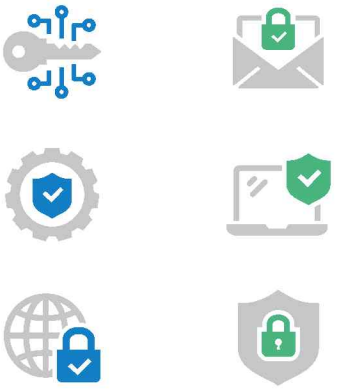
2024 VOL. 07
2024. 10

KISA INSIGHT



국내·외 피싱(Phishing) 대응 현황 및 시사점
: 미국·EU·영국·독일·일본·중국 중심으로

김관영 | 김성훈 |
이광식 | 석지희 | 김은성 | 이동연 |

DIGITAL &
SECURITY
POLICY

KISA 한국인터넷진흥원

CONTENTS

KISA INSIGHT

2024 VOL. 07

DIGITAL & SECURITY POLICY

국내·외 피싱(Phishing) 대응 현황 및 시사점
: 미국·EU·영국·독일·일본·중국 중심으로

한국인터넷진흥원 정책연구팀 김관영 | 김성훈
한국인터넷진흥원 국민피해대응단 이광식 | 석지희 | 김은성 | 이동연 |

『KISA Insight』는
디지털·정보보호 관련 글로벌 트렌드 및 주요 이슈를
분석하여 정책 자료로 활용하기 위해
한국인터넷진흥원에서 기획, 발간하는 심층 보고서입니다.

본문 내용은 한국인터넷진흥원의
공식 견해가 아님을 알려드립니다.

작성·검토

한국인터넷진흥원 정책연구실 정책연구팀

김성훈 팀장 061-820-1426 shkim@kisa.or.kr
김관영 선임연구원 061-820-1474 kwaa_woo7@kisa.or.kr

한국인터넷진흥원 국민피해대응단

이동연 단장 02-405-6640 ryuni@kisa.or.kr
석지희 팀장 02-405-6326 wind0519@kisa.or.kr
김은성 팀장 02-405-5363 eun-sung@kisa.or.kr
이광식 팀장 02-405-4783 kwangsik@kisa.or.kr

자료 조사

넥스텔리전스(주)

김동진 연구위원 070-8666-6133 djkim@nextelli.com
조현도 수석연구원 02-783-3801 nasonyun@nextelli.com

발간일 2024년 10월 30일

기획·발간처 한국인터넷진흥원 정책연구실 정책연구팀

요약

피싱(Phishing)은 대표적인 디지털 민생범죄 중 하나로, 메시지 또는 이메일 등을 악용해 사용자 또는 기업의 정보를 탈취하여 금전적 이득 등을 편취하는 행위

- 피싱의 종류에는 이메일 피싱(E-mail Phishing), 보이스피싱(Voice Phishing), 스미싱(Smishing), 큐싱(Qshing) 등이 있으며, 대표적인 피싱 수단으로 스팸(Spam)이 있음

종류	특징
이메일 피싱 (E-mail Phishing)	• 공격자는 은행이나 온라인 서비스 등 합법적인 출처에서 보낸 것처럼 보이는 사기성 이메일 전송
보이스피싱 (Voice Phishing)	• 전화를 통해 실행되는 피싱으로 통화상으로 긴박감을 조성하여 피해자의 실수를 유도
스미싱 (Smishing)	• SMS를 전송해 수신자를 속여 개인정보 등의 민감한 정보를 탈취
큐싱 (Qshing)	• QR코드를 스캔하면 악성 웹사이트로 연결하거나, 유해한 콘텐츠를 다운로드하도록 유도하는 방식

- 현재 피싱은 우리나라뿐만 아니라 전 세계적으로 발생하고 있는 범죄로, AI 보안 기업 Bolster에 따르면 '20년 이후 피싱 활동은 94% 이상 증가한 것으로 조사·분석됨

국외 주요국은 피싱 등 다양한 디지털 민생범죄로부터 국민을 보호하고, 범죄 예방 및 대응 전담 조직을 구성하여 범죄를 규제하고 관련 정책을 수립·시행

- **(미국)** 연방거래위원회(FTC), 연방통신위원회(FCC), 사이버보안 인프라 보안청(CISA)을 중심으로 피싱 등 범죄 대응 가이드라인 개발, 범죄 처벌 규정 제·개정, 피해자 보호 방안 등 추진
- **(EU)** 유럽연합 집행위원회(EC)를 통해 피싱 등과 같은 사기 행위로부터 소비자를 보호하기 위해 스팸 방지법을 제정 및 개정하고 있으며, GDPR, eIDAS 등을 통해서도 디지털 범죄 규제

- **(영국)** 온라인 사기 전담 조직을 설치함으로써 피싱을 비롯하여, 스미싱 등 범죄 문제에 대해 정부가 적극적으로 해결하고, 피해자를 보호하고자 노력하고 있음
- **(독일)** 연방정보보안청(BSI)을 중심으로 연방금융감독청(BaFi) 등이 협력하여 피싱 예방적 보안 조치 방법, 피해 사례 등의 정보를 공유하고 있으며, 금융사기 예방 등은 BaFi에서 제공
- **(일본)** 경찰청을 중심으로 국민 대상 피싱 예방·대응책을 교육·홍보하여 범죄에 대한 인식을 제고하는 한편 피싱 대책 협의회를 통해 민간 분야의 피싱 대응에 필요한 활동 추진
- **(중국)** '정보통신망 범죄 활동 방조죄'를 신설하는 형법을 '15년에 개정하고, '22년에는 전기통신금융사기 방지법을 제정하여 피싱 등을 범죄로써 강력하게 규제 중

우리나라는 국무조정실을 중심으로 보이스피싱 등 범죄 대응 및 근절하기 위해 범정부 전담팀을 운영하는 동시에 관련 정책을 수립·시행 중

- 국무조정실은 과학기술정보통신부, 방송통신위원회, 경찰청 등과 함께 2021년 '전화금융사기 대응 범정부 전담팀'을 발족하였으며, 통신·금융 대책 마련 및 보이스피싱 범죄에 엄정 대응
- 또한, 과학기술정보통신부와 방송통신위원회에서는 통신 분야 보이스피싱 대응을 위한 대책을 발굴하여 추진하고 있으며, 민·관 협력 및 AI 등 신기술을 활용한 범죄 차단 기술 개발 중

최근 피싱 범죄는 AI 등 新기술의 등장으로 더욱 지능화·고도화되고 있으며, 범죄 수단과 범위가 전 세계로 확대됨에 따라 전담팀 구성 및 글로벌 공조 체계 강화 필요

- 디지털 민생범죄 전담팀 구성을 통해 지능화·조직화하는 디지털 민생범죄 대응 방안과 규제를 강화하고, 해외 IP 우회 등을 대응하기 위한 국제 공조 체계 강화를 통해 기술 연구, 글로벌 대응 방안 마련 등 필요
- 또한 디지털 민생범죄로부터 국민을 보호하기 위한 예방·대응책 마련이 시급하며, 특히 피싱 범죄 전반을 규율할 수 있는 제도 마련 검토 필요

Ⅰ

피싱(Phishing) 개념 및 글로벌 발생 현황

1-1 피싱(Phishing)의 개념

▌피싱(Phishing)은 수신자를 속여 사용자 또는 기업의 다양한 정보*를 공개하도록 유도 또는 탈취하는 기만적인 커뮤니케이션 방법을 포괄적으로 일컫는 용어

* 공개 유도 또는 탈취하는 정보: 주민등록번호, 사용자 아이디, 기업 기밀정보, 금융정보 등

- 피싱의 종류에는 이메일 피싱(E-mail Phishing), 보이스피싱(Voice Phishing), 스미싱(Smishing), 큐싱(Qshing) 등이 있으며 각 기술적 차이로 구분되나, 목적은 정보 탈취 또는 금전적 사기 등으로 동일[1)]

- (이메일 피싱) 공격자는 수신자가 링크를 클릭하도록 유도하는 합법적으로 보이는 이메일을 전송하며, 이 링크를 사용자가 클릭하면 신뢰할 수 있는 사이트와 유사한 사기성 웹사이트로 연결되고, 여기서 수신자는 민감한 정보를 입력하라는 메시지를 받게 되는 구조

- (보이스피싱) 해외에서는 일반적으로 비싱(Vishing)으로 불리는 사기 형태로, 사기 전화 또는 음성 메시지 등을 통해 피해자를 속여 로그인 인증 정보, 신용카드 번호, 은행 정보 등 개인의 민감한 정보를 제공하도록 유도하는 사기이며 전 세계적으로 우리나라가 가장 빈번한 공격 대상이 되고 있음

- (스미싱) 넓은 범주에서 피싱의 일종으로, 문자 메시지(SMS)를 전송해 수신자를 속여 비밀번호, 신용카드 번호 또는 기타 개인정보 등의 민감한 정보를 제공하도록 유도하는 사이버 사기 유형

  - 휴대전화에 SMS를 전송하여 수신자에게 멀웨어를 다운로드하거나 합법적인 기관의 사이트처럼 보이도록 설계된 사기 웹사이트 링크로 접속하여 민감한 개인정보를 입력하도록 유도

1) Experian, What's the Difference Between Phishing, Smishing and Vishing?, 2022.3.20.
Ironscales, Smishing vs Phishing (2024.8.16. 액세스: https://ironscales.com/guides/phishing-prevention/smishing-vs-phishing)

- 전송된 SMS는 일반적으로 심각한 결과를 피하기 위해 즉각적인 조치가 필요하다고 주장하며 긴박감을 조성
  * 예시: 은행 정보를 즉시 인증하지 않으면 은행 계좌가 동결될 것이라는 메시지 등)

• (큐싱) QR코드에 링크된 악성 앱 URL 설치를 유도하여, 개인·금융정보 탈취, 모바일기기 원격 통제, 소액 결제 등 개인정보 유출을 이용한 사기를 유도하는 신종 사이버 범죄 유형

〈표 1〉 피싱(Pishing)의 유형과 특징

유형	특징	예시
이메일 피싱 (E-mail Phishing)	• 공격자는 은행이나 온라인 서비스 등 합법적인 출처에서 보낸 것처럼 보이는 사기성 이메일 전송	• 로그인 자격 증명이나 개인정보를 도용하도록 설계된 가짜 웹사이트로 연결되는 링크가 포함 • 은행에서 보낸 이메일로 가장하여 메시지 내 링크를 클릭하여 계정 상세 정보를 확인
보이스피싱 (Voice Phishing)	• 전화를 통해 실행되는 피싱으로 통화상으로 긴박감을 조성하여 피해자의 실수를 유도	• 공격자가 피해자에게 전화를 걸어 합법적인 기관에서 온 것처럼 가장하여 개인정보를 탈취 • 자녀 납치, 계정 유출 등의 긴박감을 조성하여 현금 인출 등을 유도
스미싱 (Smishing)	• SMS를 전송해 수신자를 속여 개인정보 등의 민감한 정보를 탈취	• 공격자는 은행이나 서비스 제공업체와 같이 신뢰할 수 있는 출처에서 보낸 것처럼 보이는 문자를 전송 • 전송 메시지에는 문자에는 개인정보를 훔치거나 멀웨어를 설치하도록 설계된 사기성 웹사이트로의 연결 링크 포함 • 계정 유출 등의 긴박감을 조성하여 즉각적인 조치를 취하도록 유도
큐싱 (Qshing)	• QR코드를 스캔하면 악성 웹사이트로 연결하거나, 유해한 콘텐츠를 다운로드하도록 유도하는 방식	• 전동킥보드 이용을 위한 QR코드 위에 가짜 QR코드를 덧씌워 연결 유도 후 개인정보 탈취 • 고객 사은 이벤트로 위장한 QR코드 홍보 전단에 삽입하여 연결 유도 • 주차된 차에 '불법 주차 경고장' 딱지를 붙여놓고 QR코드를 통해 벌금을 납부하라고 요구하는 것처럼 가장하여 연결 유도

출처) Experian, Ironscales 등 자료를 기반으로 정리 및 재구성

▌피싱과 유사한 스팸(Spam)이 있으나, 스팸은 일반적으로 수신을 원하지 않는 이용자에게 대량의 메일·문자 메시지·SNS 메시지(DM) 등을 전송하는 행위로 주로 광고·홍보 목적

- 본래 스팸은 저렴한 비용으로 불특정 다수의 이용자에게 대량으로 기업 또는 제품, 서비스를 홍보하는 수단으로 사용되었으나 최근에는 스팸을 통해서도 금전을 목적으로 피싱 사이트 주소 또는 악성코드가 포함된 URL 등을 첨부하는 등의 피싱 행위의 수단으로 악용되는 중

– 스팸이 피싱에 악용됨으로 인해 심각한 경제적 피해를 유발하는 등 민생범죄로 사회적 문제가 되고 있음

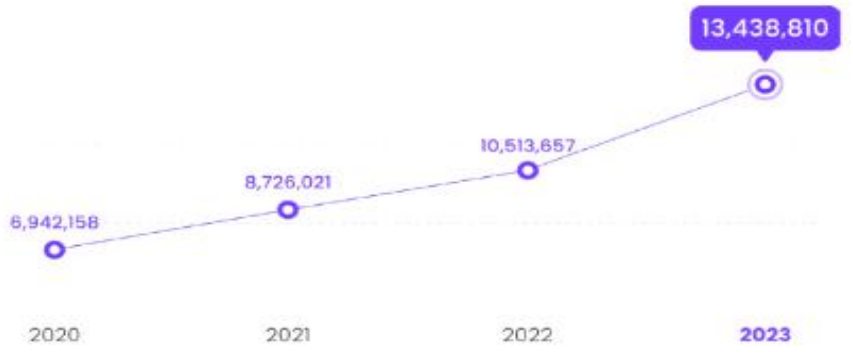
1-2 글로벌 피싱 및 스미싱 발생 현황

피싱(Phishing)

▌AI 보안 기업 Bolster에 따르면 2020년 이후 전 세계적으로 피싱 활동은 94% 이상 증가한 가운데 2023년은 1,343만 개 이상의 사기 사이트가 관측돼 전년 대비 27.8% 증가[2)]

- 가장 활발한 피싱이 관찰되었던 2023년 8월에는 220만 개의 사기 사이트가 탐지

〈그림 1〉 **글로벌 피싱 페이지 통계 추이**



출처) Bolster

2) Bolster, 2024 State of Phishing & Online Scams: Statistics, Facts, Trends & Recommendations, 2024.3.12

▌클라우드 기반 코드 제공 기업인 Spacelift의 자체 조사에 따르면, '23년 한 해 94%에 달하는 조직이 피싱 공격을 경험했으며, 성공한 피싱 공격의 74%는 사람의 실수에 기인[3)]

- 사용자가 피싱 이메일에 속아 넘어가는 평균 시간은 1분 미만

– 이메일을 열어본 후 악성 링크를 클릭하는 데 걸리는 시간의 중앙값은 21초이며, 공격자가 요청하는 정보를 제공하는 데 걸리는 시간은 28초에 불과

– 피싱 공격을 통한 데이터 침해의 동기는 재무적인 이유가 전체 공격이 95%를 차지

〈그림 2〉 글로벌 피싱 주요 동인

출처) Spacelift

- 한편, FBI의 인터넷 범죄 신고 센터(IC3)에 따르면 '13년 10월부터 '22년 12월까지 비즈니스 이메일 침해(BEC)로 인해 508억 달러 규모의 손실이 발생

– BEC에서는 공격자가 직원, 공급업체 또는 기타 신뢰할 수 있는 당사자로 가장하여 대상자를 속여 돈이나 기타 권한 있는 정보를 전송하도록 유도

▌AI 기술의 발달로 인해 피싱 공격 역시 더욱 정교하고 표적화되는 경향을 보이고 있으며 특히, 정찰, 공격 실행, 회피 기법 등 다양한 측면의 작업을 자동화

- AI 알고리즘을 활용하여 방대한 양의 데이터를 분석하고, 취약점을 식별하며, 정확하고 빠르게 취약점을 악용할 수 있게 됐으며, 생성 AI를 기반으로 메시지 내용의 다양성과 자동화를 통해 사회공학 공격이 더욱 교묘해지고 대량의 무차별적인 캠페인 양상을 보이고 있음

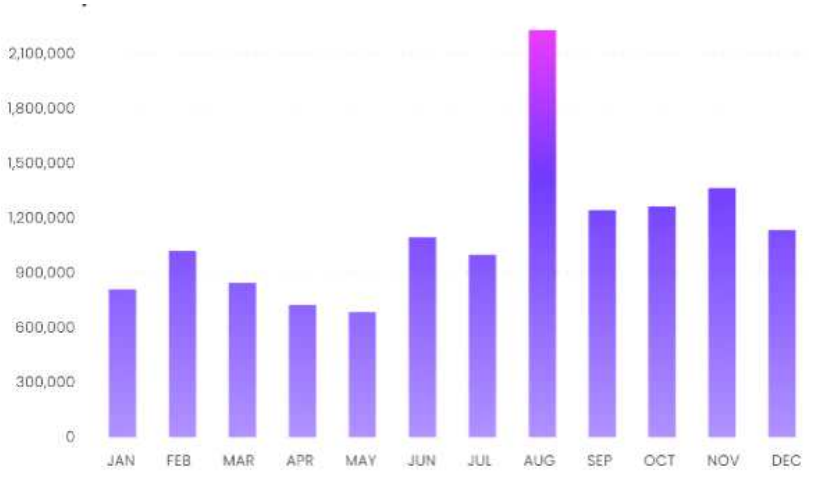
– Spacelift에 따르면, '22년 말 ChatGPT가 출시된 이후 피싱 이메일의 양은 무려 1,265% 증가했으며, 비밀번호 유출을 유도한 피싱은 967% 증가하며 급격한 증가세를 보임

3) Spacelift, Top 54 Phishing Attack Statistics & Latest Trends for 2024, 2024.8.6.

