2022년 청년 소비자
역량 제고 및 디지털 디바이드 해소사업

- 보이스피싱 예방 및 경찰청 사이버 캅 앱설치
  응급의료 정보제공 앱설치 및 활용
- 소비자24 앱 설치 및 활용방법 피해구제 방법

일 시 **2022년 12월 6일 ~ 9일**

장 소 **대구YMCA 청소년회관**
지하1층 / 1층 / 2층 / 4층 / 6층 / 703호 / 707호 / 10층

주관 : **대구경북미래소비자행동 · 대구YMCA**

주최 : **공정거래위원회 · 한국소비자단체협의회 · (사)한국소비자교육정책학회**

청년소비자 역량제고 및 디지털 디바이드 해소사업 (대구지역)

1. 사업개요

□ **일　　시** : 2022년 12월 6일(화) ~ 12월 9일(금) (4일간)

□ **장　　소** : 대구YMCA 청소년회관, 교남YMCA 강당

□ **주　　관** : 미래소비자행동 대구경북지부, 대구YMCA

□ **주　　최** : 공정거래위원회·한국소비자단체협의회
(사)한국소비자교육정책학회

□ **협력기관** : 대구경찰청

2. 교육세부일정

일시	팀별	강의시간	장소
12월 6일 (화)	1팀	14:00~14:45	대구YMCA 청소년회관 지하1층 청청놀이터
		15:00~15:45	
	2팀	14:00~14:45	대구YMCA 청소년회관 1층 다목적홀
		15:00~15:45	
	3팀	14:00~14:45	대구YMCA 청소년회관 2층 커뮤니티홀
		15:00~15:45	
	4팀	14:00~14:45	대구YMCA 청소년회관 4층 대강당
		15:00~15:45	
	5팀	14:00~14:45	대구YMCA 청소년회관 6층 교육장
		15:00~15:45	
	6팀	14:00~14:45	대구YMCA 청소년회관 7층 (703호)
		15:00~15:45	

일시	팀별	강의시간	장소
12월 7일 (수)	7팀	14:00~14:45	대구YMCA 청소년회관 7층 (707호)
		15:00~15:45	
	8팀	14:00~14:45	대구YMCA 청소년회관 10층 도서관실
		15:00~15:45	
	1팀	14:00~14:45	대구YMCA 청소년회관 지하1층 청청놀이터
		15:00~15:45	
	2팀	14:00~14:45	대구YMCA 청소년회관 1층 다목적홀
		15:00~15:45	
	3팀	14:00~14:45	대구YMCA 청소년회관 2층 커뮤니티홀
		15:00~15:45	
	4팀	14:00~14:45	대구YMCA 청소년회관 4층 대강당
		15:00~15:45	
	5팀	14:00~14:45	대구YMCA 청소년회관 6층 교육장
		15:00~15:45	
	6팀	14:00~14:45	대구YMCA 청소년회관 7층 (703호)
		15:00~15:45	
	7팀	14:00~14:45	대구YMCA 청소년회관 7층 (707호)
		15:00~15:45	
	8팀	14:00~14:45	대구YMCA 청소년회관 10층 도서관실
		15:00~15:45	
12월 8일 (목)	1팀	14:00~14:45	대구YMCA 청소년회관 지하1층 청청놀이터
		15:00~15:45	
	2팀	14:00~14:45	대구YMCA 청소년회관 1층 다목적홀
		15:00~15:45	
	3팀	14:00~14:45	대구YMCA 청소년회관 2층 커뮤니티홀
		15:00~15:45	
	4팀	14:00~14:45	대구YMCA 청소년회관 4층 대강당
		15:00~15:45	
	5팀	14:00~14:45	대구YMCA 청소년회관 6층 교육장
		15:00~15:45	
	6팀	14:00~14:45	대구YMCA 청소년회관 7층 (703호)
		15:00~15:45	
	7팀	14:00~14:45	대구YMCA 청소년회관 7층 (707호)
		15:00~15:45	
	8팀	14:00~14:45	대구YMCA 청소년회관 10층 도서관실
		15:00~15:45	

일시	팀별	강의시간	장소
12월 9일 (금)	1팀	14:00~14:45	대구YMCA 청소년회관 지하1층 청청놀이터
		15:00~15:45	
	2팀	14:00~14:45	대구YMCA 청소년회관 1층 다목적홀
		15:00~15:45	
	3팀	14:00~14:45	대구YMCA 청소년회관 2층 커뮤니티홀
		15:00~15:45	
	4팀	14:00~14:45	대구YMCA 청소년회관 4층 대강당
		15:00~15:45	
	5팀	14:00~14:45	대구YMCA 청소년회관 6층 교육장
		15:00~15:45	
	6팀	14:00~14:45	대구YMCA 청소년회관 7층 (703호)
		15:00~15:45	
	7팀	14:00~14:45	대구YMCA 청소년회관 7층 (707호)
		15:00~15:45	
	8팀	14:00~14:45	대구YMCA 청소년회관 10층 도서관실
		15:00~15:45	

3. 세부교육주제

□ **1강** : 보이스피싱 예방 및 경찰청사이버 캅 앱설치
응급의료 정보 제공 앱설치 및 활용

□ **2강** : 소비자24 앱 설치 및 활용방법 피해구제 방법

목 차·CONTENTS

주제강의
01

보이스피싱 예방 및 경찰청사이버 캅 앱설치 응급의료 정보 제공 앱설치 및 활용

02 디지털 취약계층 대상 디지털 기기 사용 방법(휴대폰, 키오스크 등)

1. 보이스 피싱 피해예방 관련 (경찰청 사이버캅 앱 설치)
2. 의료정보제공 관련 (응급의료정보 제공 앱 설치)
3. 키오스크 사용법 (ex. 무인티켓발급기 등) : 참고영상 첨부

01

경찰청 사이버캠 설치 활용하기

02 디지털 취약계층 대상 디지털 기기 사용 방법(경찰청 사이버캅 앱 설치)

02 디지털 취약계층 대상 디지털 기기 사용 방법(경찰청 사이버캅 앱 설치)

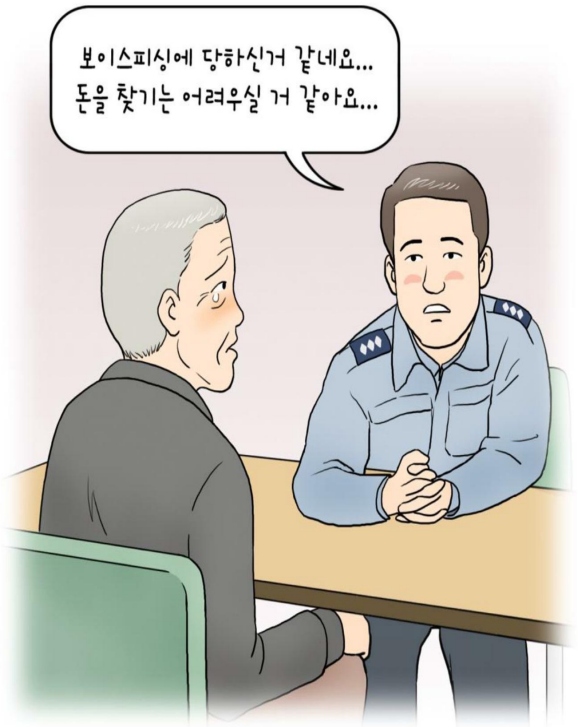
금융사기(보이스피싱, 스미싱) - 날로 진화하는 보이스피싱 사기

Ⅰ 경찰서, 검찰, 금융감독원, 은행 등을 사칭하며 여럿이 팀을 짜서 전화하는 수법도 등장

Ⅱ 은행 직원도 믿지 말고 자신의 말만 따르라고 지시 ATM기로 유도해 돈을 계좌이체 하도록 유도

Ⅲ 실제 전화번호가 찍히게 하거나 가짜로 은행이나 정부기관 홈페이지를 만들어 직접 계좌번호, 비밀번호를 입력하도록 유도

Ⅳ 울면서 횡설수설하는 어린아이 목소리를 들려주고 자녀가 다쳤다고 혹은 자녀를 납치했다며 돈을 요구하는 수법 등장

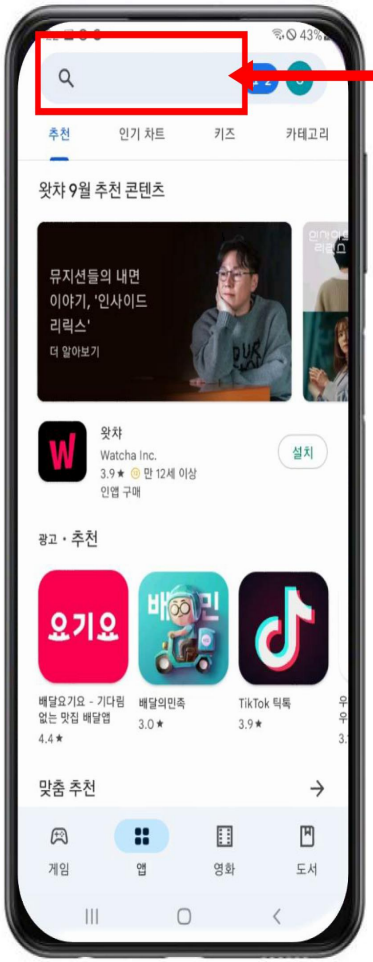


02 디지털 취약계층 대상 디지털 기기 사용 방법(경찰청 사이버캅 앱 설치)

1

02 디지털 취약계층 대상 디지털 기기 사용 방법(경찰청 사이버캅 앱 설치)

