호_아동+부모 취합_[국문]	2024-03-19 오후 2:34
지우개 서비스_14F	2024-03-19 오후 2:34
탈린그림찾기	2024-03-19 오후 2:34

출처 : 개인정보보호위원회 제공 전문강사 강의 교안 발체

2. 아동·청소년 개인정보 보호 교육의 필요성

개인정보 보호 기본계획

2024-2026

개인정보보호위원회
Personal Information Protection Commission

전략2. 개인정보 안심사회 구현

26

과제4 | 정보주체를 보다 두텁게 보호하겠습니다.

27

- ① 정보주체 권리 실질화 27
- ② 개인정보 보호 사각지대 해소 29

과제5 | 공공부문 보호수준을 더욱 튼튼히 하겠습니다.

30

- ① 공공의 개인정보 보호수준 강화 30
- ② 디지털플랫폼정부 신뢰성 제고 지원 32

과제6 | 기업의 자율적인 보호활동을 적극 지원하겠습니다.

33

- ① 민관협력 문제해결형 자율규제 활성화 33
- ② 기업 개인정보 보호역량 제고 34

과제7 | 법과 제도를 엄정하고 신속하게 집행·운영하겠습니다.

36

- ① 신속한 개인정보 침해 대응 36
- ② 법 집행력 강화 37

전략3. 글로벌 데이터 신(新)질서 주도

38

과제8 | 신뢰할 수 있는 개인정보 국외 이전 환경을 만들겠습니다.

39

- ① 개인정보 국외 이전 법제의 상호운용성 강화 39
- ② 안전한 국외 이전 환경 조성 39

과제9 | 디지털 대전환에 따른 개인정보 패러다임 전환을 선도하겠습니다.

40

- ① 합리적 개인정보 규제 개선 40
- ② 변화하는 글로벌 사회에 발맞춘 개인정보 이슈 선제적 대응 42

과제10 | 개인정보 분야 글로벌 리더십을 확보해나가겠습니다.

43

- ① 글로벌 협력 강화 43
- ② 국제 컴플라이언스 역량 제고 44

과제별 소관기관 및 추진일정

46

용어 설명

48

과제별 주요내용 및 추진방향

49

제3절 개인정보보호 환경 조성

1. 개인정보보호 교육 강화

2020년 8월 개인정보보호위원회가 중앙행정기관으로 출범한 것을 계기로 행정안전부와 방송통신위원회가 개별적으로 운영하던 개인정보처리자와 정보주체 대상 개인정보보호 교육을 재정비하여 그 효과성을 제고하였다.

개인정보보호 교육은 교육 대상을 개인정보처리자와 정보주체로 구분하고, 현장·방문교육과 온라인 교육으로 나누어 실시하였다.

또한, 자율적인 개인정보보호 교육 문화 확산 및 수도권과 지방에도 균등한 교육 기회 제공을 위해 개인정보에 대한 전문지식을 갖춘 전문가 160명을 개인정보보호 전문강사 2기로 선발·위촉하였다. 선발된 전문강사 명단은 '개인정보 포털(www.privacy.go.kr)'에 공개하여 공공·민간에서 상황에 맞는 자율적인 개인정보보호 교육이 이루어질 수 있도록 하였다.

2022년에는 대상별 맞춤형 개인정보보호 교육과정 운영을 통해 개인정보처리자 및 정보주체 대상 온라인 교육으로 총 1,004,912명, 그리고 오프라인 교육으로 총 48,607명이 이수하였다.

[표 2-6-5] 2022년 개인정보처리자 및 정보주체 개인정보보호 교육 현황 (단위: 명)