▌불안한 경제 환경에 영향을 입고 있는 기업과 소비자를 대상으로 한 사회공학 피싱 공격이 최근 주요 트렌드를 형성

• Bolster에 따르면, '23년 3월 실리콘밸리은행(SVB)를 포함 일부 중소형 은행들이 파산한 이후 감정적으로 취약해진 은행과 스타트업을 직접 표적으로 삼는 공격이 확산

〈그림 3〉 **2023년 월별 피싱 발생 건수 추이 (단위: 건)**



출처) Bolster

- '23년 금융 위기 하에서 사람들의 심리적 압박감이 고조되는 가운데 피싱 공격은 전년 대비 27.8% 증가
- 특히 코로나 이후 재택근무자가 늘고 해고 사태가 확산하면서, 전 세계적으로 가짜 채용공고를 통해 고객과 기업을 겨냥한 사기도 급증한 것으로 파악

• **미국 연방거래위원회(FTC)와 일본 경시청(警視廳)의 발표에 따르면, 피싱 범죄의 발생이 증가함에 따라 피해가 증가하고 있으며, 특히 금전적 피해 규모가 계속 늘어나는 추세**

- (미국) 피싱 범죄 중 정부 기관을 사칭하여 현금을 탈취한 피해 규모가 '23년 한화 1,004억 원이었으며, '24년 2분기에만 한화 996억 원이 발생하여, 이미 지난해 수준의 피해액이 발생되었다고 발표
- (일본) 전화 등을 이용해 비대면·신뢰를 통해 현금을 탈취하는 범죄(피싱 등)를 포함한 특수사기(特殊詐欺)[4] 범죄로 인한 피해액이 '22년 한화 3,188억 원, '23년 한화 3,892억 원이었으며, 올해도 증가할 것으로 전망

4) 특수사기(特殊詐欺) 정의 : 피의자가 전화, 우편 등으로 친족이나 공공기관의 직원 등을 사칭하여, 보험료/의료비 환급, 현금 인출 카드 부정 사용 등으로 피해자를 속여 현금을 피의자의 계좌로 송금하도록 하는 사기 범죄로 대표적인 범죄로 보이스 피싱, 가상 요금 청구 사기, 예금금 사기, SNS 피싱 등이 있음(출처 : 일본 경시청)

〈그림 4〉 미국 정부 사칭 피해액 및 일본 특수사기범죄 피해액 규모

출처) 미국 FTC 및 일본 경시청 자료 재인용, 한국인터넷진흥원

스미싱(Smishing)

▌BYOD(Bring Your Own Device)와 원격 근무가 증가함에 따라 직장 내 모바일 기기를 사용하는 사람들이 늘어나면서 사이버 범죄자들이 직원의 휴대전화를 통해 회사 네트워크에 쉽게 액세스할 수 있게 돼 스미싱 피해는 날로 증가

- Proofpoint에서 발간한 전 세계 피싱 현황 보고서에[5] 따르면 보고서 작성을 위해 실시된 설문조사에 참여한 기업 중 71%가 '23년 1회 이상의 피싱 공격을 경험하였다고 답변

– 이번 조사로 '22년의 피싱 경험률(84%) 대비 다소 감소하였지만, 여전히 피싱이 발생하고 있으며, 피싱으로 인한 피해(금전적 피해('22년 대비 144% 증가), 기업의 평판 하락('22년 대비 50% 증가)는 증가한 것으로 확인

– 또한 본 보고서에 따르면 '23년에 발생된 모바일 위협 중 스미싱이 전체의 39%를 차지하고 있음

– 매달 1,000만 건의 전화 기반 공격 전송(TOAD, Telephone-Oriented Attack Delivery)이 이뤄졌으며, 이를 통해 피해자는 민감한 정보와 자격 증명을 공개하도록 유도

5) Proofpoint, 2024 State of the Phish, 2024

• 미 연방통신위원회(FCC)에 보고된 스미싱 시도 건 수는 '19~'22년까지 꾸준히 증가하였으나, '23년에는 다소 감소하는 추세를 나타내고 있음[6)7)]

〈표 2〉 FCC 접수 원치 않는 문자 메시지 불만 건 수

2019	2020	2021	2022	2023
5,700	14,000	15,300	18,900	11,900

출처) FCC

• 사용자들은 다른 형태의 커뮤니케이션 대비 상대적으로 문자를 더 신뢰하는 경향이 있기 때문에 사이버 범죄자들에게 스미싱은 유용한 공격 수단을 제공

– 실제로 Gartner, FCC 조사에 따르면 사람들은 문자의 45%에 응답하는 반면 이메일은 6%만 응답[8)]한 것으로 확인

▌여타 사회공학 공격과 마찬가지로 스미싱 역시 신뢰할만한 기관을 사칭하여 SMS 수신자에게 불안과 긴박감을 느낄만한 거짓 상황을 설정하여 접근한 뒤 개인정보를 탈취하거나 재무적인 피해를 주는 수법을 주로 활용

• 스미싱 범죄자들은 주로 금융기관, 정부, 고객 지원 서비스, 배송업체, 상사나 동료 등을 사칭하여 피해자에게 접근한 뒤 계좌정보 탈취나 현금 송금 등을 유도

• 이외, 잘못된 번호로 문자를 보내는 척한 뒤 대화를 이어가며 피해자와의 유대감을 형성하여 금전적인 피해를 일으키거나, 피해자의 지인으로 위장하여 접근한 뒤 다단계 인증을 위한 인증 코드나 일회용 비밀번호를 탈취하여 계정을 해킹하는 등의 교묘한 유형도 확산[9)]

6) Bank of America, Five tips to help avoid smishing scams(2024.8.17. 액세스: https://business.bofa.com/en-us/content/what-is-smishing-how-to-prevent-it.html#1)
Heimdal, There Is an Increase in Smishing Attacks, FCC Warns, 2023.10.19
7) FCC, FCC ADOPTS ITS FIRST RULES FOCUSED ON SCAM TEXTING, 2023.3.16
8) Gartner, The Future of Sales Follow-Ups: Text Messages, 2019.10.4
9) IBM, What is smishing (SMS phishing)?, 2024.6.10

〈표 3〉 최근 주요 대량 스미싱 사건 발생 현황

시기	스미싱 사건	주요 내용
2023	Apple ID 복구 사기	• 사기 문자를 통해 수신자에게 가짜 링크를 전달, 비밀번호 변경을 요청하여 iCloud 계정에 대한 무단 액세스를 경고
	영국 국세청(HMRC) 세금 사기 경고	• HMRC에는 사기성 세금 환급 제안을 받았다는 문자와 이메일이 '23.9월까지 1년간 13만 건 이상 접수
2022	UPS 문자 사기	• UPS에서 보낸 것이라고 주장하는 사기성 SMS 메시지를 통해 소포 배송을 알리고 피해자는 제공된 링크를 통해 재무적 손실을 야기 • '22년 한 해 동안 UPS 사기 문자로 인한 피해 손실은 3억 3,000만 달러 규모에 이름
	OCBC 은행 SMS 피싱	• 사기범들의 은행 사칭 SMS 피싱으로 인해 약 470명의 OCBC 은행 고객으로부터 최소 850만 달러 규모의 손실 발생
2021	Amazon 사칭	• 미국 소비자들을 대상으로 아마존을 사칭하여 의심스러운 계정 활동이나 배송 지연에 대해 경고하는 내용의 사기 문자를 대규모로 발송하여, 악성 링크 클릭을 유도 • '21년 미국 소비자들의 스미싱 피해액은 약 58억 달러로, 그 중 아마존 사칭 패턴의 사기가 상당 부분을 차지
	싱가포르 은행 스미싱 공격	• 싱가포르 은행 고객을 대상으로 한 스미싱 공격으로 790명의 피해자가 발생, 1,370만 싱가포르 달러의 손실을 야기

출처) 각 언론보도 내용 재정리

1-3 국내 피싱 발생 현황

▌AI, 차세대 네트워크(5G, 6G) 등 新기술의 보편화 및 ICT 고도화로 국내에서도 피싱으로 대표되는 디지털 민생범죄가 지능화·고도화되고 있으며, 국민과 국가의 안전 위협 증가

- 이러한 변화와 발전으로 인해 국민과 국가의 안전이 위협받고 있으며, 디지털 민생범죄 역시 범죄 기법과 수단이 고도화되고, 발생률이 증가하면서 국민 일상에 심각한 위협이 되고 있음

– 특히, 보이스피싱으로 인한 피해액은 '23년 1,965억 원 규모로 이는 '22년에 비해 약 35%가 증가하는 등 국민의 경제적·심리적 피해를 매년 가중시키고 있음[10)]

10) 금융감독원, "2023년 보이스피싱 피해 현황 분석", 2024

▌국내는 올해 상반기에만 스미싱 탐지 건수가 88만여 건에 이르고, 보이스피싱도 1만여 건이 발생하는 등 피싱 범죄가 다시 심각한 사회문제로 대두되고 있음

- 다수의 국민들에게 대량 유포되어 심각한 금전 피해까지 유발하는 스미싱은 정부와 통신사의 긴급 차단 시행으로 인해 '22년 탐지 건수가 대폭 줄었으나, '23년부터는 스마트폰을 악성앱에 감염시켜 개인 연락처에 저장된 지인들에게 부고장 스미싱 문자를 발송하는 등 사칭유형이 계속적으로 증가하고 있음

- 올해 상반기 보이스피싱 발생 건수는 10,053건으로 지난해 전체 발생 건수(18,902건)의 절반 수준을 이미 넘어서며 줄어들었던 보이스피싱 범죄가 다시 증가하는 추세로 전환

- 피싱으로 인한 피해층은 주로 고령층의 피해가 컸으나 경제 사정이 어려운 청년층을 대상으로 대출을 빙자한 사기를 저지르는 등 보이스피싱 수법과 대상이 점차 다양화됨에 따라 점차 피해가 확대되는 경향이 있음

〈그림 5〉 **최근 5년간 스미싱 탐지 및 보이스피싱 발생 현황**

출처) 한국인터넷진흥원, 경찰청 자료 재정리

II

미국·EU 등 주요국 피싱 대응 현황

2-1 미국

정책적 대응 현황

▌미국은 주요 연방 규제기관인 연방거래위원회(FTC), 연방통신위원회(FCC) 및 사이버보안 전담 기관인 사이버보안 인프라보안청(CISA)이 주축이 되어 피싱과 스미싱 예방 대응책 마련을 추진 중

- FTC는 사기나 기만 등의 기업 관행으로부터 소비자를 보호하는 역할을 하는 한편, FCC는 통신 네트워크 및 서비스를 통한 각종 사기를 근절하기 위해 각각의 소관 법률 및 규정을 적용
- CISA는 대국민 의식 환기와 대응 가이드라인 개발 및 관계 당국 간 정보 공유 활동 등을 통해 피싱/스미싱 확산에 대응

▌FTC는 독점 금지법을 집행하고 소비자 보호를 증진하기 위한 연방정부의 독립 기구로, 사기, 기만, 불공정 비즈니스 관행을 방지하는 업무를 담당

- FTC는 컴퓨터사기남용법(CFAA, The Computer Fraud and Abuse Act)[11]에 따라 피싱 공격으로부터 소비자 정보를 보호하기 위해 기업이 합리적인 보안 조치를 구현하는지 여부를 감독하며, 피싱 행위에 대한 조사와 함께 가해자를 상대로 민사 소송을 제기할 수 있음

  – 컴퓨터 사기는 승인 없이 또는 승인 범위를 초과하여 보호 대상 컴퓨터에 액세스하는 행위로 정의(a)(1)

11) – 18 U.S. Code § 1030 – Fraud and related activity in connection with computers

- 구체적으로 CFAA는 컴퓨터 스파이 행위, 개인 또는 공용 컴퓨터에 대한 컴퓨터 침입, 컴퓨터를 이용한 사기 행위, 악성 코드 배포, 비밀번호 거래, 보호 대상 컴퓨터를 손상시키겠다고 협박하는 행위 등을 금지(a)(4)/(5)/(6)
- 이에 따라, 계좌 번호, 주민등록번호, 비밀번호 등의 개인정보 수집을 시도하는 이메일, 데이터 마이닝에 관여하기 위해 스파이웨어 또는 멀웨어를 설치하는 행위 등 피싱 역시 CFAA의 적용 범주에 포함

• **신원 도용 및 가정 억제법[12]에서는 다른 사람의 신원 확인 수단을 고의로 양도하거나 사용하는 것을 연방 범죄로 규정(Sec. 003(a)(7))**

- 이 법에 따라 신원 도용에 대해 사기 행위를 통해 얻은 가치에 따라 3년에서 25년 사이의 징역형에 처해질 수 있음
- 이 법은 FTC를 신원 도용 민원 접수를 위한 총괄 처리 기관으로 지정함에 따라, FTC는 민원을 기록 및 승인하고, 피해자에게 관련 정보를 제공하며, 민원을 적절한 기관에 의뢰할 책임을 부여받음
- 피싱 활동의 경우, 개인 식별 정보의 무단 사용과 관련될 시 이 법의 규정에 따라 처벌될 수 있음

• **'24.2월, FTC는 AI 기반 개인 사칭 범죄 보호를 위한 새로운 규정[13]을 확정**

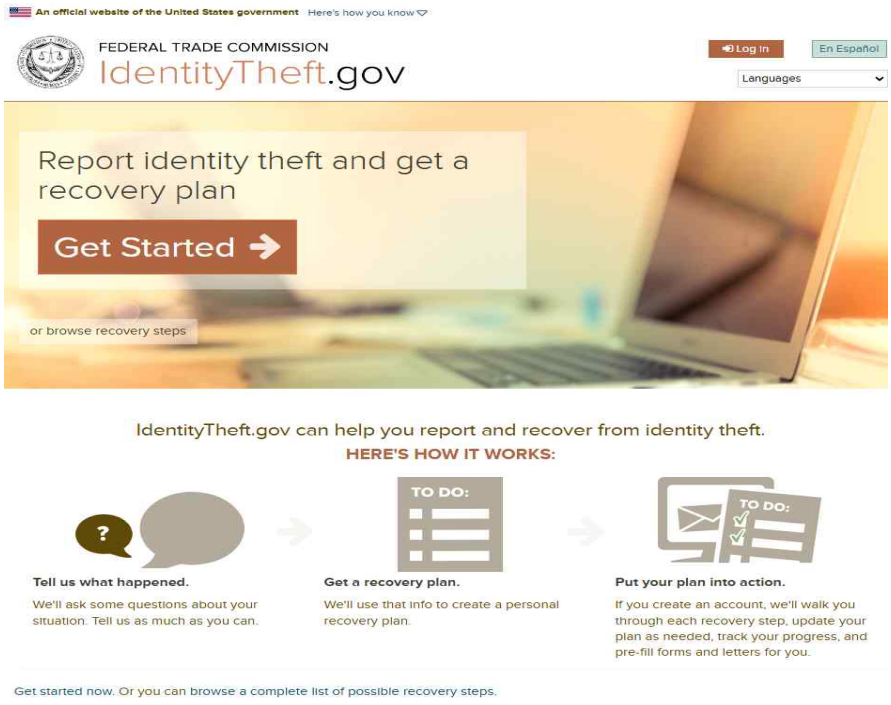
- 이 규정에서는 직접적으로 또는 암시적으로 정부 기관 또는 그 임원을 사칭하거나, 정부 기관 또는 임원과의 관계를 허위로 표시하는 행위를 규정 위반 및 FTC법상 불공정하거나 기만적인 행위 또는 관행으로 규정
- 이에 따라 정부 또는 기업 이메일 또는 웹 주소를 스푸핑하는 행위, 정부 기관 또는 기업과의 관계를 허위로 주장하는 보이스피싱 행위 등이 동 규정의 처벌 범위에 해당되게 됨

• **FTC는 도메인 내 복수의 웹사이트를 통해 피싱 관련 정보 제공과 피싱 피해 발생에 따른 후속 조치와 관련된 절차를 안내**

- FTC는 피해자가 피싱으로 인한 신원 도용을 신고하고 복구하는 데 필요한 절차를 제공하는 identitytheft.gov 웹사이트를 운영하고 관리하고 있음
- 또한, FTC는 피싱 사기, 피싱 사기 인식 방법 및 피해 방지 방법에 대해 대중에게 교육하기 위한 다양한 자료를 제공 중[14]