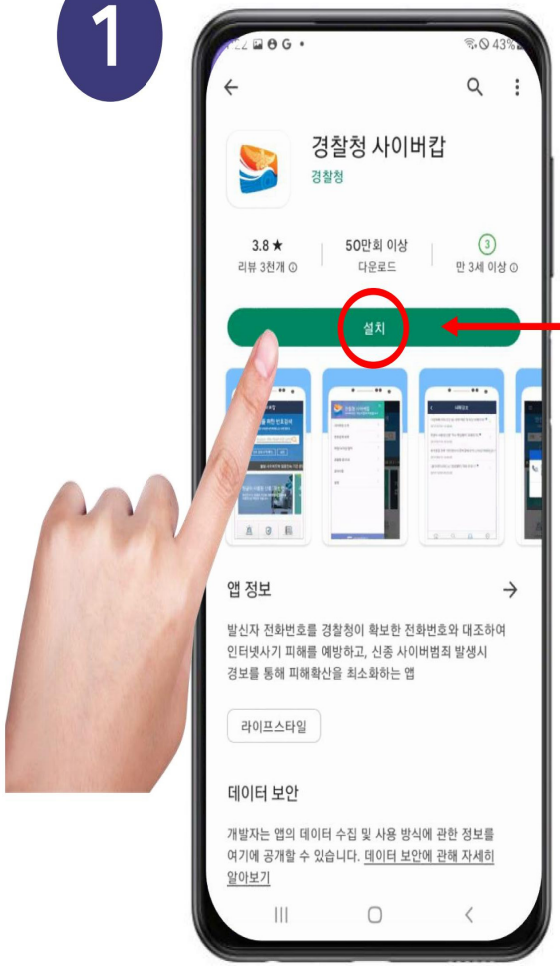
1



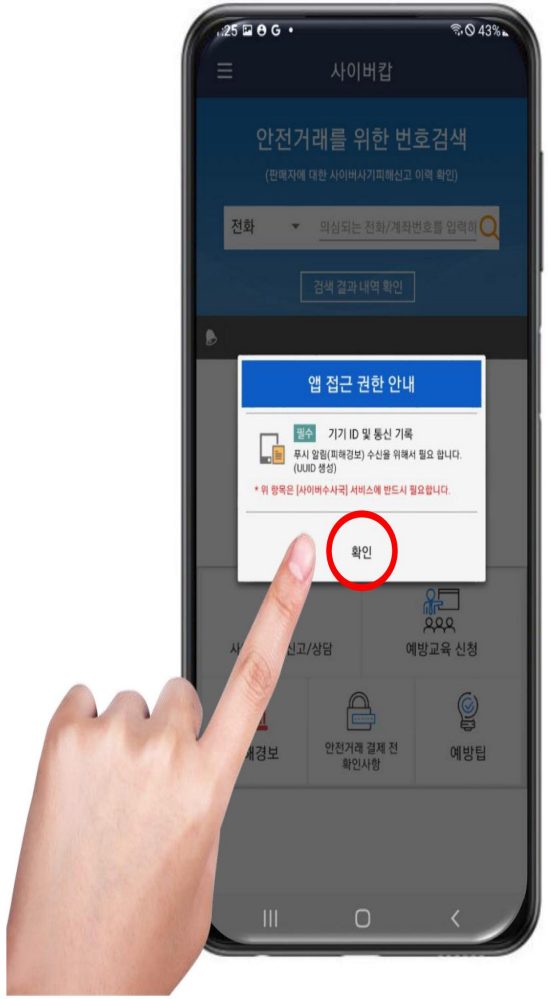
검색창에서
'경찰청 사이버캅'
입력

02 디지털 취약계층 대상 디지털 기기 사용 방법(경찰청 사이버캅 앱 설치)

1



'설치' 누르기



02 디지털 취약계층 대상 디지털 기기 사용 방법(경찰청 사이버캅 앱 설치)

1

'안전거래를 위한 번호검색'

피해가 의심되는

전화번호,
계좌,
이메일을

검색하세요

02 디지털 취약계층 대상 디지털 기기 사용 방법(경찰청 사이버캅 앱 설치)

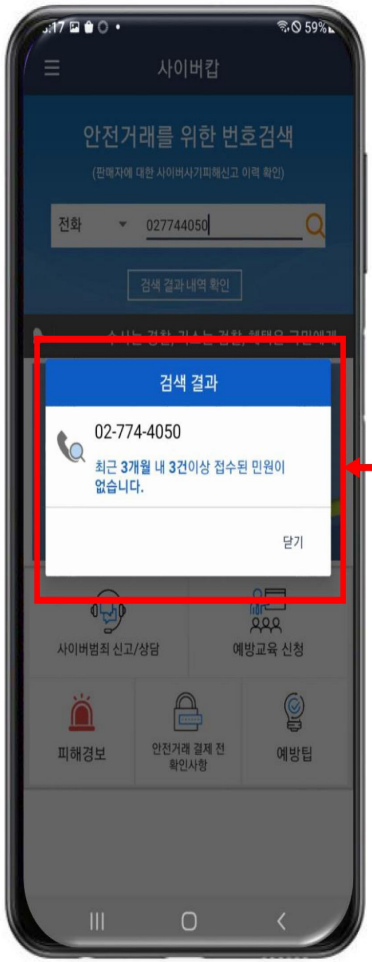
1

'안전거래를 위한 번호검색'

피해가 의심되는

전화번호, 계좌, 이메일을

검색하세요



안전한 전화번호 입니다

01

금융교육 정보제공 플랫폼 활용하기

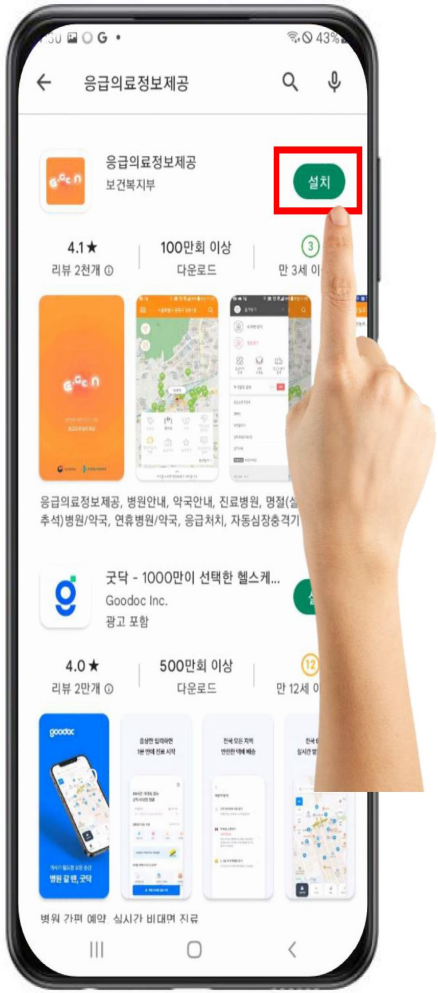
02 디지털 취약계층 대상 디지털 기기 사용 방법(응급의료정보제공 앱 설치)

2

02 디지털 취약계층 대상 디지털 기기 사용 방법(응급의료정보제공 앱 설치)

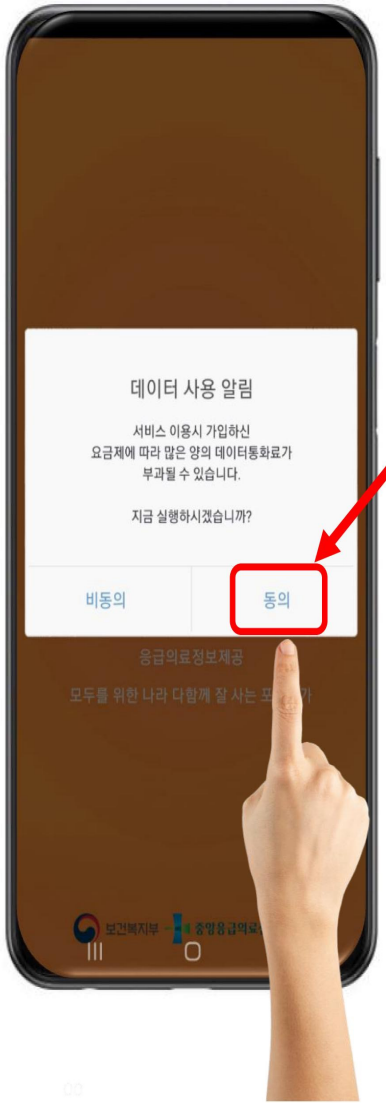
2

'응급의료정보제공'
검색

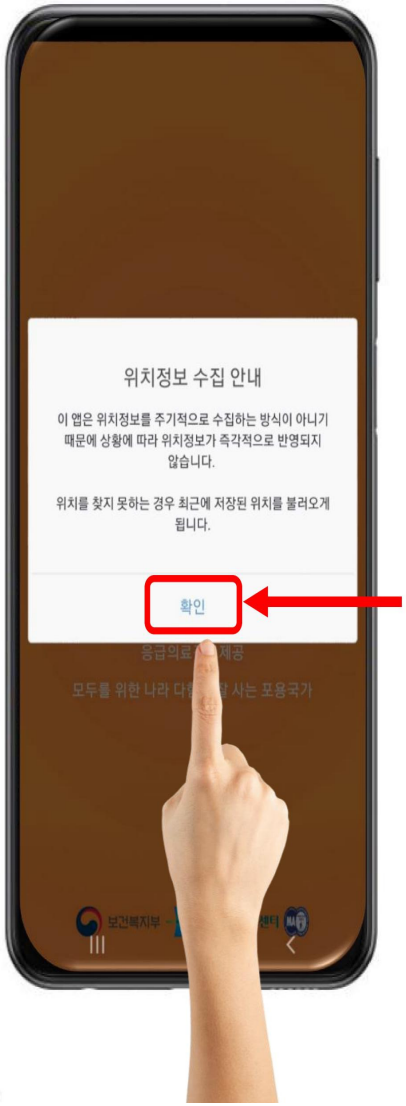


02 디지털 취약계층 대상 디지털 기기 사용 방법(응급의료정보제공 앱 설치)