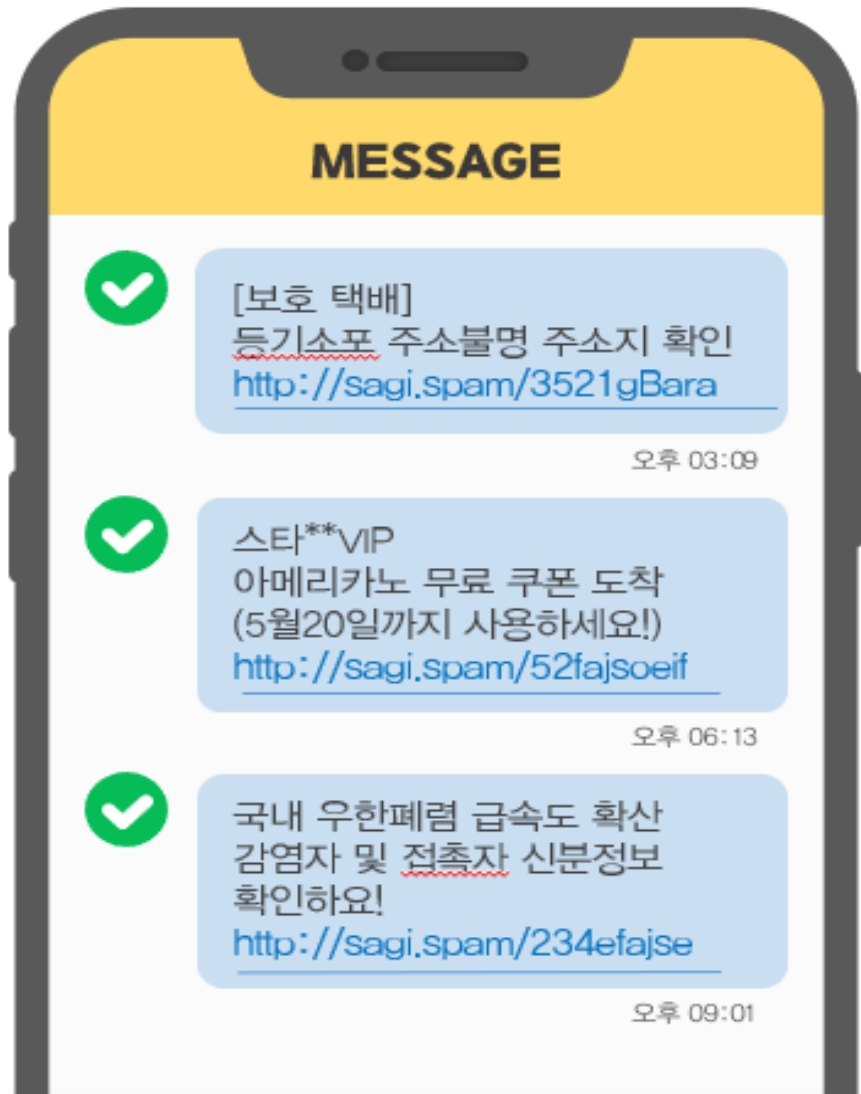
구분	온라인 교육인원	현장 교육인원	전문강사 활용 교육인원 ⁴⁰⁾	합계
개인정보처리자	880,685	11,074	142,415	1,034,174
정보주체	124,227	37,533	-	161,760
합계	1,004,912	48,607	142,415	1,195,934

공공·민간분야의 개인정보취급자·개인정보보호 업무담당자·책임자 등 개인정보처리자를 대상으로 라이브 형태의 비대면 온라인교육 및 현장교육을 병행하여 진행하였고, 수준별 교육과 특화교육을 중심으로 추진하였다.

수준별 교육은 초급·중급·고급 과정으로 구분하여 「개인정보 보호법」 등 기본적인 법·제도 사항에서부터 개인정보보호 안전성 확보조치, 유·노출 예방과 개인정보 보호책임자(CPO)의 책무까지 개인정보보호 관련 핵심 내용을 수강생의 수준에 따라 학습할 수 있도록 설계하였다.

출처 1. 개인정보보호위원회 개인정보 보호 기본계획
출처 2. 개인정보보호위원회 2023년 연차보고서(265p)

2. 아동·청소년 개인정보 보호 교육의 필요성



- ✓ 출처가 불분명한 인터넷 주소(URL)나 파일은 클릭 금지!
- ✓ 정식 앱 스토어가 아닌 인터넷 주소(URL)에서 출처가 불분명한 앱 다운로드 설치 자제!