12) The Identity Theft and Assumption Deterrence Act of 1998
13) Trade Regulation Rule on Impersonation of Government and Businesses https://www.ftc.gov/news-events/news/press-releases/2024/02/ftc-proposes-new-protections-combat-ai-impersonation-individuals
14) https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/phishing

〈그림 6〉 FTC 피싱 피해 복구 안내 사이트



출처) FTC

▌방송통신 규제 기관인 연방통신위원회(FCC)는 전화소비자보호법(TCPA), 문자 메시지 규정, 발신자 번호 스푸핑(Spoofing)[15] 규정 등의 통신 서비스 관련 법률과 규제를 통해 피싱과 스미싱 문제에 대응하고 소비자를 보호하는 역할을 담당

- FCC는 1991년에 제정된 전화소비자보호법(TCPA, The Telephone Consumer Protection Act)에 따라 음성통화, SMS 등을 활용한 텔레마케팅 통신을 제한하여 소비자 개인정보를 보호하는 역할을 담당

  – TCPA는 보이스피싱이나 스미싱에 활용될 수 있는 자동 전화 발신 및 자동 음성 메시지 발송이나 텔레마케팅 전화 사용에 대한 규제 조항을 마련

- '23.3월, FCC는 이동통신 서비스 사업자에게 미사용, 미할당 또는 유효하지 않은 전화번호에서 온 문자 메시지 등 불법일 가능성이 높은 자동 문자 메시지에 대해 차단 조치하는 것을 의무화[16]

15) 스푸핑(Spoofing) : 공격자가 네트워크, 웹사이트 등 데이터 위·변조를 통해 정상 시스템인 것처럼 위장하여 일반 사용자를 속이는 해킹 기법으로 주로 네트워크 시스템의 IP 주소, DNS 등을 위·변조함(출처: TTA 정보통신용어사전)

• FCC는 로보콜, 스푸핑 사기(Caller ID Spoofing) 방지의 일환으로 자사 홈페이지를 통해 한국어, 스페인어, 중국어, 타갈로그어, 베트남어 등 다국어로 된 원치 않는 전화 및 문자 거부 관련 정보 및 동영상 제공 캠페인을 실시[17]

– 로보콜 웹사이트에는 로보콜 FAQ, 자동 발송 문자, 스푸핑, 수신 금지(Do Not Call) 목록, 수신 차단 관련 정보 등의 메뉴를 제공[18]

• 이외 FCC는 웹사이트를 통해 신종 피싱 및 스미싱 수법에 대한 소비자 경고(Frauds, Scams and Alerts)를 발행[19]

▌피싱 등의 공격으로부터 개인과 조직을 보호하기 위해 교육, 대응책 수립 및 부처 협업 업무를 담당하는 CISA는 국가안보국(NSA), 연방수사국(FBI), 다국가 정보공유·분석센터(MS-ISAC)와 공동으로 피싱 대응 지침[20]을 마련

〈표 4〉 미국 CISA 주도 발간 피싱 대응 지침 주요 내용

주요 목차	주요 내용
피싱 기법	• (로그인 자격 증명 획득) 악성 공격자는 초기 네트워크 접속을 위해 로그인 자격 증명 탈취 • (멀웨어 배포) 멀웨어 배포를 통해 시스템을 방해하고 접근 권한을 상승시키며 교란 상태의 지속성을 유지
완화 조치	• (이메일 필터링) 피싱 이메일을 탐지하고 차단하기 위해 고급 이메일 필터링을 실행 • (사용자 교육) 사용자가 피싱 시도를 인식할 수 있도록 정기적 교육 실시 • (다요소 인증): 다요소 인증을 적용하여 보안 계층을 강화
사고 대응 조치	• (탐지, Detection) 피싱 공격의 징후를 모니터 • (격리, Containment): 감염된 시스템을 격리하여 추가 피해를 방지 • (제거, Eradication) 피싱 이메일 및 멀웨어 제거 • (복구, Recovery) 백업을 통해 시스템 및 데이터 복원

출처) CISA

16) FCC, Targeting and Eliminating Unlawful Text Messages Report and Order and Further Notice of Proposed Rulemaking, 2023.3.17
17) https://www.fcc.gov/robocalls/korean
18) https://www.fcc.gov/spoofing
19) https://www.fcc.gov/general/frauds-scams-and-alerts-guides
20) CISA, Phishing Guidance: Stopping the Attack Cycle at Phase One, 2023.10.18

• 이 가이드는 악의적인 공격자의 피싱 기법에 대한 상세한 인사이트와 피싱 시도를 방지하기 위한 기술적 완화 조치 및 사고 대응 모범 사례를 제시

– 가이드는 여러 분야의 중소기업과 소프트웨어 개발사에 이르기까지 다양한 유형의 조직이 피싱 위협으로부터 시스템을 보호하기 위한 원스톱 리소스를 제공

기술적 대응 현황

▌미국은 FCC가 주축이 되어 산업계와 공동으로 발신자 스푸핑 문제를 해결하기 위한 STIR/SHAKEN 표준을 개발했으며, 현재 FCC가 이 표준의 산업계 실행을 감독 중[21)]

• STIR(Secure Telephone Identity Revisited)은 발신자의 신원과 발신자 번호 정보의 무결성을 암호화 방식으로 검증하는 방법을 제공하는 프레임워크로, 디지털 인증서를 사용하여 발신자의 신원을 인증하고 표시된 발신자 번호 정보가 실제 발신 전화번호와 일치하는지 확인

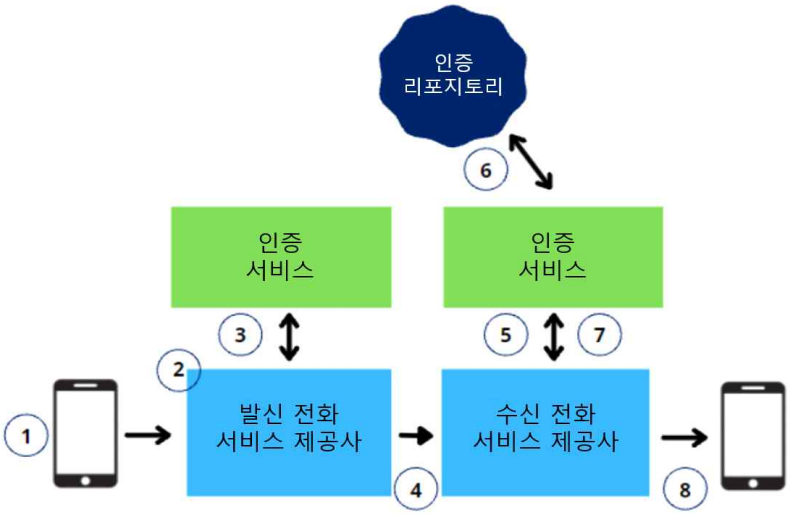
• SHAKEN(Signature-based Handling of Asserted information using toKENs)은 음성 서비스 제공업체가 STIR 프레임워크를 구현하기 위한 표준으로, 실제 전화 네트워크에서 STIR을 적용하는 방법에 대한 기술적 세부 사항과 프로세스를 정의

• STIR/SHAKEN은 전화를 걸면 발신 서비스 제공업체는 발신자의 신원을 인증하고 발신자 ID 정보에 디지털 서명을 첨부하며, 수신 서비스 제공업체는 디지털 서명을 확인하여 발신자 번호 정보가 스푸핑되지 않았는지 확인

– 이 확인 프로세스는 전화가 연결되는 동안 실시간으로 이루어지기 때문에, 발신자 번호 스푸핑을 차단하여 공격자는 사기 공격에서 흔히 활용되는 방식인 신뢰할 수 있는 조직이나 개인을 사칭하는 형태의 피싱 및 스미싱으로부터 이용자를 보호

21) https://www.fcc.gov/call-authentication

〈그림 7〉 STIR/SHAKEN 동작 순서 개념도



출처) Simplicity VoIP[22)]

• '20년부터 FCC는 통신사들에게 STIR/SHAKEN 프로토콜 채택을 의무화하기 시작

- 이 규칙 적용으로 인해 사기 전화 차단 및 대응 기능이 한층 강화된 반면, 문자 메시지에는 이러한 효과가 없음
- 따라서, STIR/SHAKEN 프로토콜 채택 의무화 이후 기존의 보이스피싱 공격은 스미싱 공격으로 초점을 옮기게 되는 상황이 발생

22) https://knowledgebase.simplicityvoip.net/knowledge/what-is-s

2-2 EU

정책적 대응 현황

EU는 2006년 스팸방지법[23] 통과 이후에도 불법적인 이메일과 문자, 스파이웨어 등의 문제가 지속적으로 확산되는 가운데 관련 법령 개정과 연구기술 프로그램 개시 및 ENISA 등의 전담 조직에 의한 피싱 및 스미싱 대처 노력이 강화

- 유럽연합 집행위원회는 규제 당국과 이해관계자들에게 스팸, 스파이웨어 및 악성 소프트웨어 퇴치 노력을 촉구
- 연구 개발 프로그램을 통해 피싱 및 스미싱 관련 위협에 대한 대처 역량 확보와 함께 산업계를 대상으로 한 규제 조치를 강화

〈표 5〉 EU 피싱 및 스미싱 대처 관련 정책 및 규제 조치 현황

추진 주체	정책/규제	주요 내용
유럽연합 집행위원회 (EC)	2006 스팸 방지법	• 피싱 및 스미싱 침해에 대한 처벌 관련 새로운 규칙 제안: 개인정보 보호 및 보안에 관한 규칙 강화
	GDPR	• 피싱 및 스미싱공격에 수반되는 개인정보 처리 및 보호에 대한 엄격한 규칙 수립
	NIS 지침	• 피싱 및 스미싱 공격의 표적이 될 수 있는 통신 및 금융 부문 등의 주요기반시설 운영자를 위한 보안 및 보고 요건을 규정
	eIDAS 규정	• 안전하고 신뢰할 수 있는 전자 식별 및 신뢰 서비스를 위한 프레임워크
	Horizon Europe	• 피싱 탐지 및 예방 및 피싱 공격 해부학 연구 추진 • 피싱 보호 프레임워크 및 정책 개발
유로폴	No More Ransom	• 랜섬웨어 피해자가 범죄자에게 돈을 지불하지 않고도 암호화된 데이터를 복구할 수 있도록 지원
EU정보보안원 (ENISA)	EU 전자 네트워크 보호	• 피싱 및 스미싱 위협 대응 위한 유럽 정보 공유 및 경보 시스템의 실행 가능성을 검토

출처) 한국인터넷진흥원

23) EU, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on fighting spam, spyware and malicious software, 2006.11

▌유럽연합 집행위원회는 2006년 스팸방지법을 통해 개인정보 보호 및 보안에 관한 규칙을 강화하고 침해에 대한 처벌의 심각성에 관한 새로운 규칙을 제안

- (소비자보호) 전자 통신 부문에서 피싱 및 스미싱과 같은 사기 행위나 스팸에 대한 소비자 보호 조치를 강화할 필요성을 인식, 소비자가 이러한 유형의 사기를 식별하고 피할 수 있도록 서비스 제공업체의 투명성 및 정보 요건을 강화할 것을 제안

- (보안 요건) 전자 통신 네트워크 및 서비스의 보안과 무결성을 보장하는 것이 중요하다는 점을 강조하며, 피싱 및 스미싱 공격의 위험을 완화하기 위한 적절한 기술·조직적 조치를 구현하기 위해 서비스 제공업체에 보안 요건을 의무 도입할 것을 제안

▌GDPR, eIDAS, NIS 지침 등 개인정보보호 및 사이버보안 관련 주요 법령 및 지침을 통해 직간접적으로 피싱·스미싱 관련 규정을 제공

- (GDPR) '18년에 발효된 GDPR은 피싱 또는 스미싱 공격을 통해 얻을 수 있는 데이터를 포함한 개인정보 처리 및 보호에 대한 엄격한 규칙을 수립

  – 피싱·스미싱에 따른 기업 데이터 유출 방지를 위해 적절한 보안 조치를 시행하도록 요구

- (NIS 지침) '16년에 채택된 NIS 지침은 피싱 및 스미싱 공격의 표적이 될 수 있는 통신 및 금융 부문 등의 주요기반시설 운영자를 위한 보안 및 보고 요건을 규정

  – 동 지침에 따라 주요기반시설 운영자는 보안 조치를 이행하고 국가 당국에 사고 보고를 의무화

- (eIDAS 규정) '14년에 도입된 eIDAS 규정은 전자 서명 및 전자 스탬프와 같은 안전하고 신뢰할 수 있는 전자 식별 및 신뢰 서비스를 위한 프레임워크를 제시

  – eIDAS 메커니즘은 온라인 거래 및 커뮤니케이션의 진위 여부를 확인하여 피싱 및 스미싱 공격을 예방하고 탐지

〈표 6〉 EU 피싱 및 스미싱 대처 관련 정책 및 규제 조치 현황

법률/규정	조항	주요 내용
GDPR	제32조 처리의 보안	• 조직은 무단 또는 불법 처리에 대한 보호를 포함하여 데이터 보안을 보장하기 위해 적절한 기술적 및 조직적 조치를 구현해야 함
	제33조/34조 개인정보 침해 통지	• 조직은 피싱으로 인해 개인정보 침해가 발생한 경우 감독 기관 및 영향을 받은 개인에게 데이터 침해 사실을 보고해야 함
	제25조 설계 및 기본설정에 의한 개인정보 보호	• 조직은 설계 단계부터 시스템에 데이터 보호 조치를 구현함으로써 피싱 공격에 대한 방지책을 마련
NIS 지침	제14조	• 필수 서비스 운영자는 네트워크 및 정보 시스템에 영향을 미치는 사고의 영향을 예방하고 최소화하기 위해 적절한 보안 조치를 취해야 함
	제16조	• 디지털 서비스 제공업체는 네트워크 및 정보 시스템에 영향을 미치는 사고를 파악하고 적절한 조치를 취하여 사고의 영향을 예방하고 최소화해야 함
eIDAS 규정	제8조	• 전자 식별 수단에 대한 보증 수준을 정의함으로써, 피싱을 통한 신원 도용 방지 기여
	제19조/24조	• 신뢰 서비스 제공업체에 피싱 공격에 대한 보호를 포함하여 보안 위험을 관리하기 위한 적절한 기술적 및 조직적 조치를 취할 것을 의무화

출처) 각 법률/규정 조항 각호 정리

EU 정보보안원(ENISA)은 보안 분야의 업무 및 기술적 전문성을 바탕으로 불법적인 온라인 활동 대처와 관련된 중요한 역할을 담당

• '19년에 채택된 유럽 사이버보안법을 통해 ENISA의 위상과 역할이 강화

- (상설 조직화) ENISA는 이전의 임시 지위를 대신하여 상설 조직의 권한을 부여받음으로써, 장기적인 계획을 수립하고 EU 전체에 걸쳐 보다 일관된 사이버보안 노력을 기울일 수 있게 됨
- (사이버보안 인증 프레임워크) ENISA는 ICT 제품, 서비스 및 프로세스에 대한 유럽 사이버보안 인증 프레임워크를 개발하고 유지하는 데 있어 핵심적인 역할을 수행

- (조정 기능 강화) EU 기관, 기관 및 회원국 전반의 사이버보안 노력을 조정하는 기관의 역할이 강화
- (인식 제고) EU 시민과 조직을 대상으로 사이버보안 인식과 교육을 증진하는 ENISA의 역할이 확대
- (국제 협력) 사이버보안 문제에 대한 국제 파트너와의 협력을 강화하는 임무를 담당
- (연구 및 혁신) ENISA는 EU 차원의 사이버보안 연구 필요성과 우선순위를 파악하기 위한 역할 강화

• 유럽연합 집행위원회는 ENISA를 통해 전자 네트워크에 대한 위협에 대응할 수 있는 유럽 정보 공유 및 경보 시스템의 실행 가능성을 검토 중

- 해당 시스템은 EU 회원국 및 관련 조직 간에 사이버보안 위협 인텔리전스 및 경고를 신속하게 공유할 수 있도록 실시간 정보 교환 거버넌스 구축, 정보 표준화 형식 정의, 위협 데이터 분석 및 의사 결정 지원 도구 개발 등이 포함될 것으로 예상

유로폴의 랜섬웨어 피해자가 범죄자에게 돈을 지불하지 않고도 암호화된 데이터를 복구할 수 있도록 지원하기 위한 No More Ransom 이니셔티브를 실시[24)]

• 본 이니셔티브는 '16.7월부터 유로폴 산하의 유럽사이버범죄센터가 McAfee, Kaspersky 등 민간 유력 보안 기업 및 국제 조직들과 공동으로 추진[25)]