2



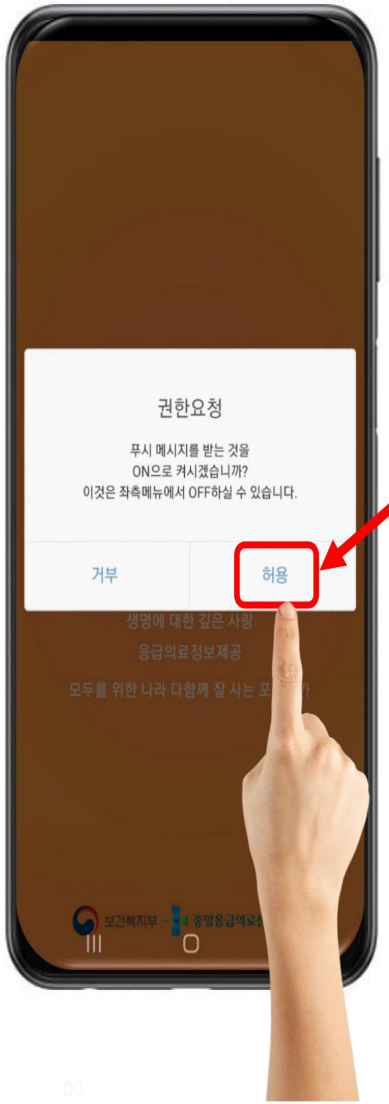
데이터 사용 알림
'동의'
누르기
: 어르신들께
꼭!!
필요하다고
설명드려야 합니다.



위치정보
수집 안내
'확인'
누르기
: 사용자의 위치를
확인합니다.

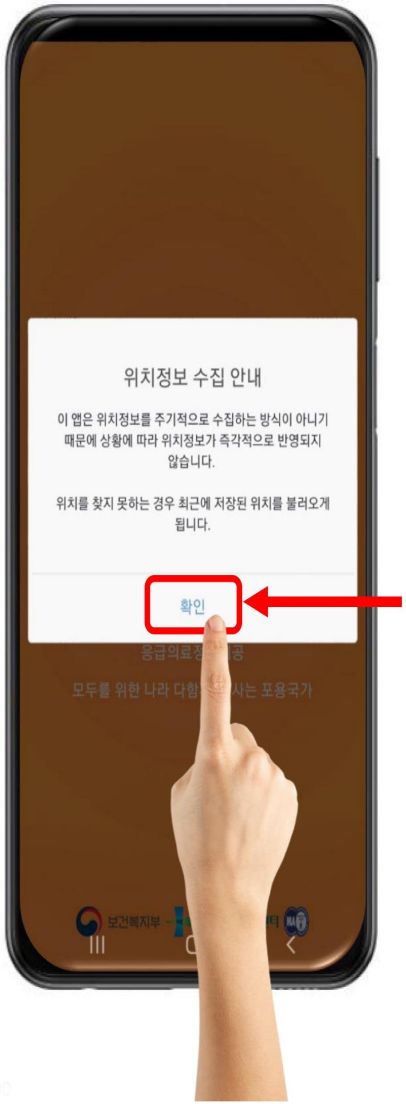
02 디지털 취약계층 대상 디지털 기기 사용 방법(응급의료정보제공 앱 설치)

2



권한요청
'허용'
선택

: 선택사항이지만,
푸시 메세지를 받는 것
이 좋다고
설명 드립니다.

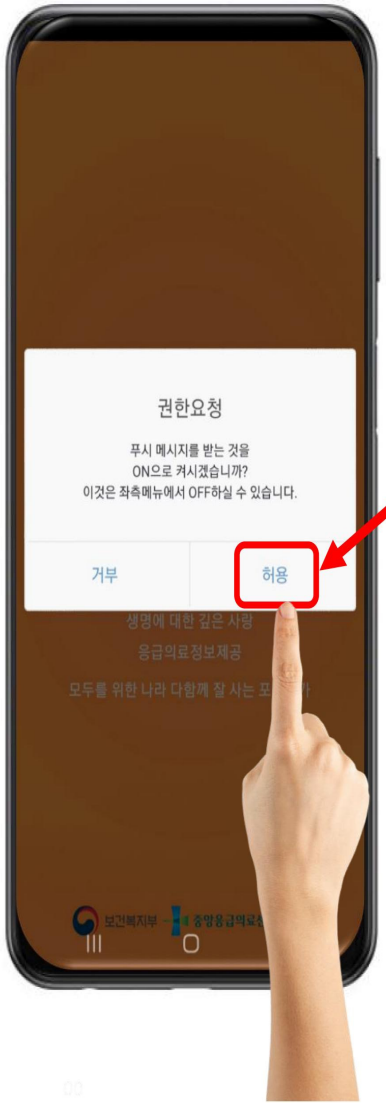


위치정보
수집 안내
'동의'
누르기

: 사용자의 위치를
확인합니다.

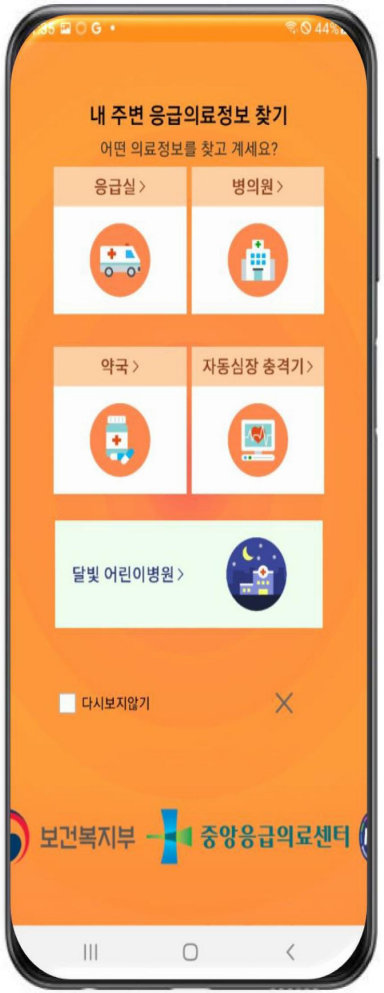
02 디지털 취약계층 대상 디지털 기기 사용 방법(응급의료정보제공 앱 설치)

2



권한요청
'허용'
선택

: 선택사항이지만,
푸시 메세지를 받는 것
이 좋다고
설명 드립니다.



응급의료
정보제공 앱
설치 끝!!

: 정보를 검색합니다.

08

활용사 트렌디

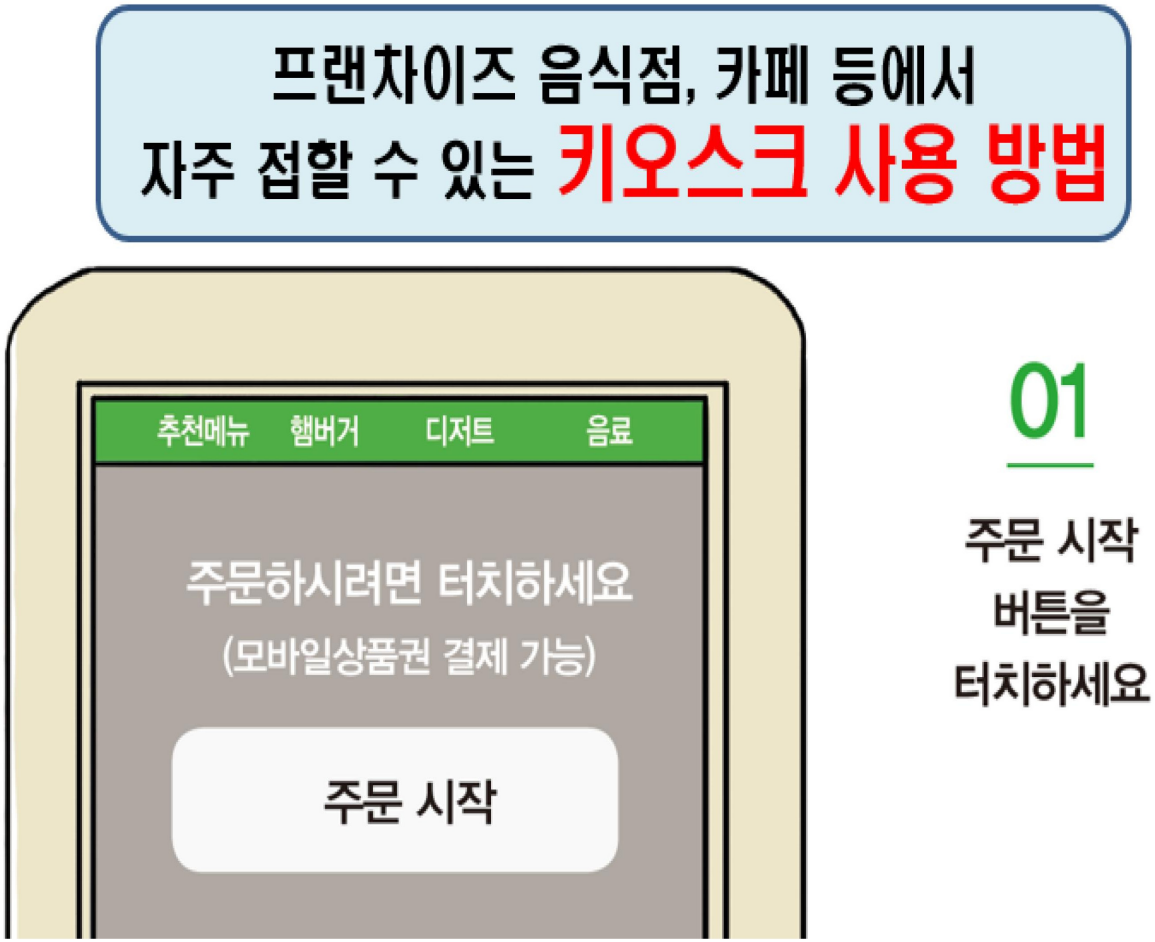
01 디지털 기기 사용 방법(키오스크 사용 영상 시청1)

https://www.youtube.com/watch?v=z3smvwkiBZA

02 디지털 기기 사용 방법(키오스크 사용 영상 시청2)

https://www.youtube.com/watch?v=Q9NuXKXGw44

03 디지털 기기 사용 방법(그림 설명자료)