2. 아동·청소년 개인정보 보호 교육의 필요성

1 앱을 설치할 때



필수적
접근권한

ex. 음악 스트리밍 앱 설치 시

저장권한

음반 이미지, 곡 재생파일 임시저장

전화권한

재생 중 전화 상태 체크,
휴대폰번호로 로그인

SNS권한

수신한 SMS 인증번호 자동입력

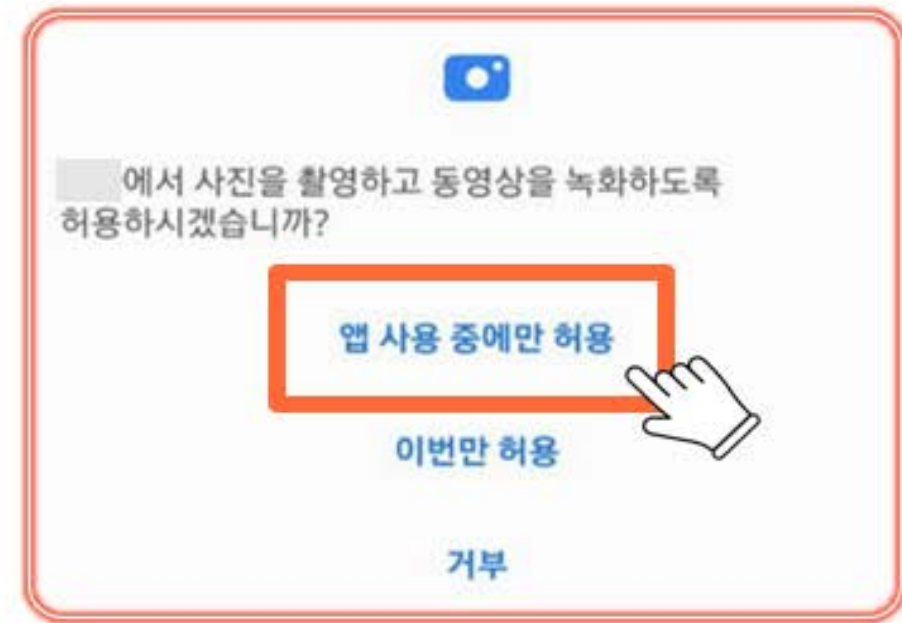
선택적
접근권한

위치권한

위치기반 상품 추천 서비스 제공

2. 아동·청소년 개인정보 보호 교육의 필요성

2 앱을 실행할 때



2. 아동·청소년 개인정보 보호 교육의 필요성

3 설치된 앱의 권한 점검하기

안드로이드

설정 - 앱 선택

해당 앱 선택

권한 선택

접근권한 확인하기

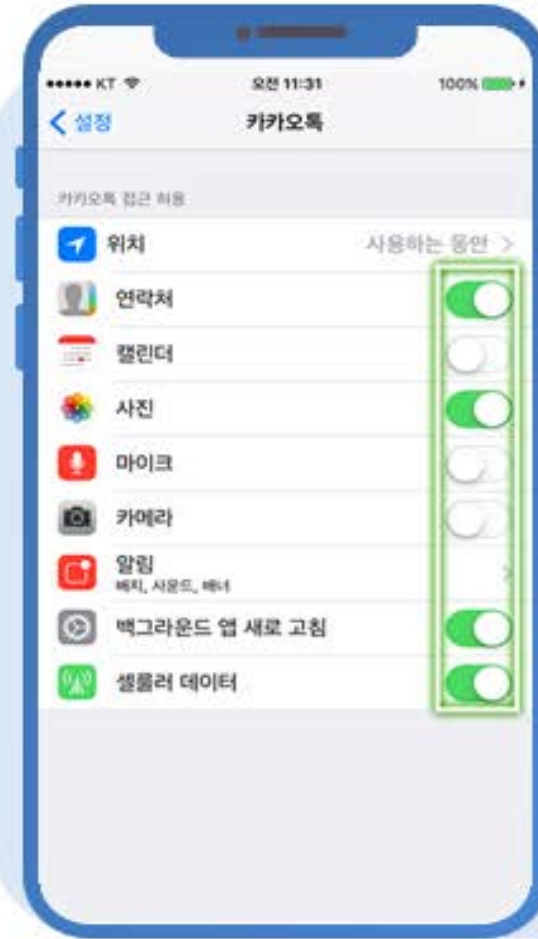


아이폰

설정 선택

해당 앱 선택

접근권한 확인하기



2. 아동·청소년 개인정보 보호 교육의 필요성

03 SNS나 메신저에서 개인정보 노출 금지!

- ✓ 사진이나 글을 업로드할 때,
 - 이름, 장소, 휴대폰번호 등이 포함되어 있는지 확인하세요
 - 범죄에 이용될 수 있는 해시태그(#)를 주의하세요
 - 게시물 전체 공개 게시물은 더욱 주의가 필요해요
 - SNS 친구 수락할 때 주의가 필요해요
 - 관심사 오픈채팅에서 모르는 사람과 대화할 때 개인정보 노출 주의
 - 게임에서 만난 사람과 메신저에서 대화할 때 개인정보 노출 주의



08 내가 작성했던 게시물 삭제 요청하기