• 다양한 유형의 랜섬웨어에 대한 복호화 도구 저장소와 무로 암호 해독 도구를 제공하여 피해자가 대가를 지불하지 않고도 데이터에 다시 액세스할 수 있도록 지원

- 현재 No More Ransom은 전 세계 170개 지원 기관이 참여하여 37개 언어로 리소스가 제공되고 있으며, 600만 명 이상의 피해자를 지원
- No More Ransom의 리소스는 150개 이상의 랜섬웨어에 대해 120개 이상의 암호 해독 도구를 제공

24) Europol, No More Ransom - do you need help unlocking your digital life?, 2021.12.6
25) 설립 파트너(founding partners)에는 Europol, Politie, kaspersky, McAfee가 포함됐으며, 후속 파트너(following partners)에는 AWS, Barracuda가 포함. 이외 다수의 참여 파트너(associate partners)도 참여 중으로 여기에는 한국인터넷진흥원도 포함

기술적 대응 현황

▌제6차 연구 프레임워크 프로그램(FP6)[26] 이후 유럽연합 집행위원회는 이해관계자들이 스팸 및 기타 형태의 악성 소프트웨어에 대응할 수 있도록 다양한 연구 개발 프로젝트 추진에 착수

- (멀웨어 차단을 위한 연구 커뮤니티 설립) 멀웨어(Malware) 차단에 특별히 초점을 맞춘 연구자, 학계 및 업계 전문가 네트워크를 구축
  - 피싱 공격에 사용되는 멀웨어를 비롯한 다양한 형태의 멀웨어를 탐지, 분석 및 완화하기 위한 협업을 촉진하고 지식을 공유하며 새로운 전략을 개발
- (유럽 인프라 개발 모니터링) 유럽 전역의 인터넷 트래픽을 모니터링하기 위한 종합적인 시스템을 구축
  - 피싱 또는 기타 사이버 공격을 나타낼 수 있는 패턴과 이상 징후를 탐지하고, 새로운 위협에 대한 조기 경보 제공
  - 공격 동향 및 방법에 대한 데이터 제공을 통한 연구 지원 및 유럽의 전반적인 사이버보안 태세 강화
- (적응형 피싱 필터 개발) 새롭고 빠르게 진화하는 공격에 대응하기 위한 보다 정교하고 동적인 피싱 방지 기술을 개발
  - 적응형 피싱 필터 기술 개발 과제에는 △피싱 시도 패턴을 식별하는 머신러닝 알고리즘 △의심스러운 활동을 탐지하기 위한 행동 분석 △자연어 처리를 통한 메시지 콘텐츠 분석 △새로운 위협 인텔리전스를 기반으로 한 실시간 업데이트 등이 있음

▌FP9과 최근 Horizon Europe 프레임워크 하에서는 사기 방지 기술 지원, 모의 테스트 기반 사용자 인식 제고, 사이버보안 인증 프레임워크 개발 등의 활동이 이뤄지고 있음[27]

- (사기 방지 기술 지원 및 교육: EUAF[28]) EUAF는 EU의 재정적 이익에 영향을 미치는 사기, 부패 및 기타 불법 행위 방지를 위한 활동을 지원(2021)

26) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM:i23012&frontOfficeSuffix=%2F
27) EOS-EU, Recommendations on the Future of Security Research Towards Framework Programme 9 https://pes.cor.europa.eu/legislativeworks/horizon-europe-framework-programme-9-research-and-innovation
28) The Union Anti-Fraud Programme, https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/programmes/euaf

- EUAF는 유럽 사기 방지 사무소(European Anti-Fraud Office, OLAF)에서 프로젝트를 관리하며, 전문 교육 및 연구 활동 등을 지원
- 전문 장비, 도구 및 데이터 기술의 획득을 주요 목적으로 하는 프로젝트에 대한 기술 지원을 제공하며, 구매 장비의 사용에 대한 교육도 함께 제공
- 기술 지원은 △조사 및 감시 장비 및 방법 △디지털 포렌식 하드웨어 △데이터 분석 기술 및 데이터 구매 △불법 거래 탐지 등의 4가지 영역의 활동으로 구성
- EUAF는 '21~'27년 동안 1억 1,420만 유로의 예산이 책정

• **(모의 테스트를 통한 사용자 인식 제고: EDIH.SH[29]) EDIH.SH는 독일 슐레스비히 홀슈타인 지역의 디지털 혁신과 변화를 촉진하기 위한 핵심 이니셔티브로, EU와 독일 정부로부터 자금을 지원받아 피싱 모의 테스트를 통해 사용자 인식을 제고(2024)**

- (주요 서비스) EDIH.SH는 AI, 고성능 컴퓨팅(HPC), 사이버보안, IoT, 센서 기술 및 상호 운용성 등을 중점 분야로 설정하여, 각 분야에 대해 혁신평가, 테스트 및 프로토타이핑, 교육 및 네트워킹, 자금 조달 및 지원 등의 서비스를 제공
- (모의 피싱 테스트) EDIH.SH는 실제와 매우 유사한 피싱 이메일을 ChatGPT를 통해 개발, 지정된 수신자 목록을 사용하여 현장 서비스에서부터 경영진에 이르기까지 모든 관련 직원에게 발송한 다음, 테스트 결과에 따라 자격 인증 조치와 교육을 실행[30]

• **(보안 프레임워크 및 정책: EU 사이버보안인증 프레임워크[31]) '19년 사이버보안법에 따라 추진 중인 EU의 사이버보안인증 프레임워크는 EU 차원에서 제품, 서비스 및 프로세스가 특정 요구 사항을 준수하는지 여부를 판단하기 위해 적합성 평가 기준을 제공(2024)**

- 현재 ICT 제품을 대상으로 하는 'EUCC', 클라우드 서비스를 대상으로 한 'EUCS' 및 5G 네트워크에 관한 'EU5G'의 3가지 사이버보안 인증 제도가 개발 중

29) The European Digital Innovation Hub Schleswig-Holstein https://european-digital-innovation-hubs.ec.europa.eu/knowledge-hub/success-stories/phishing-awareness-learning-through-realistic-simulation

30) 이메일에 제공된 링크를 통해 Google 드라이브에 저장된 것으로 추정되는 디자인의 실현 가능성에 대해 질의하나, 실제로는 Google 드라이브 링크 대신 다른 사이트로 연결되는 하이퍼링크가 포함시킴. 각 피싱 이메일에는 익명화된 식별자, 즉 각 개인에게 고유한 임의의 문자열이 포함되어 있어 개인정보 보호를 위해 신원을 밝히지 않고도 이메일의 링크를 클릭한 사람 수를 확인할 수 있음. 테스트 결과 75%의 직원이 피싱 이메일을 클릭한 것으로 확인

31) https://www.enisa.europa.eu/topics/certification/cybersecurity-certification-framework

- 사이버보안 인증 프레임워크는 보안 표준 개선, 디지털 서비스 신뢰도 증가, ID 접근 관리, 이메일 보안, 웹브라우저 보안, 사이버보안 인지도 개선 및 교육 등에 관한 기준을 제시함으로써 직간접적으로 피싱 대책 마련을 위한 다양한 기술 및 제도적 수단을 제공

〈표 7〉 EU 피싱 및 스미싱 대처 관련 연구 및 기술 이니셔티브 적용 현황

추진 과제	이니셔티브명	주요 내용
사기 방지 기술 지원 및 교육	EUAF	• 사기, 부패 및 기타 불법 행위 방지를 위해 △조사 및 감시 장비 및 방법 △디지털 포렌식 하드웨어 △데이터 분석 기술 및 데이터 구매 △불법 거래 탐지 등의 기술 지원 활동을 추진
모의 피싱 테스트	EDIH.SH	• 사이버보안 분야의 혁신평가, 테스트 및 프로토타이핑, 교육 및 네트워킹, 자금 조달 및 지원 등의 서비스를 제공 • 모의 피싱 테스트를 실시, 테스트 결과에 따라 인증 조치 및 교육 실행
보안 프레임워크	EU 사이버보안 인증 프레임워크	• EU 차원에서 제품, 서비스 및 프로세스의 특정 요구사항 준수 여부를 판단하기 위한 적합성 평가 기준을 제공 • 보안 표준 개선, 디지털 서비스 신뢰도 증가, ID 접근 관리, 이메일 보안, 웹브라우저 보안, 사이버보안 인지도 개선 및 교육 등에 관한 기준을 제시함으로써 피싱 대책 마련 기여

출처) 각 추진과제 정리

2-3 영국

정책적 대응 현황

영국은 내무부(Home Office) 주도 하에 국가 차원의 사기 대응 전략[32]을 통해 온라인 사기 전담 조직을 설치하고 각종 온라인 사기 대응을 위한 조치를 실행

- 사기 대응 전략(Fraud Strategy)은 사기를 예방하고 소비자를 보호하기 위해 특히 금융 기관과 온라인 플랫폼 등 업계 협력의 중요성을 강조
- (온라인 사기 전담 조직 설치) 400명 이상의 전문 수사관으로 구성된 국가 사기 전담반을 설립하여 피싱 및 스미싱을 포함한 정교하고 유해한 사기에 대처
- (SIM 팜 금지) 사이버 범죄자들이 수천 개에 달하는 사기 문자를 일괄적으로 전송하는 데 사용하는 SIM 팜(Farms) 행위를 금지하며, Ofcom[33]이 해당 규제를 관장
  - 여러 개의 SIM 카드를 사용하여 단시간에 대량의 메시지를 전송하기 위한 기법으로, 스미싱 및 기타 유형의 대량 스팸 메시지 전송을 비롯한 사기 행위에 자주 사용
- (대량 문자 서비스 규제) 대량 문자 발송 서비스는 사전 등록을 의무화하고 심사 과정을 거쳐 허용
- (콜드 콜 금지) 보험, 투자 상품, 암호화폐 등 모든 형태의 금융 상품에 대해 수신자의 사전 동의 없는 판촉 전화 행위인 콜드 콜(cold call)을 금지
  - 정보위원회(ICO)가 콜드 콜 금지 규제 시행을 담당하며, 이를 위반하는 기업에 대한 과징금 등의 조치를 취할 수 있음
- (사고 보고 시스템 고도화) 현행 온라인 사기 신고 통합 창구인 Action Fraud를 대체하여 보다 쉽게 온라인 사기 신고를 하고 관련 조언을 제공하는 새로운 신고 웹사이트를 개설할 예정
  - 신규 사고 보고 사이트는 챗봇을 도입하여 대량의 신고 처리를 신속하게 처리하고 경찰의 직접적 개입 필요 여부를 자동으로 판단하여 수사 자원을 할당

32) UK Home Office, Fraud Strategy: stopping scams and protecting the public, 2023.5
33) Office of Communications(영국 커뮤니케이션청): 영국에서 방송, 통신, 우편 산업 부문에 대해 정부 승인, 규제, 경쟁 관리 등을 담당하는 정부 위원회. 소관 분야의 면허 부여, 조사, 규약과 정책 관리, 경쟁 진흥, 무선 주파수 보호 등을 담당

❙ 국가사이버보안센터(NCSC)는 컴퓨터 보안 위협을 피하기 위해 공공 및 민간 부문에 조언과 지원을 제공하는 영국 정부 기관으로, 피싱 이메일, 보이스피싱, 스미싱 및 피싱 웹사이트에 대한 탐지 및 보고 가이던스를 제공 중[34)35)]

- NCSC는 피싱 이메일, 스미싱, 보이스피싱, 피싱 웹사이트, 광고를 가장한 피싱(scam advert) 신고, 피싱, 피싱 이메일/스미싱/보이스피싱 대처법 등의 정보를 제공

〈표 8〉 영국 NCSC 제공 피싱 관련 대응 정보

제공 정보	주요 내용
피싱	• 피싱의 정의 • 피싱 신고 현황: '24.8월 시점 3,400만 건의 스캠 신고 → 193,000건의 웹페이지 삭제 • 피싱으로부터의 보호법 자신과 다른 사람들이 자신에 대해 어떤 개인정보를 게시하는지 고려하여 소셜 미디어 계정 내 개인정보 보호 수준을 결정
피싱 이메일 신고 방법	• 의심스러운 이메일을 최대한 많이 전달할 것 • 사기가 확실하지 않더라도 의심스러운 이메일을 접수하면 NCSC가 확인 • 의심스러운 이메일의 링크를 클릭하지 말 것 • 스팸/정크 폴더에서 발견한 의심스러운 이메일을 NCSC에 전달할 필요는 없음
스미싱 신고 방법	• 기기별 스미싱 문자 전송법: 아이폰/아이패드 & 안드로이드 • 스미싱 신고 현황: '24.8월 시점 22,000 건의 스캠 문자 신고 → 7,726건의 서비스 차단
보이스피싱 보고	• 피싱 전화의 작동 방식 • 의심스러운 전화 신고하기 • 의심스러운 발신자와 개인정보를 공유한 경우 대처 방안 • 보이스피싱으로부터의 보호법
피싱 웹사이트 보고	• 사기로 의심되는 웹사이트 신고하기 • 이메일이나 웹사이트를 신고한 이후의 절차 • 의심스러운 웹사이트에서 개인정보를 공유한 경우 대처 방안 • 피싱 웹사이트로부터의 보호법

출처) UK NCSC

34) https://www.ncsc.gov.uk/collection/phishing-scams
35) NCSC는 phishing보다는 scam이란 표현을 일반적으로 쓰고 있으나 사이트 내 활용 용법상 본 보고서에서 소개된 개념에 비춰볼 때 피싱에 해당

• '24.7월 현재까지 NCSC는 3,300만 건의 피싱 공격 건수가 report@phishing.gov.uk를 통해 접수됐으며 이 중 345,407개의 URL에서 188,000건의 피싱 웹사이트를 삭제

- 스미싱의 경우 7726(휴대전화 키패드상에서 SPAM)을 통해 접수된 건 중 21,000건의 번호가 삭제
- 한편 보이스피싱으로 인해 금전적인 피해가 발생할 경우 경찰청 웹사이트(www.actionfraud.police.uk)나 전화로 접수

▌영국 국세청(HM Revenue and Customs, HMRC)을 사칭하는 피싱 및 스미싱 시도를 인지하고 신고하는 방법에 대한 다양한 지침을 개발 중이며, 각각에 대한 신고 창구를 마련[36]

〈표 9〉 영국 국세청(HMRC) 발간 피싱/스미싱 대응 지침 및 문서

유형	주요 지침 및 문서	발간일
피싱 식별	HMRC 관련 피싱 이메일, 의심스러운 전화 및 문자 사례	2024.4
	세금 사기 전화, 이메일 및 문자 메시지 식별 방법	2024.4
	공식 HMRC 연락처 목록 확인	2021.7
온라인 안전	HMRC 로그인 정보 안전 보관법	2023.6
	HMRC 상담원을 위한 온라인 보안 정보	2011.11

출처) UK HMRC

• 피싱은 phishing@hmrc.gov.uk, 스미싱은 6059923(전화번호)을 통해 각각 이메일과 문자로 피싱/스미싱 정보를 접수

▌컴퓨터오남용방지법 1990(Computer Misuse Act 1990) 컴퓨터 시스템 및 데이터에 대한 무단 액세스를 규제하기 위한 법률로 피싱·스미싱에 의한 침해 행위 역시 본 법률의 규제 대상[37]

• 동 법률은 컴퓨터 시스템이나 데이터에 무단으로 액세스하는 행위(제1절)와 추가 범죄를 저지르기 위한 의도로 무단 액세스하는 행위(제2절[38])에 대해 불법으로 규정

36) https://www.gov.uk/government/collections/hmrc-phishing-and-scams-detailed-information
37) https://www.cps.gov.uk/legal-guidance/computer-misuse-act
38) Section 2: Unauthorised access with intent to commit or facilitate commission of further offences, Computer Misuse Act 1990

• 또한, 피싱 이메일을 통한 멀웨어나 스파이웨어 등 컴퓨터의 작동을 손상시키려는 의도 또는 이로 인한 무단 행위 역시 범죄로 규정(제3절[39])

▌사기법 2006(Fraud Act 2006)은 허위 진술이나 정보 미공개 등 다양한 유형의 사기 행위를 규제하기 위한 법률로, 피싱·스미싱 역시 동 법의 해석에 따라 규제 대상에 해당[40]

• (허위 진술에 의한 사기, 제2절) 자신 또는 타인에게 이득을 취하거나 타인에게 손실을 입힐 의도로 허위 진술을 하는 것을 위법 행위로 규정

– 따라서 일반적인 피싱과 스미싱 역시 사칭 등을 통해 피해자를 속여 민감한 정보를 제공하도록 유도하므로 동 법의 규제를 받게 됨

• (정보 공개 불이행에 의한 사기, 제3절) 개인이 이득을 취하거나 손실을 입히려는 의도로 법적으로 공개해야 하는 정보를 공개하지 않는 상황을 규제하기 위한 조항으로, 메시지 또는 웹사이트의 실체를 공개하지 않는 피싱 및 스미싱의 경우 이에 해당