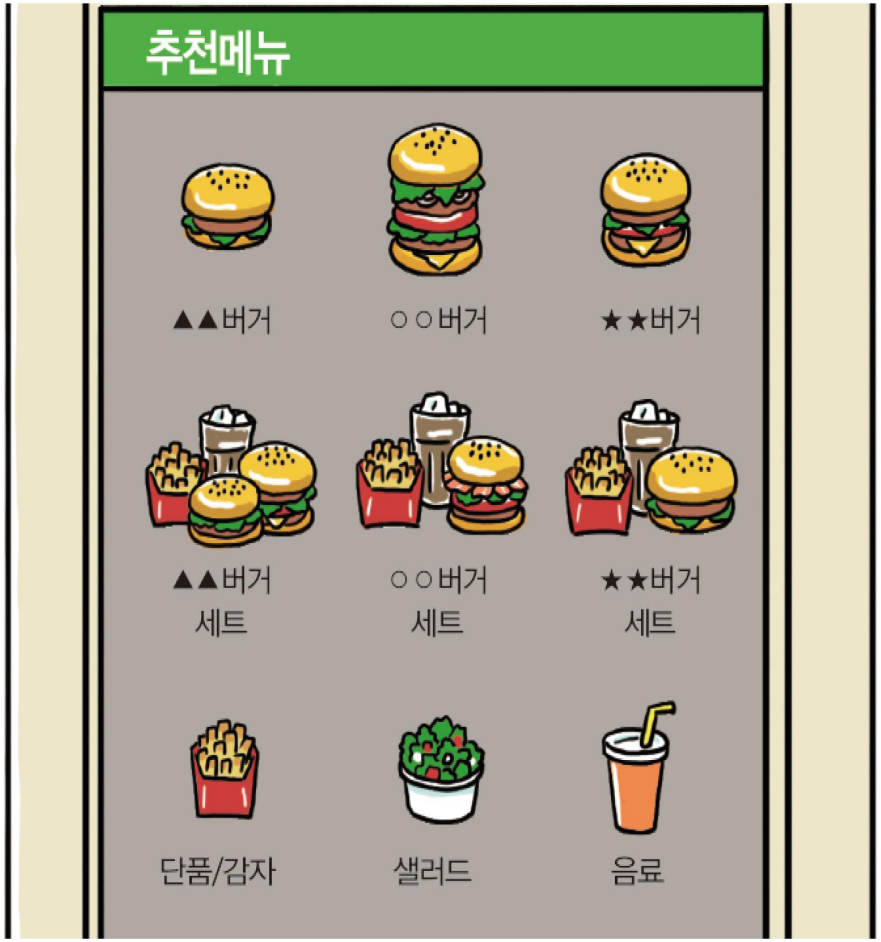


04 디지털 기기 사용 방법(그림 설명자료)

02

매장에서
식사 또는
포장(테이크아웃)
해당하는 것을
터치하세요

05 디지털 기기 사용 방법(그림 설명자료)



03

원하는
제품을
터치하세요

06 디지털 기기 사용 방법(그림 설명자료)

04

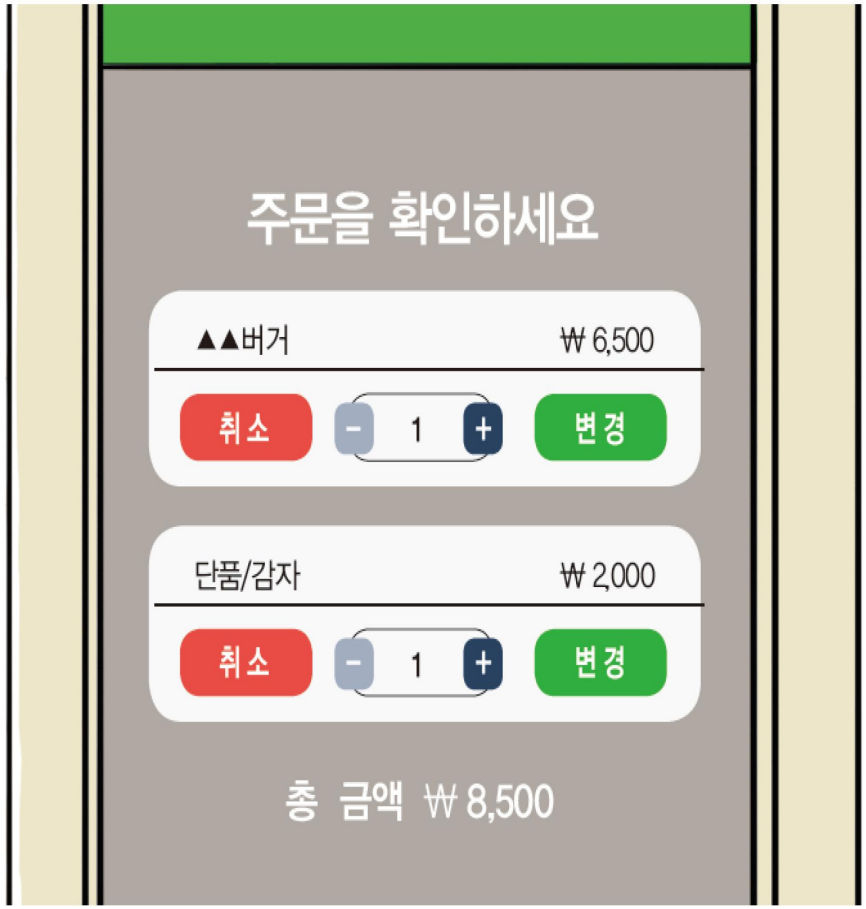
세트메뉴 등 추가 선택이 필요하면 추가메뉴를 터치하세요

07 디지털 기기 사용 방법(그림 설명자료)

05

장바구니 또는
주문완료 버튼을
터치하세요

08 디지털 기기 사용 방법(그림 설명자료)



06

주문을
확인하세요

08 디지털 기기 사용 방법(그림 설명자료)

07

결제하기를
눌러
결제수단을
선택합니다

주의해요!
피싱 사기

알아도 당할 수 있는 피싱 사기, 다음 피해자는 내가 될 수 있습니다.

2022년 청년 소비자 역량 제고 및 디지터 디바이드 해소 사업

청년 소비자 리더 황 현 송

보이스 피싱

출처 대구 경찰청 국민마당> 보이스피싱 바로알기

2021년 연령별 피해금액은 40.50대가 873억원(52.6%),
60대 이상이 614억원(37.0%), 20.30대는 173억원(10.4%)이며,
2019년 이후 60대 이상의 비중은 상대적으로 지속적으로 증가하고 있는 추세 입니다.

※ 보이스 피싱 유형

구분	내용
기관 사칭 유형	검찰·경찰 등 공공기관을 사칭하면서 개인정보를 입력하도록 한 후, 피해자의 재산을 사기이용계좌로 이체하도록 유도하여 피해 발생
대출 빙자형	저금리 햇살론으로 대환 대출을 해준다며 기존 저축은행 대출금을 사기범 계좌로 송금하도록 유도하여 피해 발생
납치 빙자형	자녀, 지인 등을 납치했다고 협박하며 입금을 강요하여 피해 발생

출처: 금융감독원 (http://www.fss.or.kr)/ 대한민국 공식 전자정부 누리집'연말연시 '가족납치' 보이스 피싱 급증 ...5가지만 기억하자!

피해시, 이렇게대처하세요!

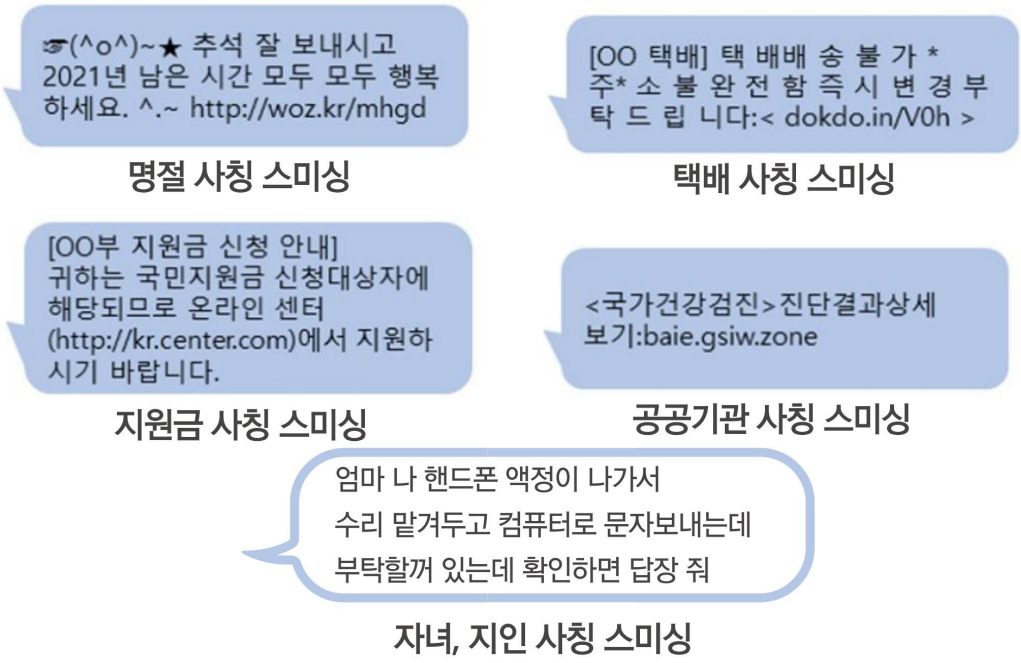
1. 송금은행, 입금은행 대표 번호 혹은
   경찰청(112)에 '지체 없이' 피해 사실 신고 후 지급 정지 신청
2. 가까운 경찰서 방문 '사건 사고 사실 확인원' 발급
3. '사건 사고 사실 확인원'을 지급 정지 신청 은행 영업점에 제출
4. 지급 정지된 계좌(사기이용계좌)의 명의자 소명 등을 거쳐 계좌에 남아 있는
   피해금 환급절차 진행

스미싱

스미싱은 문자메세지(SMS)와 피싱(Phising)의 합성어로 악성 앱 주소가 포함된 휴대폰 문자(SMS)를 대량으로 전송 후 이용자가 악성 앱을 설치하도록 유도하여 금융정보등을 탈취하는 신종 사기 수법입니다.