- ✓ 사이트에서 이미 탈퇴해버려서
과거에 인터넷에 올렸던 글들을 지우지 못하고 있다면
게시판 관리자에게 게시물 삭제를 요청하세요.

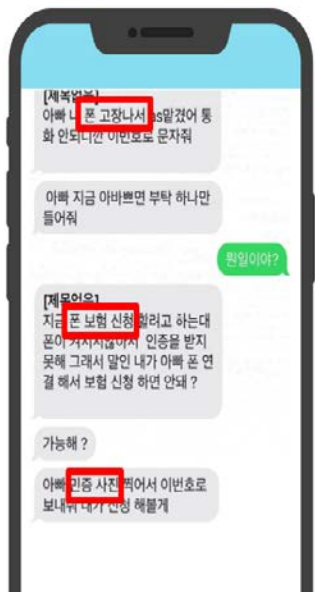


2. 아동·청소년 개인정보 보호 교육의 필요성

[신규 강의 교안 개발 : *제로트러스트 보안 패러다임을 교육 콘텐츠 인식 제고에 반영]

1. 맞춤형 이해하기 쉬운 영상 제작(보이스 피싱 사례)
2. 보이스 피싱 사례 및 대응 참여형 과정 도입(질문 후 답변)
3. 강의 교안 자료에 “스미싱 문자” 또는 “메일” 등을 통한 체험 프로그램

수준별 이해하기 쉬운 강의교안-1



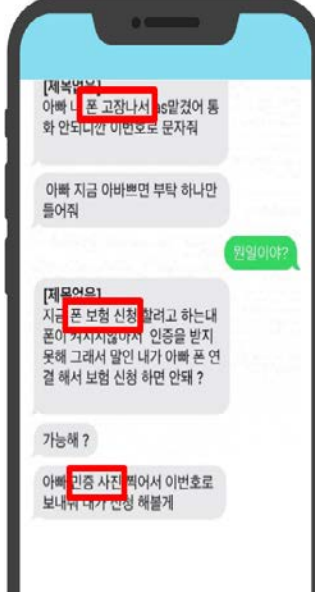
모르는 사람이 나를 사칭해서
우리 부모님한테 문자메시지를 보냈고,
부모님의 주민등록증을 요구해서
범죄를 저지르려고 해요.

질문 1

나의 어떤 정보가 유출되면
이런 범죄가 가능해질까요?



수준별 이해하기 쉬운 강의교안-2



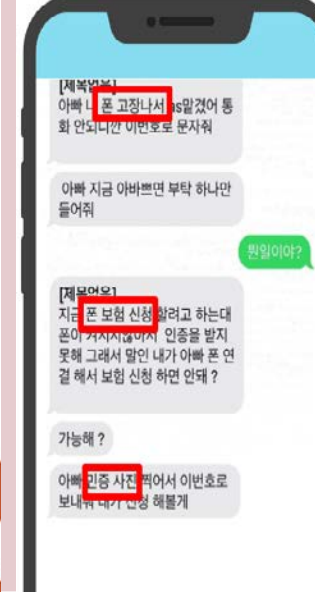
모르는 사람이 나를 사칭해서
우리 부모님한테 문자메시지를 보냈고,
부모님의 주민등록증을 요구해서
범죄를 저지르려고 해요.

질문 2

부모님의 주민등록증이 유출되면
부모님은 어떤 피해를 입게 될까요?



수준별 이해하기 쉬운 강의교안-3



모르는 사람이 나를 사칭해서
우리 부모님한테 문자메시지를 보냈고,
부모님의 주민등록증을 요구해서
범죄를 저지르려고 해요.