▌일반 자격 조건(The General Conditions of Entitlement)은 모든 전자 통신 네트워크 및 서비스 제공업체가 영국에서 서비스를 제공하기 위해 준수해야 하는 규제 조건으로 Ofcom에 의해 관리 및 집행되는 규정[41]

• (조건 C6, 발신 회선 식별 기능): 통신 서비스 제공사는 발신자 식별 서비스를 제공해야 하며, 수신자가 전화 및 메시지의 발신지를 식별할 수 있도록 지원

• (조건 C5, 전자 통신 네트워크 또는 서비스의 오용): 통신 서비스 제공사에게 사기 또는 범죄 목적으로 네트워크가 사용되는 것을 방지하기 위한 조치를 취할 것을 의무화

39) Section 3: Unauthorised Acts with intent to impair, or with recklessness as to impairing the operation of a computer, Computer Misuse Act 1990
40) https://www.legislation.gov.uk/ukpga/2006/35/contents
41) https://www.ofcom.org.uk/phones-and-broadband/accessibility/general-conditions-of-entitlement/

기술적 대응 현황

’21.10월 Ofcom은 영국 내 주요 통신사업자들과 함께 영국 번호로 가장하여 해외에서 걸려오는 거의 모든 인터넷 전화를 자동으로 차단하기 위한 기술 개발에 합의[42)]

- 범죄자들은 인터넷 기반 통화 기술을 이용해 실제 전화번호에서 걸려온 전화나 문자처럼 보이게 하는 수법을 사용하고 있으며, ’21년 여름 당시 약 4,500만 명의 소비자가 전화 사기의 표적이 된 바 있음
- Ofcom은 수개월 동안 통신사업자들과 영국 번호를 가장한 해외 스미싱 차단 기술 개발을 추진
- 그러나 일각에서는 영국 내 다수의 지역이 1970년대에 구축된 구리 기반 네트워크는 IP 통신 네트워크와는 달리 패킷 검사 및 IP 통합 기능 등의 취약성으로 인해 해외 VoIP 제공사 트래픽 차단만으로 사기 문자와 전화 수신을 차단하는 것이 어려울 것이라는 지적도 제기

영국 소재 피싱 대응 보안 인식 교육 솔루션 개발사인 Phishing Tackle은 모의 스미싱 서비스를 제공 중[43)]

- 고객은 미리 구축된 광범위한 SMS 텍스트 템플릿 목록에서 선택하거나 조직에 맞게 직접 모의 스미싱 서비스를 구축할 수 있음
  - 일부 국가에서는 각 메시지가 발신자로 표시될 이름을 지정하거나 플랫폼에서 임의의 전화번호로 전송되도록 허용할 수도 있음
- 주요 기능으로는 △맞춤형 시뮬레이션 스미싱 템플릿 생성 △실제와 같은 스미싱 및 피싱 캠페인 생성 △사용자 반응을 추적하여 조직 내 취약점 파악 등을 제공

42) BBC, Ofcom asks phone networks to block foreign scam calls, 2021.10.25.
43) Phishing Tackle, Phishing Tackle introduce world’s first simulated smishing-as-a-service, 2021.10

〈표 10〉 Phishing Tackle社의 무료 피싱 이메일 테스트 절차

단계	주요 내용
피싱 테스트 신청	• 소속 기관, 직위, 이름, 연락처 등의 정보를 입력하면 무료 이메일 피싱 테스트를 시작
이메일 템플릿 선택	• 다양한 피싱 이메일 템플릿 중 하나를 선택: 침투자 입장에서 공격 대상 조직에 가장 적합한 템플릿을 선택
클릭 시 발생 이벤트 설정	• 테스트 목적에 맞는 랜딩 페이지 템플릿을 선택 • 사용자에게 즉시 경고를 표시하고 모의 피싱 이메일을 클릭했음을 알려주는 정보 페이지를 사용할 수 있음 • 피싱 이메일에서 발견해야 할 위험 신호에 대한 정보를 제공할 수도 있음 • 그러나 의심을 불러일으키지 않고 단순히 수치만 측정하고 싶을 경우 404 페이지로 사용자를 안내
피싱 테스트 결과 다운로드	• 피싱 이메일 테스트 결과를 확인하고 클릭 취약 비율 및 추가 정보 차트가 포함된 PDF를 다운로드 • 테스트 결과 차트는 경영진과 공유할 수 있도록 이해하기 쉬운 형식으로 표현
결과 비교	• 클릭 취약성 피싱 테스트 결과를 기존에 보안 인식 교육을 받은 다른 업계 동료들과 비교

출처) Phishing Tackle[44)]

44) https://phishingtackle.com/click-prone-test/

2-4 독일

정책적 대응 현황

▌독일은 독일 형법(Strafgesetzbuch, StGB) 하에서 데이터 스파이, 컴퓨터 사기 및 데이터 위조 등의 조항을 통해 피싱·스미싱에 대한 다양한 법률 해석 및 적용이 가능[45]

- (데이터 스파이) 공격자가 무단 액세스로부터 특별히 보호되는 데이터에 무단으로 액세스하는 경우에 적용이 가능(202a, Spying on data)
  - 예를 들어 피싱 공격으로 로그인 자격증명 또는 민감한 정보가 도난당하는 경우 가해자는 동 조항에 따라 처벌될 수 있음[46]
- (컴퓨터 사기) 컴퓨터 프로세스를 조작하거나 부정확하거나 불완전한 데이터를 사용하거나 데이터를 무단으로 사용하는 사기 행위에 대한 처벌 규정(263a, Computer fraud)
  - 피해자를 속여 금융정보를 공개하거나 승인되지 않은 거래를 하도록 유도하는 피싱 공격에 대해 동 조항 적용이 가능하며, 5년 이하의 징역 또는 벌금형에 처해질 수 있음[47]
- (데이터 위조) 공격자가 합법적인 조직을 모방 또는 사칭한 가짜 웹사이트, 이메일 또는 문자 메시지를 제작해 배포하는 경우에 대한 처벌 적용이 가능한 규정(269, Forgery of documents)
  - 데이터 위조를 통해 사칭 웹사이트나 이메일, 문자 메시지를 위조하거나 허위 또는 위조된 문서를 사용하는 경우 5년 이하의 징역 또는 벌금형에 처해지며, 미수범은 5년 이하의 징역 또는 벌금형에 처해질 수 있음
- (멀웨어에 의한 IT 시스템 감염) IT 시스템을 랜섬웨어, 스파이웨어, 웜, 트로이목마 및 바이러스 등의 멀웨어에 감염시키는 행위는 형사 범죄에 해당(303b, Computer sabotage)
  - 동 조항에 따르면, 데이터를 삭제, 억제, 사용할 수 없게 만들거나 변경하거나 타인에게 손해를 입힐 의도로 데이터를 입력 또는 전송하여 타인에게 상당히 중요한 데이터 처리 작업을 방해하는 사람은 3년 이하의 징역 또는 벌금형에 처해질 수 있음

45) https://www.gesetze-im-internet.de/stgb/
46) (1) 본인 또는 타인이 의도하지 않았고 접근 보안을 우회하여 무단 접근을 방지하도록 특별히 보호된 데이터에 무단으로 접근하도록 제공한 사람은 3년 이하의 징역 또는 벌금형에 처할 수 있음
47) (1) 본인 또는 제3자를 위해 불법적인 금전적 이익을 얻을 목적으로 프로그램을 잘못 설계하거나 부정확하거나 불완전한 데이터를 사용하거나 데이터의 무단 사용 또는 기타 방법으로 데이터 처리 작업의 결과에 영향을 미침으로써 타인의 자산에 손해를 끼친 사람은 5년 이하의 징역 또는 벌금형에 처할 수 있음

▌피싱·스미싱과 관련된 업무를 담당하는 조직으로는 연방정보보안청(Bundesamt fur Sicherheit in der Informationstechnik, BSI)이 대표적이며, 이외 연방금융감독청(BaFin), 연방네트워크청 및 관할 개인정보 보호 당국 등도 관여

- BSI는 피싱·스미싱과 관련된 예방적 보안 조치를 총괄하는 역할을 담당하며, 웹사이트 상에서 스팸, 사기 메일, 기관 사칭 이메일 등에 관한 정보와 동영상 홍보 자료를 제공[48)]

  – 최근 피싱의 주요 사례 유형으로는 PayPal의 이메일을 사칭하여 GDPR 적용에 따른 고객 데이터 입력 요청, 나이키 등 주요 브랜드를 사칭하여 무료 사은품 행사에 참여를 유도한 개인정보 탈취 등이 언급

- 연방네트워크청(The Federal Network Agency)은 통신 관련 법률을 집행하며 통신 네트워크 및 서비스와 관련된 피싱 침해 통지 접수 업무를 담당

- 독일 금융 규제 기관인 연방금융감독청(Bundesanstalt für Finanzdienstleistungsaufsicht, BaFin)은 금융사기로부터 소비자를 보호하기 위해 피싱·스미싱 관련 정보를 제공하고, 금융 사고 발생 사안을 접수[49)]

  – BaFin 웹사이트에서는 스키밍, 피싱, 보이스피싱, 가짜 쇼핑사이트(fake shops), 잡 스캐밍 등의 유형 각각에 대한 정의와 보호 방법을 설명

〈표 11〉 독일 연방금융감독청(BaFin)이 제시하는 온라인 금융사기 대응책

사기 유형	주요 내용
스키밍[50)]	• ATM을 사용하기 전에 항상 주변 환경과 ATM의 상태를 살필 것 • 비밀번호를 입력할 때 키패드를 가리고 뒤에 아무도 지켜보고 있지 않은지 확인 • 계좌에서 인출되는 금액을 정기적으로 확인
피싱	• 이메일에 민감한 로그인 정보를 입력하라는 메시지가 표시되면 절대로 입력하지 말 것 • 낯선 이메일의 첨부파일, 링크, 다운로드 파일을 열지 말 것 • 합법적인 출처에서 온 파일만 다운로드할 것 • 이메일의 진위 여부가 의심스러우면 은행에 문의 • 온라인 및 소셜 미디어 사용 시 데이터에 주의할 것 • 암호화된 연결(예: SSL 표준)을 사용할 것 • 브라우저의 상태 표시줄에 자물쇠 기호가 표시되는 'https'로 시작하는 안전한 웹사이트를 이용할 것

48) https://www.bsi.bund.de/EN/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Spam-Phishing-Co/spam-phishing-co_node.html
49) https://www.bafin.de/EN/Verbraucher/Finanzbetrug/Datendiebstahl/datendiebstahl_node_en.html
50) skimming. 고객이 ATM을 사용하는 동안 카드 데이터와 PIN 번호를 훔쳐 보는 것

사기 유형	주요 내용
보이스피싱	• 예상치 못한 전화를 받았을 때 은행 정보, TAN 번호 또는 로그인 정보를 절대 알려주지 말 것 • 통화를 끊고 은행 고객 서비스에 연락하여 직원으로 추정되는 사람과 설명한 상황이 진짜인지 문의할 것 • 이메일로 전송된 번호는 사기의 일부일 수 있으므로 절대 전화하지 말 것
가짜 쇼핑 사이트	• 가격을 비교하고 지나치게 좋은 혜택은 주의를 기울일 것 • 리뷰를 확인하는 등 다른 매장도 함께 확인할 것 • 어떤 결제 수단이 제공되는지 살펴볼 것 • 민감한 데이터를 입력할 때는 주의할 것 • 이용약관 및 법적 고지의 정보를 통해 온라인 판매자의 존재를 확인
잡 스캐밍[51]	• 채용 제안 시 신원 확인용으로 계좌 개설을 위한 은행의 화상 본인 확인 절차에 참여하라는 지시에 응하지 말 것 • 입사 원서를 보내기 전에 채용 제안의 진위를 확인하기 위해 철저한 조사를 실시

출처) 독일 연방금융감독청(BaFin)

기술적 대응 현황

▌독일 정부는 연방정보보안청(BSI)이 주축이 되어 다양한 피싱 방지 및 스미싱 방지 기술을 개발하고 홍보하는 데 적극적으로 관여

• BSI는 이메일 보안 전송 기술 문서를 통해 다양한 이메일 전송 암호화 기술 규격(TR-03108 Secure Email Transport)을 공개[52]

- 이메일 보안 전송 기술은 암호화된 연결을 통해 이메일 클라이언트와 이메일 서버 간에 이메일을 교환에 적용하는 기술
- 암호화된 이메일 교환은 암호화 전송 중에는 암호화되지 않은 이메일을 제3자가 읽을 수 없으므로 데이터 무결성을 유지하고, 통신 당사자의 신원을 보장하며, 개인정보를 보호하는 역할을 함

51) Job scamming. 합법적인 고용주의 웹사이트나 구인 공고를 위장하여 구직자를 속이는 사기 수법
52) https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03108/TR03108.pdf?__blob=publicationFile&v=3

- 동 보고서에서는 이메일 제출 및 검색, DANE(DNS-based Authentication of Named Entities) 보안 메일, MTA-STS 보안 메일, 이메일 전송용 TLS 리포트 등을 이메일 교환에 따른 암호화 기술로 언급
- DANE의 경우 DNS를 사용하여 이메일 암호화 및 인증을 위한 공개 키를 저장하고 배포함으로써 이메일 기반 피싱에 대한 보안을 강화

• '15년 초 BSI는 FIDO(Fast IDentity Online) 얼라이언스에 가입하여 FIDO 인증 표준을 장려[53]

- FIDO는 온라인 보안을 강화하고 비밀번호에 대한 의존도를 낮추기 위해 설계된 개방형 인증 표준으로, BSI는 이를 통해 피싱을 방지하고 전반적인 사이버보안을 개선하고자 함

〈표 12〉 FIDO 인증 표준 사양 현황

표준 사양	주요 내용
FIDO2	• 비밀번호 없는 인증을 지원하기 위해 FIDO 얼라이언스에서 개발한 일련의 사양 – WebAuthn(웹 인증): 강력한 공개 키 기반 자격 증명을 생성하고 사용하기 위한 표준 웹 API를 정의하는 W3C(월드와이드웹 컨소시엄)에서 발표한 웹 표준 – CTAP(클라이언트-인증자 프로토콜): 외부 인증자(예: 보안 키 또는 모바일 장치)가 인증 목적으로 클라이언트(예: 웹 브라우저)와 통신할 수 있도록 하는 프로토콜
UAF (범용 인증 프레임워크)	• 비밀번호가 필요 없는 인증 환경을 제공하도록 설계 • 사용자는 지문 스캔, 얼굴 인식 또는 PIN 입력과 같은 로컬 방법을 사용하여 인증 • 생체 인식 센서를 일반적으로 사용할 수 있는 모바일 환경에 특히 유용
FDO (FIDO Device Onboarding)	• FDO는 IoT 디바이스의 온보딩 프로세스를 간소화하기 위한 FIDO 얼라이언스의 최신 사양 • 장치를 네트워크에 온보딩하는 안전하고 자동화된 방법을 제공하여 수동 개입 없이 장치가 올바르게 인증되고 구성되도록 보장

출처) FIDO[54]

53) Identity Week, German BSI joins FIDO Alliance, 2015.10.16
54) https://fidoalliance.org/certification/

2-5 일본

정책적 대응 현황

▌일본은 경찰청을 중심으로 일반인을 대상으로 한 기본적인 피싱 대응책을 홈페이지를 통해 제시하는 등의 인식 확산 활동을 강화

- 경찰청 내 사이버 경찰국은 피싱 기법, 피싱 피해를 당했을 때의 대응책, 피해 방지 대책, 사업자의 대책 등의 정보를 제공[55)]
  - 경찰청이 공개한 주요 피싱 기법으로는 이통사, 택배사, 금융기관을 사칭하여 이메일, SMS를 발송하여 '피싱 사이트로 유도'하는 방식과, 기업이나 기관을 사칭하기 위한 '발신자 정보 위장'하는 방식이 소개
  - 피해 방지 대책으로는 △이메일이나 SMS에 포함된 링크는 클릭하지 않을 것 △컴퓨터와 스마트폰의 보안 유지 △통신사 등에서 제공하는 보안 설정 활용 △ID 비밀번호를 반복해서 사용하지 않을 것 △일회용 비밀번호 활용 등을 제시
- 이외 경제산업성, 총무성, 개인정보보호위원회 등이 정부 공조 및 민간 협력을 통해 피싱 예방을 위한 홍보 및 기술 전파 관련 업무를 공동으로 지원
  - 이들 기관은 피싱 사기를 방지하기 위해 신용카드사를 대상으로 발신 도메인 인증 기술(DMARC)의 도입 요청에 공동 대응 중

▌민간에서는 피싱대책협의회(Council of Anti-Phishing Japan)가 가이드라인 발간 및 홍보 등을 통해 일본 피싱 대책 활동의 구심점 역할을 하고 있음[56)]

