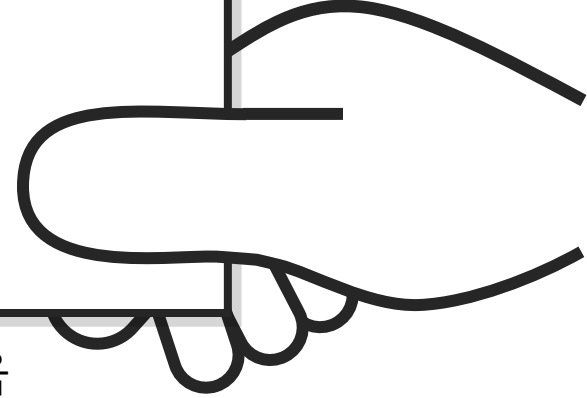




보이스피싱 예방 & AI 디지털 상식 교육

전북우리사이 온기순환팀 3회차 교육



오늘 교육을 통해 이런 것들을 배워요.

1. 보이스피싱과 AI 범죄 이해하기

- AI 목소리 복제(딥보이스) 등 새로운 수법의 위험성을 이해합니다.

2. 올바른 대처 방법 익히기

- 의심스러운 전화를 받았을 때 당황하지 않고 행동하는 법을 배웁니다.

3. 안전한 습관 기르기

- 개인정보와 금융정보를 지키는 생활 습관을 실천합니다.

목차

1. 보이스피싱 및 AI 지능범죄 예방 교육
2. 개인정보 보호 교육
3. 보이스피싱 역할극
4. 디지털 상식 OX 퀴즈

보이스피싱 및 AI 지능범죄 예방 교육

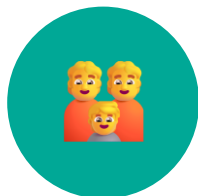
보이스피싱이란?

'Voice(음성)' + 'Private Data(개인정보)' + 'Fishing(낚시)'가 합쳐진 말로,
전화/문자 등으로 상대를 속여 돈이나 개인정보를 가로채는 범죄입니다.



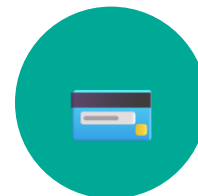
기관 사칭형

검찰·경찰·금융감독원 등을 사칭해
"수사 대상"이라며 겁을 줍니다



가족·지인 사칭형

자녀·손주를 사칭해 사고나
납치 등 위급 상황을 꾸밉니다



대출·금융 사기형

저금리 대출, 정부지원금을
미끼로 돈을 요구합니다

AI 음성 복제, '딥보이스' 범죄

딥보이스(Deep Voice)란?

인공지능(AI)이 사람의 목소리를 아주 짧게 듣고도 똑같이 흉내 낼 수 있는 기술입니다.

단 몇 초 분량의 통화 목소리만 있어도 가족이나 지인의 목소리를 정교하게 복제해 전화 사기에 악용할 수 있습니다.

왜 더 위험할까요?

- ! 실제 가족·지인의 목소리와 거의 구별이 어려움
- ! SNS·유튜브 등에 남긴 음성만으로도 복제 가능
- ! "목소리가 진짜니까 진짜겠지"라는 방심을 노림

기억하세요: 목소리가 똑같아도 요구하는 내용이 '급한 송금·정보 요구'라면 반드시 의심!

이런 일이 실제로 일어났습니다.

사례 1

"엄마, 나 사고 났어"

자녀 목소리를 흉내 낸 전화를 받고 놀라
합의금 명목으로 급히 송금한 사례

사례 2

검찰 사칭 전화

"계좌가 범죄에 연루됐다"며 검찰을 사칭,
안전계좌로 이체를 요구한 사례

사례 3

손주 목소리 딥보이스

AI로 복제한 손주 목소리로 급전을 요구해
금전 피해를 입은 사례

※ 실제 보도된 유형을 재구성한 사례입니다

[\(21\) "아빠 나 큰일 났어" 보이스피싱 실제 대화 \[제보영상\] / YTN - YouTube](#)

[\(21\) "목소리도 우는 것도 똑같아"... 딥보이스 사기 피해 잇따라 \[MBN 뉴스7\] - YouTube](#)

가족·지인 사칭 AI 음성피싱, 이런 특징이 있어요.