질문 3

부모님이 문자메시지 보낸 사람을
의심할 때 범죄자는 어떻게
부모님을 믿게 하려고 할까요?

정보초등학교 4학년 2반 8번 400
정보초등학교 5학년 1반 2번 300
정보초등학교 6학년 3반 9번 500



출처 : 개인정보보호위원회 제공 전문강사 강의 교안 발췌

* 제로트러스트 보안원리 “Never Trust, Always Verify”



3. 보이스 피싱 사례 및 시사점

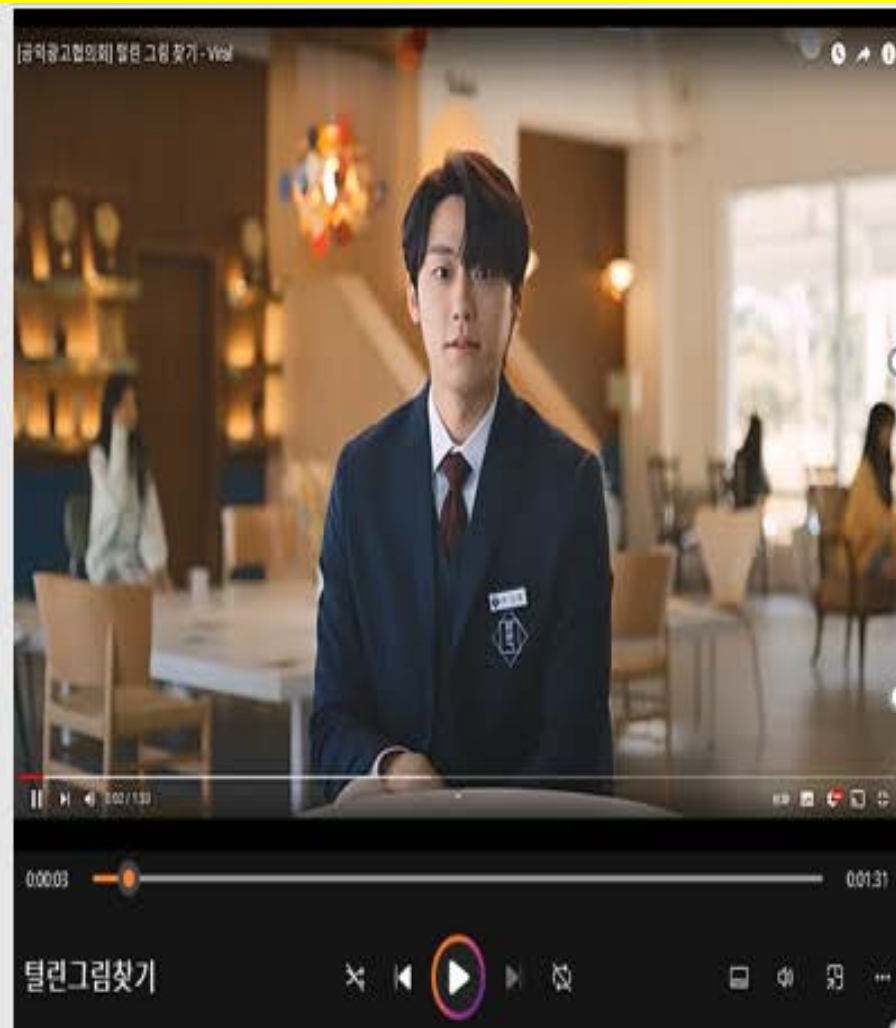
게임 콘텐츠 이용료 명목으로 30분 동안 100만원이 결제된 A씨. 게임회사로부터 소액이 수차례 결제돼 50만원에 이르는 금액이 승인됐다는 문자를 받은 B씨 등 구글계정을 해킹 당해 사용하지 않는 게임 콘텐츠 이용료가 결제됨(출처:조선비즈)



보이스피싱 통합대응센터		2024년 01월 12일[금] 오전 11:07:25	
발생유형 TOP 5		답변유형 TOP 5	
스미싱	111	스미싱 대처 방법	118
단순상담	91	개인정보 유출 대응방법	50
전화금융사기	66	피싱 여부 확인	48
미끼문자	37	보이스피싱 제보방법	25
인터넷 사기	2	대응기관별 역할	6
기타	5	기타	65
합계	312	합계	312