- 피싱대책협의회(Council of Anti-Phishing Japan)는 '05.4월에 설립된 조직으로, 총무성이 주관하여 금융청, 경찰청 등 정부 기관과 전국은행협회, 지방자치단체 등이 참여하는 범정부 형태로 성장하였으며 그 외 금융기관, IT기업, 통신사업자 등 산업계 인사도 참여
  - 이러한 구성을 기반으로 협의회는 피싱 사기 대응 및 예방 등을 위한 민·관 협력체계를 구축
- 협의회 사무국은 JP CERT 코디네이션 센터가 담당하며, 주요 활동은 다음과 같음
  - (정보 수집 및 제공) 피싱 사기에 대한 최신 정보를 수집하여 일반 소비자와 기업에 제공
  - (주의 환기) 피싱 사기의 수법과 대응 방안에 대한 경각심을 일깨워 피해를 예방할 수 있는 정보를 전달
  - (기술·제도적 검토) 피싱 대응을 위한 기술적 방법 및 제도 개선을 검토하고 가이드라인을 수립 및 시행

55) https://www.npa.go.jp/bureau/cyber/countermeasures/phishing.html
56) https://www.antiphishing.jp/

• 협의회는 정보 제공의 일환으로 피싱대책 가이드라인을 개발하여 사업자 및 일반 이용자를 대상으로 한 체계적 대책 방안을 제시

• 피싱 대책 가이드라인은 '11년부터 발간하기 시작하여 매년 갱신되고 있으며, 최신 버전은 '24.6월에 발간

〈표 13〉 일본 피싱대책협의회 발간 피싱 대책 가이드라인(2024년판) 주요 내용

피싱 대책 가이드라인	이용자 피싱 사기대책 가이드라인
• 웹사이트 운영자 피싱 대책 – 웹사이트 운영자에 있어 피싱 피해 – 이용자를 지키기 위한 피싱 대책 – 피싱 피해 발생을 신속하게 확인하기 위한 대책 • 피싱 대책 매뉴얼 – 피싱 피해 발생 시 대응과 대책 – 이용 환경에 관한 주의환기 • 이용자 피싱 대책	• 당장 가능한 피싱 대책 – 피싱 메일 대책 – 웹필터 활용 – 올바른 URL과 정식 애플리케이션을 이용한 접근 – 스푸핑 메일 주의 – PC와 모바일 단말을 안전하게 보호 – 정규 애플리케이션 설치 – 결제 내역 확인 – 잘못된 중요 정보 입력 시 대응

출처) 일본 피싱대책협의회

▌규제 측면에서는 일본의 부정접속금지법[57]이 피싱 행위를 포함한 부정 접속 행위를 금지

• 이 법은 1999년에 제정되어 '00년에 시행되었으나, '12년 법률 개정을 통해 피싱 행위에 대한 규제가 강화[58]

• '12년 개정 법률을 통해 동 법에 규정된 가짜 웹사이트나 이메일을 사용하여 사용자로부터 개인정보(ID, 비밀번호, 신용카드 정보 등)를 가로채는 피싱 행위 금지에 대한 처벌 규정이 강화

– 위반자에게는 3년 이하의 징역 또는 100만 엔 이하의 벌금이 부과(동법 제7조, 제12조 제4호)

• 타인의 아이디와 비밀번호를 부정하게 취득하거나(동법 제4조), 부정하게 보관하는 행위(동법 제6조)도 금지되어 있으며, 여기에는 피싱 행위를 통해 취득한 정보를 보관하는 행위도 포함

• 또한, 타인의 아이디나 비밀번호를 사용하여 접근 권한이 없는 컴퓨터나 네트워크에 무단으로 접속하는 행위도 금지(동법 제11조)

57) 不正アクセス行為の禁止等に関する法律
58) TSL Magazine, 不正アクセス禁止法とは？規制対象となる行為・改正の概要・違反事例も解説, 2020.1.14

기술적 대응 현황

▌일본은 경제산업성, 총무성 및 경찰청은 이메일의 발신자를 인증하는 기술인 DMARC (Domain-based Message Authentication, Reporting & Conformance)의 보급을 공동으로 추진 중

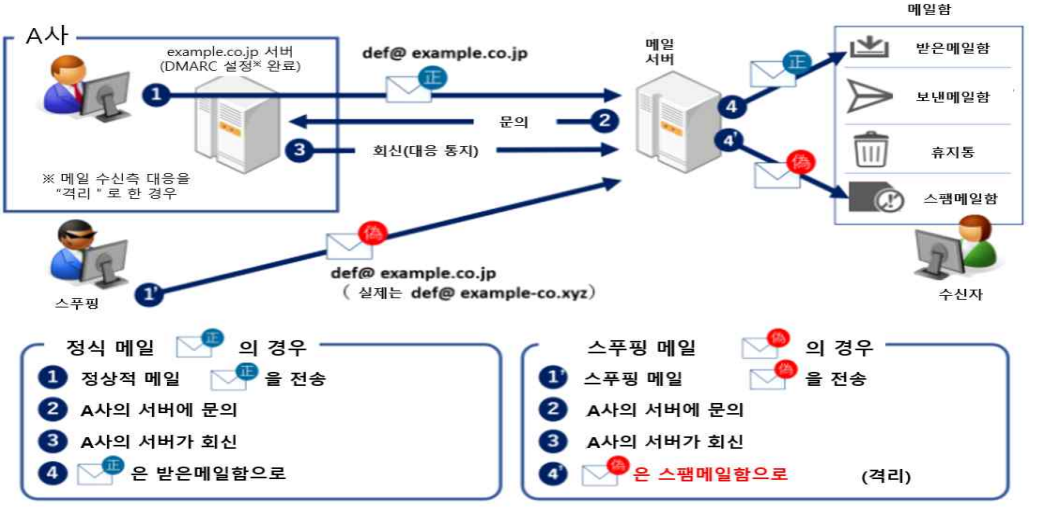
- DMARC는 신용카드 피싱 사기에 노출된 이용자 보호를 위해 신용카드사를 대상으로 도입을 권고

  – DMARC 도입 권고는 악의적인 제3자가 신용카드사 등을 사칭한 이메일 등을 이용자에게 발송하여 해당 이메일 등의 링크를 통해 가짜 사이트로 유도한 후 이용자의 신용카드 번호 등을 탈취하는 형태의 피싱 공격이 일본에서 확산됨에 따른 조치

- 이들 기관은 이용자에게 공개하는 모든 도메인 이름(메일을 발송하지 않는 도메인 이름도 포함)에 대해 DMARC를 도입할 것을 요청

- 이에 따라 신용카드사는 DMARC 도입 시 수신자 측에서 스푸핑 메일을 수신 거부할 수 있는 정책을 운영해야 함

〈그림 8〉 DMARC 개념도



출처) 일본 경찰청[59]

59) https://www.npa.go.jp/bureau/cyber/countermeasures/phishing.html

▌일본의 대표적 이동통신사업자인 NTT도코모는 SMS를 악용한 피싱 사기에 대응하기 위해 위험한 사이트 URL 등이 포함된 SMS를 자동으로 거부할 수 있는 '위험 SMS 거부 설정'을 제공 중[60)]

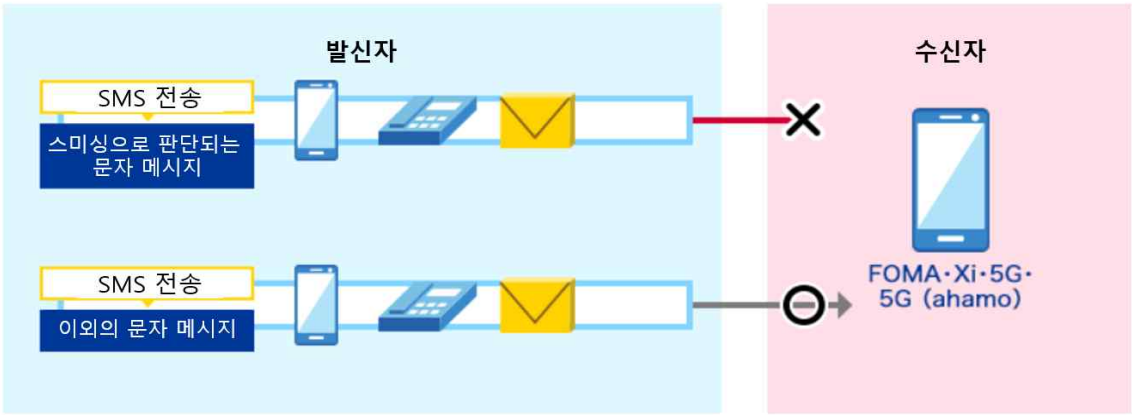
- 이 기능은 악성 앱을 설치하도록 유도하거나 개인정보를 탈취하려는 사이트로 유도하는 SMS를 판단하여 고객이 수신하지 못하도록 하는 기능
- 고객이 SMS를 수신하기 전에 발신자 정보 및 본문 내용을 바탕으로 도코모 네트워크에서 피싱 SMS를 자동 판단
- 이외에도 NTT도모코는 비밀번호를 사용하지 않는 생체인증 서비스와 안심보안 등을 통해 피싱으로부터 고객 보호 조치를 실시

– (어카운트 패스워드리스 인증) 비밀번호 대신 스마트폰의 생체인증 접속이나 화면 잠금 기능 서비스를 제공

– (안심 보안) 바이러스 탐지, 위험 사이트 차단, 스팸메일 방지, 의심스러운 전화 수신 알림, 위험한 Wi-Fi 핫스팟에 접속했을 때 경고 화면을 표시

– (안심 보안 프라이버시) 고객의 개인정보가 인터넷에 부정하게 유출되지 않도록 모니터링하는 서비스

〈그림 9〉 NTT도코모 위험 SMS 거부 개념도



출처) NDD docomo[61)]

60) NTT docomo, フィッシング詐欺を未然に防ぐ「危険SMS拒否設定」の提供を開始, 2022.1.13
61) https://www.docomo.ne.jp/info/spam_mail/sms/?icid=CRP_INFO_anti-phishing_prevention_to_CRP_INFO_spam_mail_sms

2-6 중국

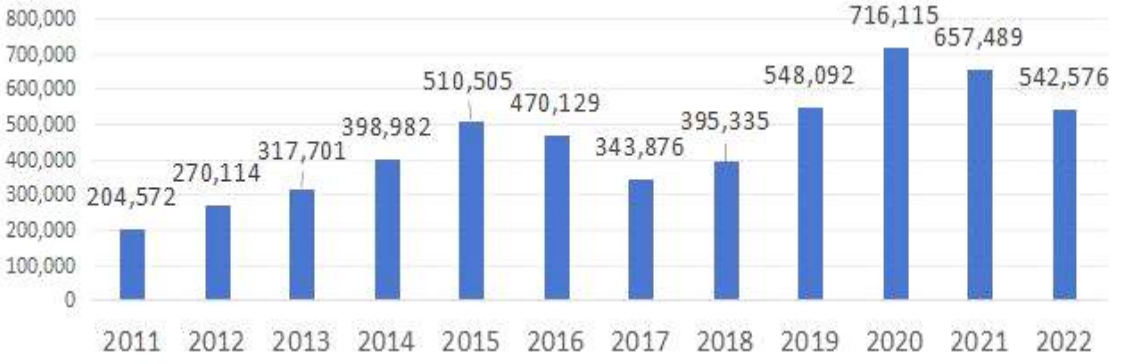
정책적 대응 현황

▌중국에서는 통신망을 이용한 피싱 사기 급증에 대응해 형법[62]에 '정보통신망 범죄활동 방조죄'를 신설하고 '전기통신금융사기 방지법[63]'을 시행하는 등 규제를 강화

• 중국의 피싱 사기 피해는 '11년부터 꾸준히 증가하다가 '15년 형법에 '정보통신망 범죄활동 방조죄'를 신설하며 주춤했으나 '18년부터 다시 증가

– 통신망 사기는 전화번호 매매부터 악의적 목적의 웹사이트 허위 가입, 개인정보 매매, 보이스피싱 시행 등 전체 범죄 사슬의 가담자를 필요로 하며, 정보통신망 범죄활동 방조죄는 통신망 사기 등의 범죄에 쓰이도록 은행카드와 전화카드를 불법 매매해 계좌와 휴대전화 정보를 제공하는 유형이 일반적

〈그림 10〉 2011~2022년 중국 피싱 사기 신고 건수



출처: 중국 국가통계국, KOTRA 재인용

• 중국은 보이스피싱 등 피싱 범죄 피해가 늘어나면서 '22년 9월 2일 '전기통신금융사기 방지법'을 제정하여 '22년 12월 1일부터 시행 중으로, 동 법은 재물을 불법 점유하려는 목적으로 전화 등 전기통신 수단을 사용하여 타인을 속이는 행위를 '전자통신금융사기'로 규정

– 동 법은 전기통신 부서의 실명제 요구사항 이행, 은행의 자금세탁 및 사기방지 책임 이행, 결제기관의 금융계좌 수량 제한, 인터넷 기업의 정보관리 강화 등 각 부처의 책임을 명확히 함

62) 中华人民共和国刑法
63) 中华人民共和国反电信网络诈骗法

- 전자통신금융사기 범죄행위를 하여 편취한 재산의 액수가 매우 큰 경우 또는 관련 정황이 특수하고 심각한 사건에 해당하는 경우 '전기통신금융사기 방지에 관한 법' 제38조 및 '형법' 제266조에 따라 사기죄를 적용하여 최대 무기징역에 처하고 벌금 또는 재산 몰수를 병과
- 공안부(公安部)에 따르면 동 법의 시행 이후 '24.5월 기준 전국 통신망 사기 사건은 총 54만 3천 건이 적발되고 범죄 용의자도 대거 검거되었으며, 전국의 통신사기 사건 수와 손실액이 30% 감소한 것으로 나타남

• **중국 공안부는 전기통신금융사기 방지법의 철저한 이행을 위해 '23.11월 '전기통신망 사기 및 관련 위반 범죄에 대한 공동처벌조치(초안)'[64]을 공개하고 의견수렴을 진행**

- 초안은 통신 및 온라인 사기 퇴치를 위한 법률 이행을 보장하는 징계 원칙, 징계 대상, 징계 조치 등 6개 분야 19개 조항으로 구성됨
- 처벌 대상에는 통신사기 행위 또는 통신사기 관련 사이버범죄 방조, 신용카드 관리 방해, 국민 개인정보 침해, 범죄수익 은폐 등의 혐의로 형사처벌을 받은 사람이 포함되며, 불법 행위를 위해 국경을 넘어 범죄자를 조직하는 행위도 대상에 포함됨
- 휴대전화 유심칩, 사물인터넷(IoT) 카드, 유선 전화, 통신 회선, 은행 계좌, 디지털 위안화 지갑, 인터넷 계정, 도메인 이름, IP 주소 등을 불법 구매, 판매, 임대한 사람들은 위반 행위의 심각성에 따라 처벌을 받게 됨
- 개인과 단체 모두 징계 대상으로 금융, 통신, 네트워크, 신용 수단을 통한 징계 조치도 명시되어 있으며, 불법 행위에 대한 등급 분류에 따라 징계를 적용하고 심사와 판단, 징계 기간, 통보 등 절차를 표준화할 계획

▌중국 정부는 통신망을 이용한 피싱 범죄에 대한 대중의 인식 제고를 위해 피싱 사기 수법의 유형 공개 및 대국민 캠페인을 실시

• **중국 국가안전부(国家安全部)는 '24.3월 공식 웨이보 계정을 통해 피싱 이메일에 사용되는 일반적인 수법의 유형을 소개하고 대응 방법을 안내**

- 해당 안내에 따르면 피싱 사기 유형은 정부 기관 이메일과 흡사한 이메일 인터페이스를 구축해 경고 메시지로 위장한 피싱 이메일로 계정과 비밀번호를 획득하는 유형 및 피해 이메일 사용자 정보를 사전에 수집 및 분석해 맞춤화된 이메일 제목과 내용으로 악성 파일을 다운로드하게 만드는 방식을 일반적으로 사용
- 이러한 피싱 사기 위험을 예방하려면 사이버보안 위험에 대한 인식을 높이고 사이버공격 방법을 사전에 이해해야 하며, 출처를 확인할 수 없는 의심스러운 이메일이나 계정과 비밀번호를 요구하는 경우 링크나 첨부파일을 클릭해서는 안 되고, 보안성이 높은 비밀번호 설정과 정기 업데이트 등의 보안 조치 개선이 필요

64) 电信网络诈骗及其关联违法犯罪联合惩戒办法（征求意见稿）

• 중국 중앙선전부(中央宣傳部)와 공안부는 통신망 사기 범죄 퇴치를 위해 '24.6월 '전국민 사기 방지 행동' 캠페인을 전국적으로 실시

- 동 캠페인에 따라 각 지자체는 지역사회, 농촌, 가족, 학교, 기업의 5대 핵심 타깃을 상대로 지역과 산업적 특성에 따라 맞춤형 홍보를 시행하고 소상공인, 회계 담당자, 미성년자, 노인에 대한 홍보를 강화하며 통신망 사기유형과 최신 사기 수법에 대한 정보를 제공