출처: KISA 인터넷 보호나라>사이버위협>스미싱

※ 스미싱 유형



출처: 과학기술정보통신부>보도자료>추석 명절, 선물 배송 등을 사칭한 문자사기(스미싱) 주의!>

피해시, 이렇게대처하세요!

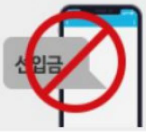
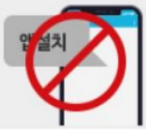
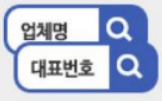
번호 도용 문자 발송 차단	모바일 결제 확인 및 취소	악성 어플리케이션 삭제	공인 인증서 폐기 및 재발급 하기

스미싱 관련 상담 및 신고 (국번없이) 118

출처: 한국 인터넷 진흥원>알림마당>보도자료>KISA 보안 공지를 사칭한 스미싱 문자 주의

피싱 사기 십계명

신고: 경찰청 (국번 없이) 112, 피해 상담 및 환급 (국번 없이) 1332

1	범죄 연루되었다며 자금이체 또는 현금 전달 요구 시 응하지 말 것	
2	메신저로 보내는 경찰, 검찰, 금감원의 공문은 모두 가짜임을 명심할 것	
3	저금리 대출 위해 기존 대출금 상환 요구 시 응하지 말 것	
4	어떠한 명목이든 대출과 관련하여 선입금 요구 시 응하지 말 것	
5	어떠한 경우에도 은행직원이 직접 현금을 전달받는 경우는 없음을 명심할 것	
6	수사기관·금융기관의 앱 설치 요구는 무조건 무시할 것	
7	출처 불명의 인터넷주소(URL)는 누르지 말고 의심부터 할 것	
8	구매하지 않은 결제문자는 정식업체 여부 및 대표번호 검색해볼 것	
9	문화상품권, 구글기프트카드 핀번호 요구에 절대 응하지 말 것	
10	가족 부상·납치 전화 시 반드시 112신고 등 주변 도움부터 요청할 것	

출처 대구 경찰청 국민마당> 보이스피싱 바로알기

주제강의
02

소비자24 앱 설치 및 활용방법 피해구제 방법

01

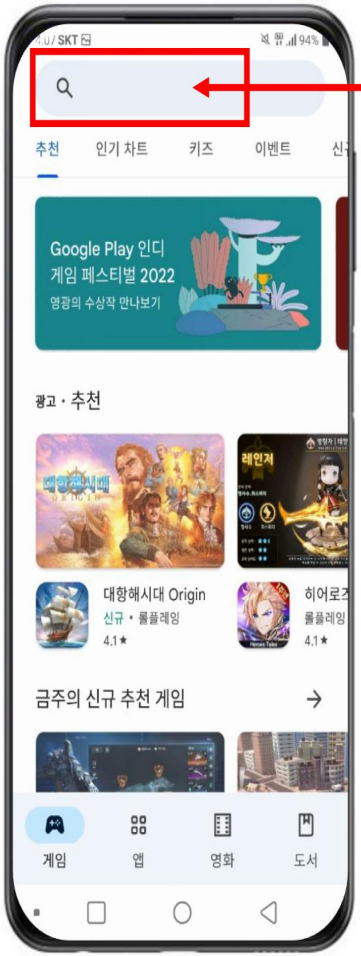
여러 소비자 정보를 확인할 수 있는 소비자24 앱 깔기

03 여러 소비자 정보 찾아볼 수 있는 소비자24 앱 깔기

03 여러 소비자 정보 찾아볼 수 있는 소비자24 앱 깔기

1

플레이스토어 선택!



'소비자24' 입력

05 여러 소비자 정보 찾아볼 수 있는 소비자24 앱 깔기

2

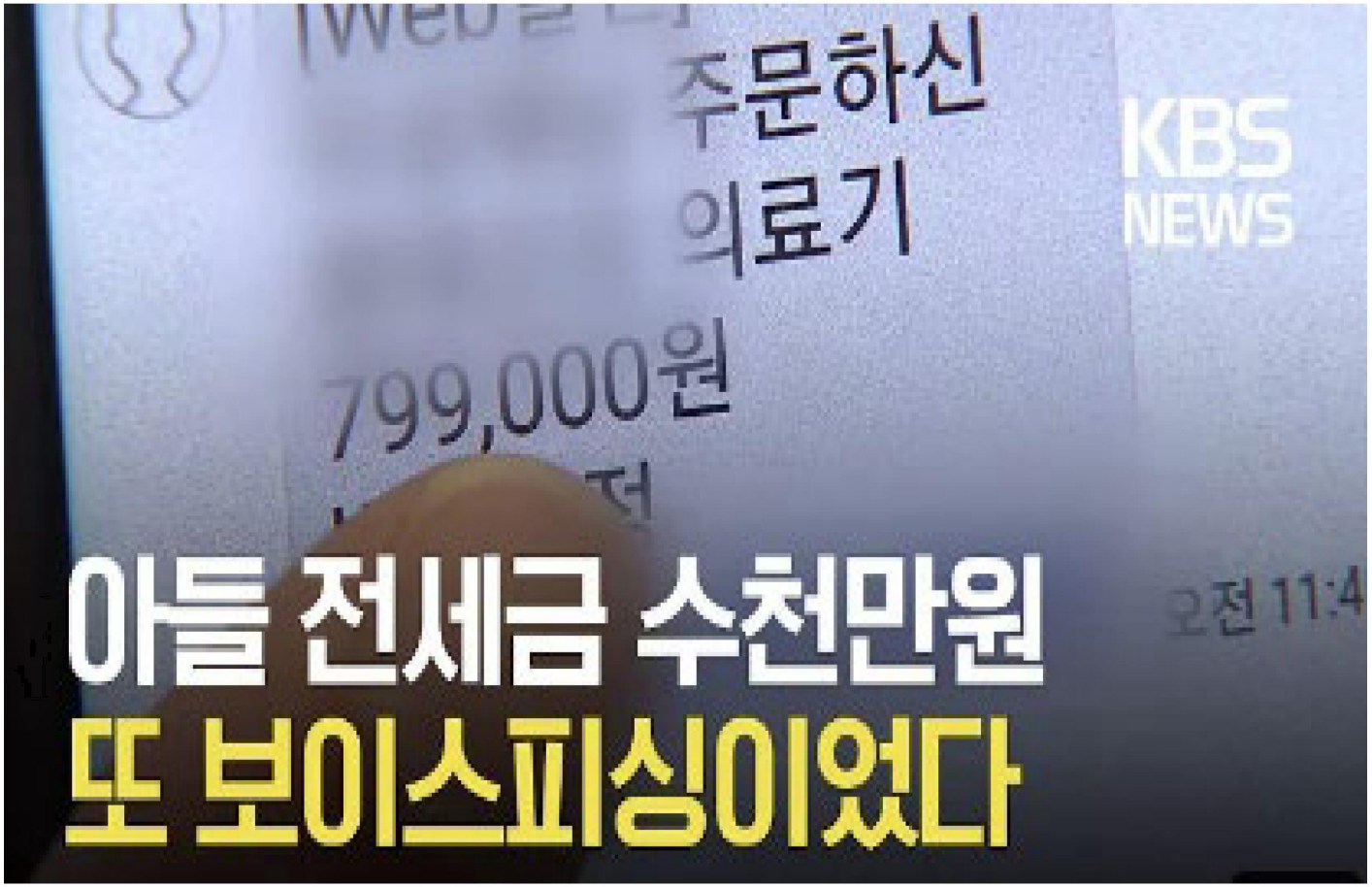
선택!

피해예방정보 확인!