3. 보이스 피싱 사례 및 시사점

피싱 사례에 대한 수준별 교육 콘텐츠를 제작하여 효과적인 교육에 활용함
교육 콘텐츠 제작 : 영상 콘텐츠(1~2분), 해당 사례 모의테스트, 설문참여
(보이스피싱 유형: 1. 보이스피싱, 2. 스미싱, 3. 큐싱, 4. 스피어 피싱, 5. 사이버 성폭력 등)



3. 보이스 피싱 사례 및 시사점

보이스피싱

피해사례 1.



가족, 지인 사칭



타인의 메시지를 해킹하거나 모르는 번호로 가족, 지인을 사칭하여 신분증 또는 신용카드 번호 등 개인정보 요구 후 자금을 편취하는 수법

보이스피싱

피해사례 2.



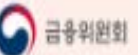
정부, 금융기관 사칭



정부 및 금융기관에서 보내는 공지사항 (지원금 신청, 간편대출신청, 정보유출 피해확인 등)인 것처럼 문자를 발송하여 피싱사이트로 유도 및 개인정보를 입력하게 하고 예금 등을 편취하는 수법

보이스피싱

피해사례 3.



원격제어 앱 설치 유도



결제 허위문자 발송 후 수사기관을 사칭하여 개인정보 유출을 빌미로 원격제어 앱을 설치하도록 유도, 계좌에 직접 접근하여 금전을 탈취하는 수법

3. 보이스 피싱 사례 및 시사점

다양한 방법으로 대상자를 속이는 스미싱 공격 발생

공공기관 사칭

[WEB발신]
대검찰청입니다.
귀하의 사건이 접수되어 아래 URL 로
접속하여 주시기 바랍니다.
www.xxxxxxxx.com

수사기관 사칭

[WEB발신]
서울 xx 경찰서입니다.
아래 김xx님의 사건이 접수되어
상세 내역 확인 바랍니다.
www.xxxxxxxx.com

택배회사 사칭

[WEB발신]
대한통운 택배 알림 입니다.
상품의 위치를 확인하려면 아래 URL 로
접속하시기 바랍니다.
www.xxxxxxxx.com

카드사 사칭

[WEB발신]
[XX CARD 사용내역]
Xxxxxx 에서 150,000원.
상세내역 확인
www.xxxxxxxx.com

금융기관 사칭

[WEB발신]
국세 환급금이 발생하였습니다.
환급 받기 위해 아래 URL 로 접속하여
환급 계좌를 입력하여 주시기 바랍니다.
www.xxxxxxxx.com

카드사 사칭

[WEB발신]
xx 카드가 발급 되었습니다.
발급 진행 상황을 조회 하세요.
www.xxxxxxxx.com



3. 보이스 피싱 사례 및 시사점

범정부 보이스 피싱 TF를 통한 금융권 등 규제기관 및 사법기관이 많은 노력을 기울이고 있으나 선량한 시민들을 대상으로 한 무차별 공격은 더욱 확산되고 있다. 그 원인으로 지속해서 발생했던 대규모 개인정보 유출 사고가 근본적인 원인으로 판단되며, 아동·청소년의 중요한 시기에 안전한 개인정보 보호 및 활용 방안에 대한 교육이 부재했던 바에 기인한다. 현재 개인정보보호위원회는 개인정보보호 교육의 공공성에 부합하여 최대 피해자인 디지털 네이티브 세대를 위해 **“아동·청소년 개인정보 보호 정책을 중점사업으로 추진”** 하고 있으며, 그 일환으로 개인정보보호 전문가를 통한 신청 학교에 찾아가는 개인정보보호 교육을 실시하고 있다. 향후 보이스 피싱 예방에 가장 효과적인 예방대책으로 기여할 것이다. 지속적으로 **“보이스 피싱 최신 사례 및 효과적인 영상 콘텐츠 등을 개발”**하여 개인정보보호 교안으로 지속 보급되었으면 한다.

보호할 수 없다면, 증명할 수 없습니다.
(Never Trust, Always Verify)

감사합니다