- 공안부는 국가사기방지센터, 외교부 영사보호센터, 교육부 해외유학센터를 통해 '해외 통신망 사기 예방 핸드북'을 발간해 유학생과 화교 집단의 예방 인식과 역량 향상을 도모했으며, 캠페인 기간 주요 언론매체와 인터넷 플랫폼은 사기 방지와 관련된 기사를 집중 게재함으로써 대국민 홍보와 교육, 예방 효과를 강화

기술적 대응 현황

▌중국은 공안부, 공업정보화부(工业和信息化部)를 주축으로 통신망 사기 범죄 예방을 위한 사기 방지 앱 출시, 휴대전화 카드와 인터넷 계정 조회 서비스 출시 등 다양한 기술적 조치를 채택

• 중국은 '21.3월 휴대전화 사기 방지 소프트웨어인 국가사기방지센터 앱을 공식 출시하여 '24.6월 기준 총 4억 2천만 건의 조기 경고 및 설득 메시지를 전송

- 이 앱의 첫 번째 기능은 조기 경고와 설득 메시지 전송으로, 사용자가 사기로 의심되는 전화나 문자 메시지를 받은 경우 조기 경고 메시지를 전송하여 설득

- 두 번째는 사기 단서의 신속한 신고 기능으로, 사용자가 생활 중 사기에 대한 단서를 발견하면 앱의 원클릭 신고 기능으로 신고할 수 있음

- 세 번째 기능은 앱을 사용해 의심스러운 인터넷 사용자의 실제 신원과 소셜 계정, 결제 계정을 확인해 온라인 거래에서 사기 위험을 줄일 수 있음

- 네 번째 기능은 사기 방지에 관한 지식 습득으로, 앱을 통해 사기 방지 지식과 사기 수법에 대한 정보를 정기적으로 게시하여 사용자의 사기 인지와 예방 능력을 향상

• 중국 공업정보화부와 공안부는 '21.7월에는 12381 사기 조기경보 및 설득용 SMS 시스템을 출시해 사기 위험이 있는 사용자에게 실시간 문자 메시지 경고를 제공

- 12381 시스템은 빅데이터, 인공지능과 기타 기술을 이용해 공안기관에서 제공한 사건과 관련된 번호를 기반으로 잠재적인 피해자를 자동 분석 및 발견해 조기 경고 문자 메시지를 전송

- '23.6월까지 발송된 10억 7천만 건의 메시지 중 조기 경고와 설득 정확도는 60% 이상에 달하는 것으로 확인됨

• 공업정보화부는 사기꾼들이 타인의 신원 정보를 이용해 전화카드를 신청하는 행위를 막기 위해 전국 휴대전화 카드에 대한 '원패스 확인' 서비스를 도입

- 사용자는 전국 93개 성급 기간통신업체와 39개 이동통신 재판매업체의 관련 데이터에 접근해 본인 명의로 발급된 휴대전화 카드 보유 개수를 온오프라인 등 다양한 채널로 확인할 수 있으며, 48시간 이내에 전국 휴대전화 카드의 발급 현황을 조회 가능

• 각급 공안기관은 조기 경보와 설득 전화로 통신망 사기의 잠재 피해자에게 경고와 설득을 하고 있으나 실제 업무에서는 수신자가 해당 전화를 사기나 장난 전화로 착각하는 경우가 많아, 공안부와 공업정보화부는 전화의 공신력을 증명하기 위한 '사기 방지 명함' 기능을 출시

- 차이나 유니콤, 차이나 텔레콤 및 차이나 모바일의 3대 통신사가 모두 참여하는 이 기능은 각급 공안기관이 조기경보에 사용하는 전화번호를 제공하고 수신전화 알림을 제공하여 공안기관의 조기 경고와 설득 전화의 성공률과 효과를 크게 개선

• 공업정보화부는 사용자가 알지 못하는 인터넷 계정 등록으로 인한 사기 위험을 방지하기 위해 '22년부터 전국 인터넷 계정에 대한 '원패스 확인 2.0' 서비스를 공개

- 이 서비스는 본인 명의 휴대전화 카드 발급 현황을 확인할 수 있는 원패스 확인 서비스를 기반으로 인터넷업체 및 통신사와 연계해 출시한 인터넷 계정 간편조회 서비스
- 이용자는 휴대전화 번호와 주민등록번호 뒤 6자리를 입력해 휴대전화 번호와 연결된 인터넷 계정을 확인할 수 있음
- 사용자가 자신이 알고 있는 정보와 조회된 인터넷 계정이 일치하지 않는다고 문의하는 경우, 인터넷 회사의 계정 해제 처리 체계에 따라 해당 계정을 해제할 수 있어 사용자 본인이 등록하지 않은 인터넷 계정으로 인한 사기를 효과적으로 차단할 수 있으며, '23년 5월 기준 사용자 문의 수는 1,510만 건을 넘어섰음

III

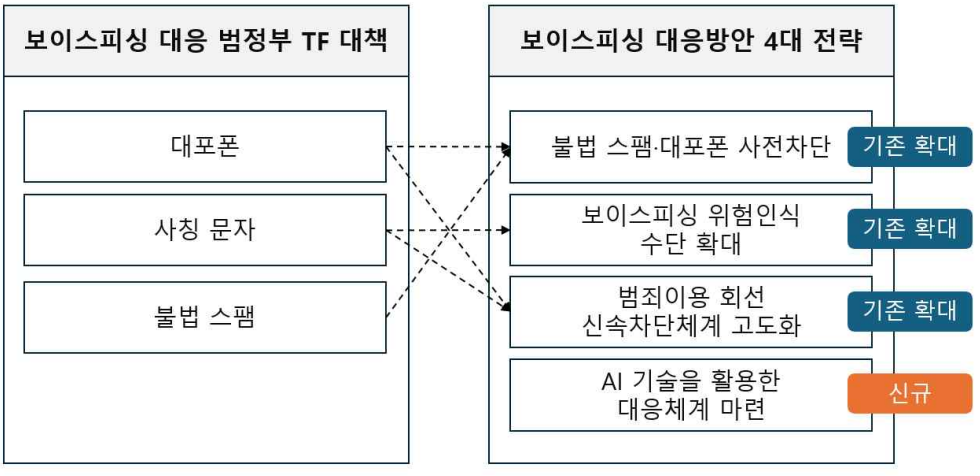
국내 피싱 대응 현황

3-1 정책적 대응 현황

▌정부는 국무조정실 중심으로 '전화금융사기(보이스피싱) 대응 범정부 전담팀('21.12. 발족)'을 운영 중이며, 범정부적 대책 마련과 함께 강력한 단속과 수사를 실시

- 범정부 TF에서는 보이스피싱 범죄 근절하기 위한 통신·금융 대책을 마련('22.9., '24.2., '24.7. 발표)하고, 보이스피싱 범죄 단속·수사·처벌 강화를 통해 피싱 범죄자에 대하여 엄정 대응

〈그림 11〉 통신 분야 보이스피싱 대응 범정부 TF('24.2) vs 보이스피싱 대응방안 4대 전략('24.7) 비교



출처) 과기정통부 보도자료 및 전략자료 재인용

- 이러한 노력으로 보이스피싱 피해액은 2년 연속 감소하여 '23년 피해액이 4천억 원 대로 감소

※ 보이스피싱 피해액(억원) : ('18)4,040→('19)6,398→('20)7,000→('21)7,744→('22)5,438→('23)4,472

❙ 과학기술정보통신부와 방송통신위원회는 통신서비스 부정 이용 방지를 통한 사전 예방과 보이스피싱 위험 감지 수단 확대 및 범죄에 악용된 전화·문자를 신속하게 차단하는 통신 분야 보이스피싱 대책을 발굴하여 추진

〈표 5〉 통신 분야 보이스피싱 대책 주요 추진과제

연도	과제명	주요내용
2022년	단기 이통사 통합 다회선 개통 제한 제도 시행	사업자간 회선정보 공유로 단기간 전체 이통사 통합 기준을 초과하는 가입 회선수 제한
	휴대전화 개통시 본인확인 절차 강화	부정가입방지시스템 강화 및 신분증 스캐너 도입 확대 등
	이통사 및 유통망에 대한 조사·단속	사업자가 휴대전화 개통시 본인확인 의무를 준수하는지 조사·단속 실시
	통신사 전화번호 관리책임 강화	유선전화 개통 시 개인 5회선, 법인 종사자수 기준으로 회선수 제한
	공공·금융기관 전화·문자 신뢰성 향상	안심마크(인증마크+안심문구) 표시 시범 도입
	전화번호 유효성 검증절차 개선	발신번호 등록시 번호의 실소유자 확인을 위한 유효성 검증시스템 구축(안) 마련
	이용중지 전화번호 공유·차단 실시	중지된 전화번호가 재사용 되지 않도록 해당 전화번호를 문자사업자 간 공유하여 추가적인 발송 차단
	국제전화 안내 의무 강화	① 단말기 국외 발신 안내 표시 오류 수정 등 단말 자체 국외 발신 안내 표시 개선 ② 국제전화 음성 안내 서비스 제공 ③ 국내에 있는 이용자의 전화번호가 도용되어 해외 로밍 형태로 허위 인입 시 수신 차단
	보이스피싱 이용 통신단말장치 차단 등	① 보이스피싱 이용 사실이 확인된 통신단말장치에 대한 차단 ② 수사과정에서 발견된 대포폰 및 스미싱 전화번호에 대한 이용 중지
	불법문자 신속 차단	문자메시지 전송규격에 식별코드를 삽입하여 불법문자 신속 차단 (7일 → 2일)
	원스톱(간편) 문자신고 채널 도입	의심 문자 수신 시 '스팸' 신고창이 바로 확인되도록 단말기 기능 개선
	보이스피싱 대응 R&D	AI, 빅데이터 등 ICT 신기술을 활용한 R&D를 추진하여 보이스피싱 범죄 全과정(①탐지·예방-②추적-③수사지원) 대응력 제고

연도	과제명	주요내용
2024년	재판매사업자 관리·감독 강화	문자재판매사 진입요건 상향, 사업운영 과정에서의 관리·감독 강화
	다회선 개통제한 및 본인확인 강화	① 알뜰폰 개통 시 스캐너를 통한 신분증 위조 여부 확인 강화 ② 개통 가능 회선 수 제한 강화(月 3회선 → 반기 3회선)
	명의도용방지서비스 이용확대	민관합동으로 다양한 채널을 활용하여 명의도용 방지 서비스 홍보 강화
	해외로밍 통해 발송된 문자 알림	해외 로밍발신 문자 안내문구 표시
	문자 안심마크 확대 적용	① 문자 안심마크 대상 확대 ② 안심마크 위조 방지 기술 적용
	인터넷 대량문자 발송 안내	휴대전화번호로 대량문자 발송시 해당 전화번호 소유자에게 안내 문자 발송
	'미끼문자'신고편의 제공	휴대전화 단말기에 보이스피싱·스미싱 등 범죄의심 문자·전화 신고 버튼 생성
	범죄 이용 회선 차단 확대	위법한 전화·문자를 발신한 회선뿐만 아니라 연결된 전화·문자 발송 계정 전체를 차단
	원스톱 보이스피싱 대응 서비스	DPG 활용 원스톱 보이스피싱 가드(가칭) 시스템 구축
	통신사AI 활용 보이스피싱 대응지원	'그놈 목소리' 데이터 이통사에 공유하여 보이스피싱 대응 서비스 출시
	딥보이스 활용 보이스피싱 대응	'AI기본법'을 제정하여 딥보이스 안전성·신뢰성 확보, 민간차원의 안전장치 도입 권고 및 워터마크 제도화 추진
	AI기반 보이스피싱 조기탐지 R&D	단말단에서 능동적·선제적으로 보이스피싱을 탐지하여 신속 차단할 수 있는 기술 개발
	대량문자 발송업체 관리 강화 등	① 불법스팸 차단기간 확대(1개월 → 3개월) ② 대량문자 발송업체 자격요건 및 책임 강화 ③ 통신서비스이용증면원 검증 의무화
	단말기 내 스팸 문자 자동 차단	불법 스팸을 단말기 내에서 자동 필터링·차단

출처) 각 정부 부처 보도자료

▌금융위에서는 계좌개설 본인확인 강화, 입금 한도를 축소하여 피해를 예방하고 사기 이용 계좌를 신속하게 지급정지하는 금융 분야 보이스피싱 대책을 발굴하여 추진

〈표 6〉 금융분야 보이스피싱 대책 주요 추진과제

연도	과제명	주요내용
2022년	대면편취형 보이스피싱 구제절차 적용	대면 편취형 보이스피싱도 「통신사기피해환급법」이 적용될 수 있도록 개정 추진
	ATM무통장입금 한도 축소	① 실명확인 없는 ATM무통장입금 한도 축소 : 1회 100만원 → 50만원 ② 수취계좌 실명확인 없는 ATM무통장입금 수취한도 설정 : 1일 300만원
	비대면 계좌개설 본인확인 강화	① 신분증 진위확인시스템 이용 확대 ② 안면인식 시스템 도입
	1원 송금 방식의 실명확인 절차 보완	① 인증번호 유효기간 15분 이내로 단축 ② '계좌개설용' 문구 표기
	오픈뱅킹 피해규모 축소	① 비대면 계좌개설로 오픈뱅킹 가입 시 3일간 오픈뱅킹을 통한 자금이체 차단 ② 오픈뱅킹 신규 가입 시 3일간 이용한도 축소(1일 한도 : 1천만원 → 300만원) ③ 이상거래 탐지강화
	오픈뱅킹 방어수단 마련	① 개인정보노출자 사고예방 시스템 등록 시 오픈뱅킹 가입제한 ② 본인계좌 지급정지 시스템 구축
	원격제어 방지	원격조종 앱 차단
	여전사 본인확인 강화	여전사도 카드발급 / 대출신청 단계 중 신분증 사본을 받고, 진위 확인 시스템 사용
	보이스피싱 범죄자 처벌 강화	① 보이스피싱에 1년 이상 유기징역 또는 범죄수익의 3배 ~ 5배 상당 벌금 부과 ② 단순 조력행위자에도 5년 이하의 징역 또는 5천 만원 이하 벌금 부과
	보이스피싱 예방제도 설명 강화	계좌 개설 시 보이스피싱 예방 서비스 설명 및 가입 의사 확인
	홍보활동 강화	경각심 제고 효과를 극대화할 수 있는 수단을 통해 홍보용
2024년	비대면 계좌개설 본인확인 강화	안면인식 시스템 도입
	통장협박 대응	계좌 일부지급정지를 통해 통장협박에 대응할 수 있도록 「통신사기비해환급법」개정 추진
	간편송금 대응	사기이용계좌 정보공유를 통해 신속한 지급정지 가능토록「통신사기비해환급법」개정 추진
	사기이용계좌 재사용 제한	사기이용 이력이 있는 계좌는 한도제한 계좌로 운영
	계좌개설 시 거래목적 확인 강화	고객 계좌 개설시 금융기관에게 금융거래목적 확인을 의무화
	여신거래 안심차단 시스템 도입	신용대출, 카드론 등 신규 여신거래를 이용자가 사전 차단할 수 있는 시스템 구축

출처) 각 정부 부처 보도자료

참고 1 국내 피싱 등 디지털 범죄 관련 법령 및 제도

▌(피해 예방·처벌) 피싱은 현행 형법상 "권한 없는 자에 의한 정보처리로 재산상의 이익을 취득하는 범죄행위"로 규정하고 있으며, "컴퓨터사용사기죄" 적용이 가능

- 컴퓨터 등 정보처리장치에 허위의 정보 또는 부정한 명령을 입력하거나 권한 없이 정보를 입력·변경해서 정보처리를 하게 함으로써 재산상의 이익을 취득하거나 제3자에게 취득하게 해서는 안 됨(형법 제347조의2[65])

  – 이를 위반할 경우, 10년 이하의 징역 또는 2천만 원 이하의 벌금에 처해질 수 있음

- 누구든지 다른 사람을 속여 재산상 이익을 취하거나 폭언·협박·희롱 등의 위해를 입힐 목적으로 전화(문자메시지를 포함)를 하면서 송신인의 전화번호를 변작하는 등 거짓으로 표시하여서는 안 됨(전기통신사업법 제84조의 2)

  – 이를 위반할 경우, 3년 이하의 징역 또는 1억 원 이하의 벌금에 처해질 수 있음[66]

▌(피해 구제) 피싱과 스미싱은 통신사기피해환급법과 정보통신망법 등에 의해 피해자에 대한 구제책을 마련

- (이용자계좌에 대한 임시조치) 금융회사는 자체 점검을 통하여 이용자의 계좌가 전기통신금융사기의 피해를 초래할 수 있는 의심 거래 계좌에 대해 해당 이용자 계좌의 이체, 송금 또는 출금을 지연시키거나 일시 정지하는 조치를 취해야 함(통신사기피해환급법 제2조의5, '24.2 개정[67])

  – 금융위원회는 '24.2월 개정된 「통신사기피해환급법」에 따른 시행령 개정을 '24.8월까지 완료할 계획으로, 이에 따라 간편 송금 시에도 신속한 지급정지가 가능하고, 통장 협박 피해자에 대한 구제도 신속해질 것으로 예상

- (피해 환급금 지급) 전기통신금융사기를 통해 재산상의 피해를 입은 피해자는 피해금을 송금·이체한 계좌를 관리하거나, 사기 이용계좌를 관리하는 금융회사에 대하여 사기이용계좌의 지급정지 등 전기통신금융사기의 피해구제를 신청할 수 있음(통신사기피해환급법 제3조의1[68])

- 금융감독원은 채권이 소멸된 날부터 14일 이내에 피해환급금을 지급받을 자 및 그 금액을 결정하여 그 내역을 피해구제를 신청한 피해자 및 금융회사에 통지하여야 하고, 통지를 받은 금융회사는 지체 없이 피해환급금을 피해자에게 지급하여야 함(동법 제10조제1항)

• **(소액결제 피해) 통신서비스 이용자는 통신과금 서비스가 자신의 의사에 반하여 제공되었음을 안 때에는 해당 통신사업자에게 이에 대한 정정을 요구할 수 있음(정보통신망법 제58조4의③[69])**

- 통신과금서비스제공자는 이용자의 정정요구가 이유 있을 경우 판매자에 대한 이용 대금의 지급을 유보하고 그 정정 요구를 받은 날부터 2주 이내에 처리 결과를 알려주어야 함

- 즉, 통신요금으로 과금된 소액결제금에 대해 이용자가 이의를 제기할 시 통신사가 아닌 결제 대행사와 콘텐츠 제공사가 협의하여 결제금 청구 취소 여부를 결정해야 함

65) 형법 제347조의2 (컴퓨터등 사용사기) 컴퓨터등 정보처리장치에 허위의 정보 또는 부정한 명령을 입력하거나 권한 없이 정보를 입력·변경하여 정보처리를 하게 함으로써 재산상의 이익을 취득하거나 제3자로 하여금 취득하게 한 자는 10년 이하의 징역 또는 2천만원 이하의 벌금에 처한다.