디지털 금융사기 예방법

: 다양한 피례 사례 알아보기

01 디지털 금융사기 피해 사례 영상 시청



https://www.youtube.com/watch?v=1QzOSkOefGg

02 디지털 금융사기 피해 사례 알아보기

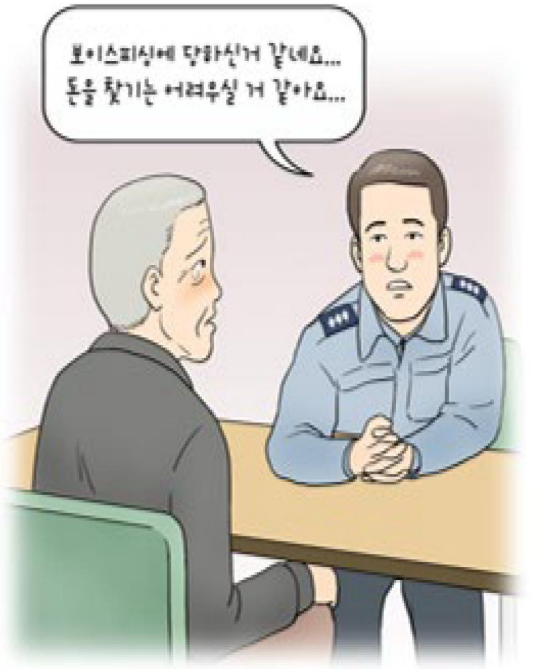
금융사기(보이스피싱, 스미싱) - 날로 진화하는 보이스피싱 사기

Ⅰ 경찰서, 검찰, 금융감독원, 은행 등을 사칭하며 여럿이 팀을 짜서 전화하는 수법도 등장

Ⅱ 은행 직원도 믿지 말고 자신의 말만 따르라고 지시 ATM기로 유도해 돈을 계좌이체 하도록 유도

Ⅲ 실제 전화번호가 찍히게 하거나 가짜로 은행이나 정부기관 홈페이지를 만들어 직접 계좌번호, 비밀번호를 입력하도록 유도

Ⅳ 울면서 횡설수설하는 어린아이 목소리를 들려주고 자녀가 다쳤다고 혹은 자녀를 납치했다며 돈을 요구하는 수법 등장



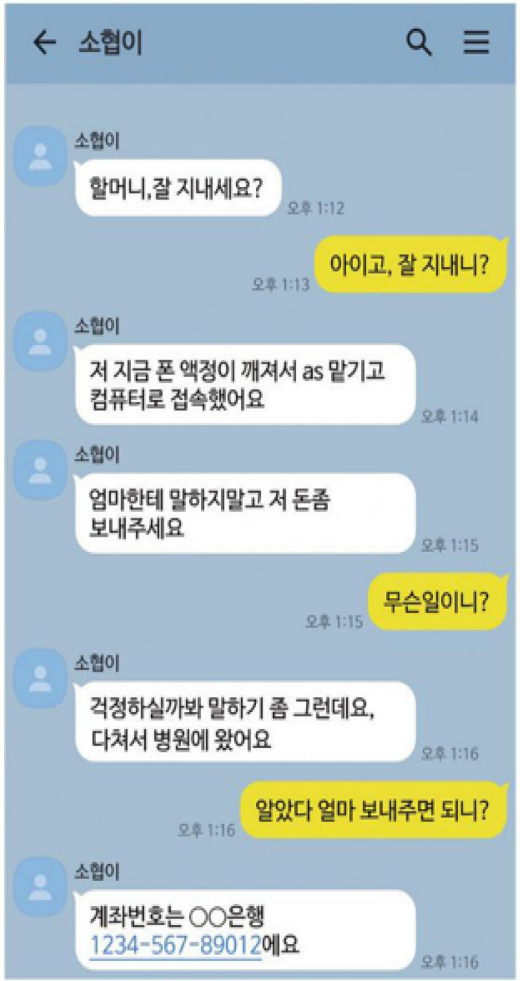
03 디지털 금융사기 피해 사례 알아보기

1

04 디지털 금융사기 피해 사례 알아보기

[금융사기 유형 1]

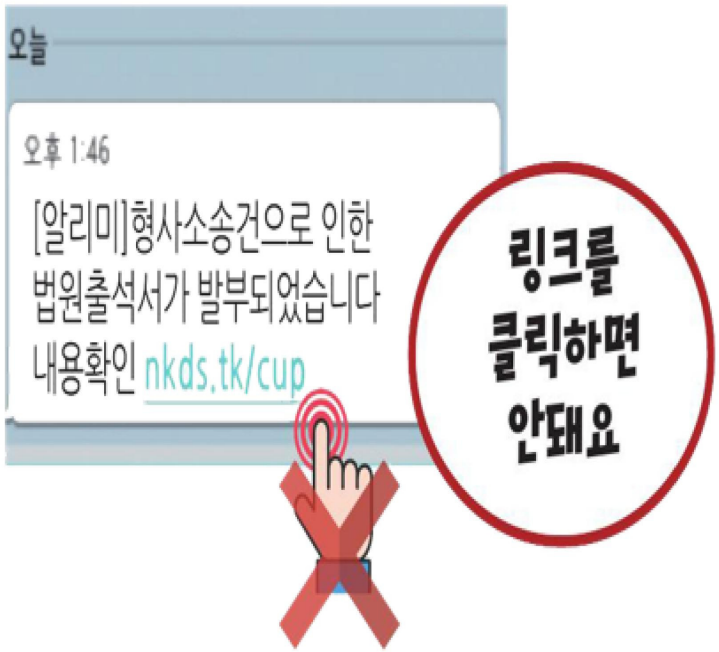
- 전화, 메신저 등으로 **공공기관** 또는 **지인이라 속여** 소비자에게 송금, 예금 인출 등을 유도하여 경제적 피해를 주는 수법



05 디지털 금융사기 피해 사례 알아보기

[금융사기 유형 2]

- **낯선 문자나 메신저로 보내 온 주소**를 휴대폰 사용자가 누르면 휴대폰의 정보를 빼내어 가는 수법



06 디지털 금융사기 예방

경찰 • 검찰 • 금감원 • 금융기관 등을 사칭하여 개인정보나 계좌이체를 요구하면 100% 사기입니다.

개인정보를 미리 알고 접근하는 경우에도 내용의 사실여부를 반드시 확인해야 합니다

공공기관 사이트에 접속시켜 보안카드번호를 전체 입력하라는 등 많은 금융거래 정보를 요구하면 100%사기입니다.

07 디지털 금융사기 예방

[금융사기 대처요령]

- ✓ **의심** 하고!
- ✓ **전화** 끊고!
- ✓ **확인** 하고!

금융감독원 콜센터 ☎1332
경찰청 ☎112

2022년 청년 소비자 역량 제고 및 디지털 디바이드 해소사업

참고자료

보이스피싱 범죄현황과 대응방안

〈참고자료〉

보이스피싱 범죄현황과 대응방안

〈대구YMCA〉

1. 취약계층 디지털 피해상황과 예방교육의 필요성

○ 인터넷과 전화 및 스마트기기 보급률이 세계 최고 수준에 이르고 있으며 이러한 인프라를 악용한 사이버범죄는 지속적으로 발전하고 있음. 특히 보이스피싱은 정보산업 시대를 살아가는 시민에게 익숙한 범죄로서 보이스피싱 사기피해가 나타난 2000년대 초반과는 달리 청소년 피해자가 늘어나고 있음.

- 2006년 5월 인천 거주 피해자가 국세청을 사칭한 사기전화를 받고 800만원을 송금한 최초의 사례이후, 주로 노인층이나 주의깊지 못한 사람들이 주된 피해자였음.

연도	발생건수	피해액(억원)	검거 건수
2015	18,549	2,040	15,887
2016	17,040	1,468	11,386
2017	24,259	2,470	19,618
2018	34,132	4,040	29,952
2019	37,667	6,398	29,278

참조: 한치운, 2020, “보이스피싱 심리조작 수법과 소비자보호 방안”.

- 최근 보이스피싱 10대-20대 피해 현황은 2019년에 3,855명이었으며, 2020년에는 5,323명으로 급증하여 약 38% 늘어났음(서울경제, 2021. 3.21일자).

○ 초기 보이스피싱 범죄는 여러 기관이나 지인을 사칭해 시나리오를 바탕으로 입금을 요구하는 형태에서 컴퓨터나 스마트폰을 해킹해 금융관련 정보를 탈취하거나 정보를 조작하는 등의 수법을 동원하고 있음.

- 2008년에는 피해자를 피싱사이트로 유동해 금원을 편취하는 파밍(Pharming)수법이 등장
- 2011년에는 메신저로 악성 링크를 발송해 금융정보를 탈취하고 금원을 편취하는 스미싱(Smishing) 수법이 나타남(김동호, 2020).
- 2013년에는 악성애비나 악성코드로 피해자가 기기를 감염시켜 금원을 편취하는 메모리 해킹(memory hacking), 기업의 이메일 계정을 해킹해 거래 대금을 편취하는 무역사기 사례도 등장함(김대근외, 2016).

○ 최근에는 안면이나 음성 딥페이크 등 인공지능 기술을 활용하거나 스푸핑을 통해 발신번호를 변작하기도 함. 스미싱을 통해 악성앱을 설치하고 스마트폰을 해킹하기도 하며, 선불 USM을 악용하거나 SIM Box를 활용해 해외번호를 국내번호로 변작하기도 함.

- 사례 보이스피싱 조직은 가짜앱을 만들어 설치를 유도하고 스마트폰을 해킹해 은행 대표전화를 가로챔. 피해자가 의심하고 실제 기관의 전화번호로 확인 전화를 걸어도 보이스피싱 조직원이 전화를 받는 상황이 벌어짐(ChosunBiz, 2021. 3.17일자).

○ 2020년 금융감독원의 자료에 의하면, 전체 피해금액에서 메신저 피싱 피해가 차지하는 비중이 15.9%로 전년 대비 10.8% 증가하였음(김동민, 202; 금융위원회, 2020; 현새롬, 2021).

- 악성 프로그램을 유포해 파일을 암호화하고 복호화를 조건으로 금품을 요구하는 팬섬웨어도 활개를 치는 등 전통적인 보이스피싱 유형에 다양한 기술을 활용하거나 사기수법을 혼용하는 등의 형태로 수법이 진화하고 있음.

- 원격제어 앱을 설치하도록 유도해 직접 피해자의 휴대전화를 조작하는 방식으로 대출을 받거나 금액을 이체하는 사례도 드러남.
- 노인이나 장애인, 청소년·아동 등 디지털 기술과 금융 시스템에 대한 이해가 낮은 계층은 딥테이크 기술을 활용한 안면이나 음성조작, 발신번호 조작 등을 활용한 수법에 고스란히 당할 수 밖에 없는 취약한 상황임.
- 2020년 메신저 피싱의 연령별 분포를 살펴보면 30대 이하는 3.4%, 40대는 4.6%, 50대는 43.3%, 60대 42.5%로 고령층이 전체 메신저 피싱 피해의 85.5%를 차지함.