다급하게 '지금 당장' 돈을 보내라고
재촉함



평소와 다른 계좌로 입금을 요구함



사고·합의금·병원비 등 급박한 상황을
강조함



영상통화를 피하거나 화질이 안 좋다는
핑계를 댐



전화를 끊지 못하게 하거나 다른 사람과
상의를 막음



가족 이름·개인정보를 먼저 언급하며
신뢰를 유도함

의심스러운 전화, 이렇게 대처하세요.

1

일단 전화를
끊습니다

당황하지 말고 침착하게
통화를 종료하세요

2

본인이 직접
확인합니다

가족·지인에게 알고 있던 번호로
직접 전화해 확인하세요

3

돈을 절대 보내지
않습니다

확인 전까지는 어떤 명목으로도
송금하지 않습니다

4

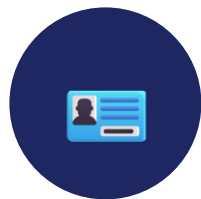
112 또는
금융기관에
신고합니다

의심되면 즉시 경찰(112)이나
은행에 알립니다

개인정보 보호 교육

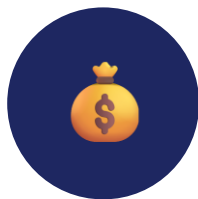
개인정보·금융정보, 왜 소중할까요?

이름, 주민등록번호, 계좌번호, 비밀번호 같은 정보는
범죄자에게는 '돈으로 바꿀 수 있는 열쇠'와 같습니다.



신분 도용

내 이름으로 대출을 받거나
계약을 체결할 수 있습니다



금융 피해

계좌 정보가 유출되면
예금이 인출될 수 있습니다



2차 피해

유출된 정보로 또 다른
사기 전화가 걸려옵니다

개인정보·금융정보 안전하게 지키는 법



비밀번호·계좌번호는 절대 문자나 전화로 알려주지 않기



택배·과태료 등을 가장한 문자는 클릭하지 않고 삭제하기



출처가 불분명한 문자의 링크(URL)는 누르지 않기



낯선 앱 설치를 유도하면 절대 설치하지 않기



공동인증서·보안카드 사진을 남기거나 전달하지 않기



중요한 서류(통장, 신분증)는 잘 보관하고 사본을 함부로 주지 않기

전화로 개인정보를 요구한다면?

❌ 이렇게 하지 마세요

- 전화로 주민등록번호·계좌번호 알려주기
- 은행/기관이라며 앱 설치 요구에 응하기
- "확인해줄게요"라며 ARS 버튼 누르기
- 가족이라 자칭해도 바로 돈 보내기

✅ 이렇게 하세요

- "필요하면 직접 방문하겠습니다"라고 답하기
- 공식 대표번호로 다시 걸어 사실 확인하기
- 가족 등 주변 사람에게 먼저 이야기하기
- 의심되면 바로 112 또는 금융감독원 (1332)에 문의

보이스피싱 역할극

1. 검찰 사칭 
2. 경찰 사칭 
3. 은행 직원 사칭 
4. 가족 지인 사칭 
5. 환급금 사칭 

혹시 피해를 입었다면, 즉시 신고하세요!

112

경찰청

피해 신고 및 계좌 지급정지
요청

1332

금융감독원

금융 피해 상담 및 안내

118

인터넷진흥원

스미싱·인터넷 사기 신고

피해 즉시 신고하면 계좌 지급정지로 추가 피해를 막을 수 있습니다.

디지털 상식 OX 퀴즈

가족이라며 급하게 돈을 요구하면, 먼저 전화를 끊고 원래
알던 번호로 다시 확인해야 한다.

O

검찰·경찰은 전화로 '안전계좌'에 돈을 이체하라고 요구하지
않는다

O

비밀번호나 계좌번호는 은행 직원이라고 해도 전화로
알려줘도 된다.

X

AI 기술로 가족의 목소리를 그대로 흉내 낼 수 있다.

O

보이스피싱이 의심되면 112에 신고하면 도움을 받을 수 있다.

O

돈을 이미 보냈어도, 빨리 신고하면 피해를 줄일 수 있는
방법이 있다.

O

오늘의 세 가지 약속

1. 낯선 전화로 급하게 돈을 요구하면 일단 끊고 직접 확인한다
2. 전화·문자로 개인정보와 금융정보는 절대 알려주지 않는다
3. 의심되면 주저 말고 112 또는 금융감독원(1332)에 신고한다