○ 보이스피싱 범죄는 단순한 범죄 수사방식으로는 범죄를 근절할 수 없고 피해자를 구제하기도 어려움. 범죄를 계획하고 실행하는 조직, 금액을 환전하거나 세탁하는 등의 조직들이 각각 역할을 나눠 단계별로 다양한 형태의 범행수법을 활용함. 사칭하는 기관도 지속적으로 변경하고 새로운 범죄모델을 만들기도 하며, 당시 이슈나 사회의 상황 등을 고려해 사칭대상을 지능적으로 선정하기도 함.

- 보이스피싱 범죄가 발생하더라도 이후의 법률적, 정책적 사후 대응이 제대로 이루어지기 어렵고 수사기관과 사법기관의 대응이 무력화되는 경우가 다반사임.
- 경찰청과 금융감독원이 그러한 행위와 흐름을 추적하며 끊임없이 대응해 오고 있으나 어떤 기술이 탐지되면 곧바로 변종을 개발해 활용하고 유포하는 등 오늘날 보이스피싱 조직은 매우 지능적임. 또한 금융기관이 보이스피싱에 관련된 계좌를 차단하더라도 이미 탈취한 금액을 여러 계좌로 분산해 두었거나 비트코인으로 환전하거나 게임 아이템을 구매하고 다시 환전하는 등의 여러 방식으로 범죄수익을 세탁해 현금화하고 있음.
- 결국 이에 대응하는 당국은 범죄피해의 규모를 정확히 파악하기도 어렵고 이를 추적하고 몰수하기도 어려운 실정임. 중국이나 다른 제3국을 경유해 범죄가 이루어지는 경우에는 국가 간 수사공조가 없이는 접근하기도 어려운 경우가 많음.
- 따라서 민간과 공공이 함께 공동 대응체계를 구축하고 청소년과 어르신 등 디지털 취약계층의 디지털 문해교육 및 피해예방 교육을 통한 범사회적인 차원의 위험 완화를 위한 대책을 강구해야 할 필요성이 있음.

2. 보이스피싱 이해

1) 보이스피싱이란?

○ '보이스피싱'은 일반적으로 '목소리를 통하여 개인정보를 낚아 올린다'는 의미이며, 음성이라'는 뜻의 '보이스(Voice)'와 사기 범죄라는 의미의 "피싱(Phishing)'을 결합한 합성어임.

- 경찰청과 금융감독원의 '피싱사기'에 대해 ① 기망행위로 타인의 재산을 편취하는 사기범죄의 하나로 ② 전기통신수단을 이용한 비대면 거래를 통해 ③ 금융분야에서 발생하는 일종의 특수사기범죄라고 정의함.
- 〈전기통신금융사기 피해방지 및 피해금 환급에 관한 특별법〉은 '보이스피싱'을 '전기통신금융사기'로 개념화하고 그 의미를 전기통신을 이용하여 타인을 기망·공갈함으로써 재산상의 이익을 취하거나 제3자에게 재산상의 이익을 취하게 하는 행위로 ①자금을 송금·이체하도록 하는 행위 ② 개인정보를 알아내어 자금을 송금·이체하는 행위라고 정의함.

2) 보이스피싱 유형과 수법

〈전통적인 보이스피싱 범죄 주요유형〉

주요 유형	주요수법
▸자녀납치 및 사고를 빙자하여 편취	• 범행 전에 부모와 자녀의 연락처를 확보한 범죄자가 부모에게 변조한 자녀의 전화번호로 연락하여 납치나 사고를 당했다는 방식으로 기망하여 계좌이체 등으로 편취
▸메신저에게 지인을 사칭하여 송금요구	• 해킹한 메신저 아이디 등 계정정보에 등록된 피해자의 지인과 메신저로 대화하여 교통사고 등 급하게 돈이 필요하다고 속여서 편취
▸인터넷 뱅킹을 이용하여카드론 대금 및 예금 등 편취	• 피해자가 범죄사건으로 수사받고 있다는 등으로 속여 피싱사이트에 접속하게 한 후, 입력한 정보로 알아낸 피해자의 금융거래 관련 정보를 이용하여 범죄자가 직접 피해자 명의로 대출을 받은 후 금원을 편취

주요 유형	주요수법
▸금융회사, 금감원 명으의 허위 긴급공지 문자메시지로 기망, 피싱 사이트로 유도하여 예금 등 편취	• 은행의 보안등급 향상 등 피싱사이트 링크가 포함된 문자를 발송한 후 피해자가 피싱사이트에 접속하여 입력한 금융거래 관련 정보로 범죄자가 피해자 명의 계좌에 있는 금원을 이체하거나 대출하는 방법으로 편취
▸전화통화를 통해 텔레뱅킹 이용정보를 알아내어 금전 편취	• 고령 피해자를 대상으로 전화하여 피해자 명의 계좌가 범죄에 악용되었다는 등으로 현혹하여 개인정보 및 금융거래 관련 보안 정보를 알아낸 후 피해자 명의계좌에 있는 금원을 이체하거나 대출하는 방법으로 편취
▸피해자를 기망하여 자동화 기기로 유인 편취	• 경찰·검찰을 사칭한 범죄자가 피해자에게 전화하여 계좌 등이 범죄에 악용되어 조치가 필요하다는 등으로 속여 범죄자의 계좌로 금원을 이체하거나 금융기관 직원이 개인정보를 유출하였다고 속여 자동화기기에서 피해자가 범죄자의 계좌로 금원을 이체하는 방법으로 편취
▸피해자를 기망하여 피해자에게 자금을 이체토록 하여 편취	• 경찰·검찰을 사칭하여 수사를 위해 계좌거래내역을 확인해야 한다는 드의 이유로 범죄자의 계좌에 이체하거나 국세청 직원을 사칭하여 미납세금을 납부하라고 속여 범죄자의 계좌로 금원을 이체하는 방법으로 편취
▸신용카드정보 취득 후 ARS를 이용한 카드론 대금 편취	• 피해자 신용카드 정보를 범죄가가 확보하여 대출을 받은 후 피해자에게 범죄자금이 입금되었다고 속여 다시 범죄자의 계좌로 이체하는 방법으로 편취
▸기관사칭 상황극 연출에 의한 피해자 기망 편취	• 피해자에게 경찰 또는 검찰의 수사상황을 들리도록 상황을 연출하여 피해자를 기망한 후, 범죄에 악용된 피해자의 금융정보 확인을 위해 필요하다며 범죄자의 계좌로 자금을 이체하도록 한 후 편취
▸물품대금 오류송금 빙자로 피해자를 기망하여 편취	• 피해자에게 물품대금 등 허위 계좌 입금 문자를 발송한 후, 잘못 송금한 금원의 반환을 요구하여 편취

참고: 현새롬, 2021, “보이스피싱 범죄수법의 진화와 제도적 대응방안에 관한 연구”.

○ 그러나 이러한 보이스피싱 개념도 IT기술의 발달에 따라 변화하여 의미도 달라지고 있음.

- 통신매체를 수단으로 피해자와 연결하여 대화를 통해 피해자를 기망한 후, 피해자가 금전을 제공하도록 유도하여 금원을 편취하는 수법에서 나아가 전화를 이용하여 피해자로부터 금융정보를 취득 후, 범죄자가 직접 금융거래를 시도하여 금원을 편취하는 형태로 범위가 확장됨.

3) 보이스피싱 범죄의 특징

(1) 초국가적 특성(김대근외 2016; 박홍두, 2021)

○ 보이스피싱은 기존의 일반적 범죄와는 달리 특정지역과 한정하여 발생하지 않음.

- 국내에 발생하는 보이스피싱의 경우, 대부분 중국이나 필리핀 등 해외에 보이스피싱을 위한 서버를 구축한 뒤 우리나라에 거주하는 피해자를 상대로 범행한 후 그 범죄수익은 자금세탁을 거쳐 다시 국외로 반출하는 흐름을 보이고 있음.
- 이러한 초국가적 속성으로 국내에서 보이스피싱 범죄조직을 적발하여 체포한다고 하더라도 상위조직이 해외에 있어 지속적하여 범죄가 발생함.

(2) 조직범죄적 특성(윤해성·곽대경, 2009; 김도윤, 2020).

○ 보이스피싱은 초기에는 개인이 작은 규모로 실행하는 범죄였지만, 현재는 조직범죄의 형태를 갖추고 있음.

- 보이스피싱 범죄조직은 범죄 실행의 총책(주범)을 중심으로 하부조직에 프로그램 개발·제작·유포, 타인의 명의로 통장을 개설한 뒤 통장을 소유한 자가 해당 계좌의 소유권을 보유하는 이른바, '대포통장'의 모집과 공급, 현금 인출과 송금, 시스템 운영 등으로 체계화되고 있음.
- 이러한 조직범죄적 성격으로 인해 수사기관이 주범을 검거하지 않는 이상, 주범을 중심으로 하부조직은 바꿔가며 범행을 지속하기 때문에 보이스피싱 범죄를 근절하는 것이 매우 어려움.

- 최근에는 보이스피싱, 피싱, 파밍 등 개별적 유형의 범죄가 대출사기, 초건만남사기 등 높은 범죄수익을 가져오는 다양한 범죄와 융합되는 형태르 ㄹ보이면서 범죄조직의 규모가 '기업형'이라고 할 수 있을 정도로 확대추세임.
- 이로인해 사기행위에 가담하는 자들이 조직내부에서 타인의 역할이나 직위 등에 대해서는 알 수 없으며 소수 혹은 단독 관리자를 중심으로 운영과 관리가 이루어지는 점조직 형태로 운영됨.
- 보이스피싱은 예비, 음모단계부터 체계적이고 조직적인 편취행위가 이루어지며, 범행과정에서 비대면 프로그램을 활용하게 되어 범행에 대한 죄책감도 줄어들어 범행에 쉽게 가담할 수 있도록 유인하는 효과까지 유발하는 것으로 평가됨.

(3) 지능적·가변적 특성

○ 보이싱피싱 범죄는 실행과정에서 각 단계별로 다양한 형태의 범행 수업을 지속적으로 만들어내는 지능적 특성을 지니고 있음.

- 사칭기관을 변경하거나 수법을 바꾸기도 하고, 점차 정교한 기망수단을 활용하는 등 지속적으로 새로운 방법들을 통해 범죄를 실행함.
- 피해자가 피해사실을 인지하더라도 신고할 수 없거나 수사를 지연할 수 있는 수단들을 활용하거나 범죄 발생 이후 사법적 또는 법·정책적으로 대응이 이루어지면 수법을 변경하거나 허점을 악용하여 국가적 대응을 무력화함.
- 범죄자는 복잡한 정보통신기술과 금융결재 방식의 취약점을 찾아내 악성 프로그램을 설치하는 등의 방식으로 범행수법을 진화시키고 있음.
- 정보보안업체나 수사기관이 악성프로그램을 탐지하면 즉시 변종 프로그램을 개발하여 유포할 만큼 지능적 양태를 보이고 있음. 또한 금융기관이 범죄와 관련된 계좌를 신속하게 파악하여 지급을 정지하게 되더라도 지급을 정지하기까지 상당히 짧은 시간임에도 불구하고 수많은 금융계좌로 분산 이체하고, 비트코인 환전, 불법외환거래 등을 실시하여 범죄수익의 출처와 흐름을 파악하기 어렵게 함.

(4) 정보의 비대칭성

○ 보이스 피싱 범죄에서는 범죄조직이 보유한 정보가 피해자가 인지하고 있는 정보의 양보다 많기 때문에 이른바 '정보의 비대칭성'이 중요한 요소로 작용함.

- 일반인은 금융과 행정 등 비공개 정보를 알수 없다는 점과 유출된 개인정보를 범죄자가 어느 정도까지 인지하고 있는지 알 수 없음. 이러한 이유로 특히 대출사기나 보험사기 등과 같이 금융회사의 관련 정책이나 정보 등 복잡한 금융시스템에 대한 이해도가 낮은 고령층이나 사회적 취약계층의 정보의 비대칭성을 이용한 범죄가 많아 피해가 집중되고 있음.

3. 보이스피싱 대응현황과 한계

1) 보이스피싱 초기 대응정책

○ 2007년 보이스피싱 피해예방 10계명 발표

- 당시 정통부와 한국정보보호진흥원은 '전화금융사기(보이스피싱) 피해예방 10계명'을 발표했고, 이동통신 3사, 초고속인터넷 사업자와 주요 포털 등 인터넷 서비스 제공자, 관련 협회들이 참여했음.

연번	내 용
1	• 미니홈피, 블로그 등 1인 미디어 내에 전화번호 등 자신 및 가족의 개인정보를 게시하지 않습니다.
2	• 종친회, 동창회, 동호회 사이트 등에 주소록, 비상연락처 파일을 게시하지 않습니다.
3	• 자녀 등 가족에 대한 비상시 연락을 위해 친구나 교사 등의 연락처를 확보합니다.
4	• 전화를 이용하여 계좌번호, 카드번호, 주민번호 등 정보를 요구하는 경우 일체 대응하지 마십시오.
5	• 현금지급기(CD/ATM)를 이용하여 세금 또는 보험료 환급, 등록금 납부 등을 하여 준다는 안내에 일체 대응하지 마십시오.

연번	내 용
6	• 동창생 또는 종친회원이라고 하면서 입금을 요구하는 경우 반드시 사실관계를 재확인하시기 바랍니다.
7	• 발신자 전화번호를 확인합니다.
8	• 자동응답시스템(ARS)를 이용한 사기전화를 주의하세요.
9	• 휴대폰 문자서비스를 적극 이용하세요.
10	• 속아서 전화사기범들 계좌에 자금을 이체했거나 개인정보를 알려준 경우, 즉시 관계 기관에 신고하세요.

○ 2007년 외국인 계좌 개설시 신원확인 의무화

- 2007년 8월부터 외국인 예금계좌를 개설하는 경우 여권 외에도 사업자등록증, 취업증명서 등을 제출하도록 해 신분확인 절차를 강화했음.

○ 2009년 발신번호 표시제도 도입

- 2009년 5월 방송통신위원회는 통신사업자들과 협력해 국제착신전화에 국제전화 식별번호를 표시하도록 하는 발신번호 표시제도를 도입했음. 동제도는 해외에서 국제교환망을 통해 국내로 전화신호가 들어오는 경우 국제전화번호앞에 001(KT), 002(LGU+), 006(텔링크), 00391(별정통신사업자) 등의 번호를 붙여 국제전화를 접수한 통신사업자의 고유한 식별번호를 붙이도록 하였음. 관공서를 사칭하고 발신번호를 국내번호처럼 조작하는 경우에 대응하기 위한 시도였음.

2) 2020년 보이스피싱 척결 종합방안

- 관계부처는 전방위적인 예방 및 차단 시스템 구축, 단속과 처벌의 실효성 확보, 발생 피해에 대해 종합적인 피해구제 강화, 관계부처 간 상시협업체계 구축 및 강화, 홍보강화를 통한 경각심 강화 5가지 전략으로 구성된 대책을 수립하였음.

〈2020년 보이스피싱 척결 종합방안〉

보이스피싱 범죄 시도가 성공하지 못하도록 전방위적인 예방, 차단시스템 구축	
내용	• 보이스피싱에 이용되는 전기통신수단 신속예방·차단
	• 스마트폰 등 통신수단 부정사용 자체를 사전에 방지하기 위해 “개통-이용-중지” 단계에 걸쳐 신속·종합적 대응체계 구축
	• 다양한 통신수단(전화번호, 악성앱, 피싱사이트 등)이 보이스피싱 등에 이용된 경우, 신속하게 이용중지·차단하도록 개선
	• 보이스피싱 예방을 위한 디지털 신기술 개발·활용촉진
	• 통신사업자 등이 각종 빅데이터·AI 연계 시범사업 등을 활용하여 보이스피싱 탐지·대응기술·서비스 고도화할 수 있도록 지원
	• 보이스피싱 의심 금융거래 모니터링 강화
	• 민간사업자의 예방 의무 강화
	• 금융회사의 보이스피싱 예방을 위한 의무를 강화
금융범죄의 유인 자체를 없앨 수 있도록 단속과 처벌의 실효성을 확보	
내용	• 보이스피싱 관련 수사·단속 강화
	• 보이스피싱 관련 범죄 처벌 강화
이미 발생한 피해에 대한 종합적 피해구제 강화	
	• 금융회사를 통한 피해구제 제도 정비
	• 보이스피싱 보험을 통한 피해구제 활성화
집행이 실효성을 높일 수 있도록 관계부처 간 상시 협업체계를 구축 강화	
내용	• 관계부처·기관 협업 강화
	• 금융·통신·수사당국, 민간사업자 공동 대응체계 구축
보이스피싱에 대한 홍보 강화를 통해 국민들의 경각심을 환기	
	• 전방위·입체적 홍보 강화
	• 방송, 광고, 캠페인 등을 통한 입체적인 대국민 홍보실시
	• 신종수법 수시 경보발령, 방지서비스 안내 등을 통한 국민 경각심 강화

3) 소비자 측면에서 보이스피싱 예방 방안

○ 보이스피싱 피해를 예방하기 위해서는 사기범의 의도에 넘어가지 않고 끊임없이 의심하며 해당기관에 직접 확인을 해보는 것이 중요함.

- 기업 및 공공기관은 보이스피싱 사기범이 주로 사용하는 단어나 말투 등을 사용하지 않아야 하며, 소비자에게 안내를 할때에는 간결한 단어를 사용하여 명쾌하게 정보를 전달해야 함.
- 소비자의 경우에는 모르는 전화는 받지 않는 것이 보이스피싱 예방에 가장 중요하지만, 전화를 받게 되었다면 사기범의 페이스로 전화 대화가 진행되는 것을 경계해야 한다. 사기범과의 대화 도중에 질문을 하거나 반론을 던지는 등의 조치를 취하는 것이 바람직함.

소비자 피해 예방방안	• 될 수 있으면 모르는 전화는 받지 않을 것
	• 나를 포함 누구나 속을 수 있다는 사실을 인정하고 나는 괜찮을 것이라는 생각을 하지 않는 것이 중요함
	• 금융기관 사칭 등을 빠르게 감지 한후 통화를 중단하고 해당기관에 직접 확인해 볼 것
	• 상대방의 호의 및 제안에 대한 질문 및 반론 제기

참조: 한지훈, 2020, “보이스피싱 심리조작 수법과 소비자 보호방안

□ 참고문헌

김문희. 2016. “ 스마트폰 정보보안 위협과 보이스피싱 대응방안에 관한연구. 울산대학교 대학원 석사학위 논문.

김덕용. 2018. “보이스피싱에 대한 경찰의 대응방안”. 한국디지털콘텐츠학회.

양영진. 2008. “보이스피싱 범죄의 근절방안에 관한 연구”. 경남대학교 석사학위논문.

윤해성·곽대경. 2009. “보이스피싱의 예방과 대책마련을 위한 연구. 한국형사정책연구원.

한치운. 2021. “보이스피싱 심리조작 수법과 소비자보호방안”. 연세대학교 정보대학원 석사학위 논문.

현세롬. 2021. “보이스피싱 범죄수법의 진화와 제도적 대응방안에 관한 연구. 고려대학교 정보보호대학원 석사학위 논문.

2022년 청년 소비자

역량 제고 및 디지털 디바이드 해소사업

주관 : **대구경북미래소비자행동 · 대구YMCA**

주최 : **공정거래위원회 · 한국소비자단체협의회 · (사)한국소비자교육정책학회**