66) 제84조의2제1항을 위반하여 다른 사람을 속여 재산상 이익을 취하거나 폭언 · 협박 · 희롱 등의 위해를 입힐 목적으로 전화(문자메시지를 포함한다)를 하면서 송신인의 전화번호를 변작하는 등 거짓으로 표시한 자, 제84조의2제2항을 위반하여 영리를 목적으로 송신인의 전화번호를 변작하는 등 거짓으로 표시하는 서비스를 제공한 자

67) 통신사기피해환급법 제2조의5 (이용자계좌에 대한 임시조치) ① 금융회사는 자체점검을 통하여 이용자의 계좌가 전기통신금융사기의 피해를 초래할 수 있는 의심거래계좌 (이하 "피해의심거래계좌"라 한다)로 이용되는 것으로 추정할 만한 사정이 있다고 인정되면 해당 이용자 계좌의 전부 또는 일부에 대하여 이체 또는 송금을 지연시키거나 일시 정지하는 조치 (이하 "임시조치"라 한다)를 하여야 한다.

68) 제3조 (피해구제의 신청 등) ① 제2조제2호가목 또는 나목에 해당하는 행위로 인하여 재산상의 피해를 입은 피해자는 피해금을 송금·이체한 계좌를 관리하는 금융회사 또는 사기이용계좌를 관리하는 금융회사에 대하여 사기이용계좌의 지급정지 등 전기통신금융사기의 피해구제를 신청할 수 있다.

69) 정보통신망법 제58조의4③ 통신과금서비스이용자는 통신과금서비스가 자신의 의사에 반하여 제공되었음을 안 때에는 통신과금서비스제공자에게 이에 대한 정정을 요구할 수 있으며(통신과금서비스이용자의 고의 또는 중과실이 있는 경우는 제외한다), 통신과금서비스제공자는 이용자의 정정요구가 이유 있을 경우 판매자에 대한 이용 대금의 지급을 유보하고 그 정정 요구를 받은 날부터 2주 이내에 처리 결과를 알려 주어야 한다

3-2 기술적 대응 현황

※ 본 내용은 '24년 8월까지 발표 및 추진된 관련 보도자료 등을 기반으로 작성

(민관협력 보이스피싱 대응 AI 기술) 정부는 보이스피싱 민생범죄 확산에 대응의 일환으로 관계기관 및 민간 기업들과 다양한 AI 기술·서비스 개발 사업을 추진[70]('24.6)

- 과학기술정보통신부, 개인정보보호위원회, 금융위원회, 금융감독원, 국립과학수사연구원, 한국인터넷진흥원(KISA)은 'AI·데이터 기반 보이스피싱 예방을 위한 상호 업무협약(MoU)'을 체결
- 통신사 등 민간 기업 역시 보이스피싱 예방 AI 기술·서비스를 개발할 때 금감원, 국과수 등으로부터 보이스피싱 통화 데이터를 제공받아 AI 모델 학습, 성능 테스트 등에 활용할 수 있도록 협력
  - 금감원은 보이스피싱 피해자의 신고를 통해 수집한 통화 음성데이터를 과학수사 지원 목적으로 국과수에 지속 제공
  - 국과수는 해당 데이터를 비식별화 등 전처리 등을 거쳐 데이터를 필요로 하는 민간에 제공하는 데이터 공유체계 구축
  - 개인정보위와 KISA는 데이터 제공·수집·이용 과정 중 발생할 수 있는 개인정보 보호법상 쟁점에 대해 법령 해석, 실증 특례 등 규제개선 방안 등을 검토키로 함

(통신 3사 피싱 범죄 대응) 통신 3사는 보이스피싱 및 스미싱에 대응하기 위해 AI 기술을 적용한 차단 서비스를 앞다퉈 개발

- (SK텔레콤, AI 스팸 표시 기능) SK텔레콤은 '22년부터 전기통신금융사기 전담 대응팀을 신설, 긴밀한 신규 협력체계 구축 및 신규 기술 개발, 고도화를 추진 중으로, '24. 4월, AI 앱인 '에이닷'의 전화 서비스에 'AI 스팸 표시' 기능을 추가
  - 모르는 번호로 전화가 걸려오면 화면에 피싱 주의, 스팸 주의, 스팸 의심 같은 문구가 자동으로 뜨게 되는 방식
  - 즉, 해당 번호로 온 전화를 이용자가 받지 않았거나, 받았더라도 금방 끊은 전화 사례를 AI가 분석해 스팸 위험 등급을 매김. "보이스피싱에 쓰이는 특정 번호 패턴을 학습해 등급 판단에 반영

70) 대한민국 정책브리핑, '보이스피싱' 대응 AI 기술·서비스, 민·관 협력으로 개발한다, 2024.6.3

• (KT, AI 스팸 수신차단 서비스) KT는 고객이 받고 싶지 않은 광고성 스팸 문자를 AI가 자동으로 차단하는 서비스를 개발

- KT는 3년간의 준비 기간 동안 일 평균 150만 건 이상의 스팸 데이터를 딥러닝 학습시켜 해당 시스템을 개발
- 기존에는 스팸 필터링 시스템에 새 스팸 문자 유형을 분석하고 반영하는 데 3개월 정도 걸렸으나, AI가 종전에 수작업으로 하던 부분까지 담당하면서 이 기간이 일주일 이내로 대폭 감소
- 사람이 하던 때보다 연 1,000만 건의 스팸 문자를 더 차단할 수 있게 됐고 차단 정확도 역시 99% 수준까지 발전
- 이외에도 KT는 IP를 추적해 스팸을 차단하는 'IP 기반 실시간 스팸 차단' 시스템, 보이스피싱 번호 긴급 차단 시스템인 '서킷브레이커(가칭)', AI와 빅데이터 분석 기술을 결합해 스팸 위험도를 알려주는 '스팸 위험도 문자 내 표시' 서비스 등을 '24년 중 출시할 예정

• (LG유플러스, 고객 피해 방지 분석시스템) LG유플러스는 사내에 보유한 고객의 피해대응 정보와 경찰청, KISA 등 외부 기관이 가진 정보를 종합 분석하는 솔루션을 개발

- 해당 시스템은 LG유플러스가 운영하는 'U+스팸차단'을 통해 수집한 차단정보(스팸번호·문구·URL 등)는 물론 네트워크 구간에서 수집한 정보를 종합하여, 특정 문구나 단어뿐 아니라 스팸 발신자가 주로 쓰는 내용 구성까지 파악해 차단
- 고객 피해 방지 분석 시스템은 공공시스템인 KISA 스팸종합 모니터링 신고내용과 경찰청 신고 데이터 등을 결합하여 머신 러닝을 통해 분석
- 한편, '23.9월에는 스팸문자 발송 서버를 추적해 원천 차단하는 '리다이렉티드 URL 트레이스(Redirected URL Trace)' 기술을 도입해 지금까지 누적 1,100만 건의 스팸 메시지를 차단

IV

시사점

4-1 디지털 민생범죄 대응 조직 강화 필요

▌국외 주요국은 피싱 등 범죄 대응 전담 조직으로 국가 사이버보안 기구 지정 및 규제 기관 설치 등 다양한 형태의 거버넌스를 구축하고 이를 중심으로 각 부처 간 공조 체계 수립

- **(미국)** 연방거래위원회(FTC), 연방통신위원회(FCC), 사이버보안 인프라 보안청(CISA)을 중심으로 피싱 등 범죄 대응 가이드라인 개발, 범죄 처벌 규정 제·개정, 피해자 보호 방안 등 추진
  - 특히, FCC는 이동통신 서비스 사업자를 대상으로 보이스피싱, 스미싱 등에 악용될 수 있는 유효하지 않은 전화번호 및 불법적 내용을 포함하고 있는 문자 메시지에 대한 차단을 의무화하는 정책 시행
  - 또한 CISA는 국가안보국(NSA), 연방수사국(FBI) 등과 함께 피싱 등 다양한 디지털 범죄를 예방·대응하기 위한 개인, 기업 대상 가이드라인 또는 지침을 개발하여 배포하고 있으며, 피싱 기법 및 사례 소개, 피해 완화 조치, 사고 대응 조치 등 분야별 지침 마련
- **(EU)** 유럽연합 집행위원회(EC)를 통해 피싱 등과 같은 사기 행위로부터 소비자를 보호하기 위해 스팸 방지법을 제정 및 개정하고 있으며, GDPR, eIDAS 등을 통해서도 디지털 범죄를 규제하고 있음
  - (스팸방지법) 피싱 등으로 인한 침해에 대한 개인정보보호 및 보안 관리 규정을 제정하고, 특히 소비자가 피싱, 스팸 등을 식별하고 회피할 수 있도록 서비스 제공업체를 대상으로 관련 정보를 공개하도록 의무화함
- **(영국)** 온라인 사기 전담 조직을 설치함으로써 피싱을 비롯하여, 스미싱 등 범죄 문제에 대해 정부가 적극적으로 해결하고, 피해자를 보호하고자 노력하고 있으며, 관련 정책·제도 수립 및 시행 중
  - 특히, 국가사이버보안센터(NCSC)를 통해 사이버보안 위협을 포함하여, 이메일 피싱, 보이스피싱, 피싱 사이트 등에 대한 탐지·분석하고, 이들을 예방·대응하는 지침과 관련 정보를 제공 중
- **(독일)** 연방정보보안청(BSI)을 중심으로 연방금융감독청(BaFi) 등이 협력하여 피싱 예방적 보안 조치 방법, 피해 사례 등의 정보를 공유하고 있으며, 금융사기 예방 등은 BaFi에서 담당하여 제공

- **(대한민국)** 국무조정실을 중심으로 보이스피싱 대응 범정부 태스크포스(TF)를 통해 부처 간 정보 공유 및 피해 신고 일원화를 도모하고, 정보보호 전문기관인 한국인터넷진흥원도 국민피해대응단 조직을 신설하여 국민 생활 범죄 대응에 총력

▌우리나라도 보이스피싱뿐만 아니라 피싱 등 디지털 민생범죄를 전담하는 조직 구성에 대해 적극적인 검토가 필요하며, 범죄 수단·범위가 전 세계로 확대됨에 따를 글로벌 협력 강화 필요

- 현재 보이스피싱을 중심으로 운영되고 있는 범정부 전담팀을 확대하거나 주요국과 같이 디지털 민생범죄 전담팀 구성을 통해 지능화·조직화하는 디지털 민생범죄의 대응과 규제 강화 방안 모색
- 해외 IP 또는 통신사로 우회, AI를 활용한 전 세계 발신 스팸과 보이스피싱 전화 등 대응 방안이 부족한 상황으로 이를 해결하기 위한 글로벌 협력 강화를 통한 대응 방안 마련 및 공동 기술 개발 필요

4-2 디지털 민생범죄 전반에 대한 정책 마련 필요

▌주요국의 피싱 및 스미싱 관련 정책 및 규제는 국가별 빈번한 형태의 피싱 피해 유형과 양상을 반영

- **(미국)** 컴퓨터사기남용법(CFAA), 전화소비자보호법(TCPA) 등을 통해 피싱 범죄에 대한 처벌과 피해자에 대한 구제를 시행하는 한편, 신원 도용 및 가정 억제법으로 불법 수집·신용 도용 등으로 인한 피싱을 범죄로 규정 및 처벌하고 있음
- **(영국)** 피싱 등을 온라인 사기 범죄로 규정하고 이를 대응하기 위한 전략을 발표하여 시행하고 있으며, NCSC를 통해 컴퓨터를 기반으로 하는 사기, 즉 피싱 전반에 대해 탐지·대응하고 있음
  - 또한 컴퓨터오남용방지법 1990, 사기법 2006 등을 통해 피싱에 의한 침해 행위 및 사기 행위를 각각 규정하여 강력하게 규제하고 있음
- **(일본)** 산업계 차원에서 기업과 일반인을 대상으로 한 피싱 피해 등에 대응하기 위해 대책 가이드라인을 제정함으로써 민간 주도의 자발적 규범을 형성하고 시행 중
  - 더불어, 범정부적 성격의 협의회와 경찰청 산하 피싱 대응 전담팀을 구성하여 운영하는 한편, 피싱에 대한 기본법으로 “사이버 시큐리티 기본법”을 따르는 등 관련 법률을 제정·시행 중

▌지속적으로 증가하고 있는 디지털 민생범죄로부터 국민을 보호하기 위한 예방·대응책 마련이 시급하며, 특히 피싱 범죄 전반을 규율할 수 있는 제도 마련 검토 필요

- 우리나라는 현행 통신사기피해환급법에 따라 피싱 범죄 중 보이스피싱에 대해 피해를 구제받을 수 있으며, 컴퓨터사용사기죄를 통해 피싱 범죄 피의자를 처벌할 수 있으나 피싱 전반을 규율하지 않음

- 특히 통신사기피해환급법은 보이스피싱 피해자가 계좌를 통해 피의자에게 금액을 송금 또는 이체하였을 경우로 한정하고 있으며, 피해자가 금융회사에 피해 사실을 신고 및 피해구제 신청을 하도록 하고 있음

• 따라서 피싱 범죄 전반에 규정하고, 범죄 예방과 대응, 피해 사실에 대한 처벌을 강화하고, 피해 구제 범위를 확대하는 등의 제도 개선과 함께 피싱 대응을 위한 종합적인 정책 마련 필요

4-3 디지털 민생범죄 대응 기술 개발 필요

▌주요국의 경우 통신 규제기관이 주축이 되어 통신사업자와 공동으로 기술 개발하여 서비스 중

• 미국 연방통신위원회(FCC)의 STIR/SHAKEN 표준 채택, 영국 통신 규제 기관인 Ofcom의 해외 VoIP 전화 차단 기술 개발, 독일 연방정보보안청(BSI)의 이메일 보안 전송 표준 기술 개발 작업 등은 네트워크 단에서 피싱 및 온라인 사기 공격을 차단하고자 하는 기술적 노력의 일환

• 우리나라 역시 기술 개발의 효용성 및 사회적 가치 제고 관점에서 규제 기관을 주축으로 통신사업자 또는 ISP 간 피싱 대응을 위한 공동 기술 개발을 위해 힘을 모아 협력하고 있음

- 더불어 국민이 많이 사용하는 SNS 플랫폼을 활용하여 피싱 의심 문자를 판단해 주는 스미싱 확인 서비스를 제공함으로써 단순 인식 제고 등 교육을 넘어 실제로 국민들이 스스로 피해를 예방할 수 있는 프로그램을 강화하고 있음

▌AI 등 新기술 기반 고도화되는 디지털 민생범죄 대응을 위해 정부를 비롯한 민간 분야에서도 적극적으로 노력이 필요하며, 피싱 대응을 위한 기술 개발 확대 검토 필요

• 디지털 범죄는 시간이 지남에 따라 더 정교하고 지능적으로 변화하고 있으며 특히 AI, 빅데이터, 음성 인식 등의 디지털 기술이 발전하면서 범죄자들은 이러한 기술을 악용하여 더 교묘하며, 피해 증가

- 특히, AI 딥보이스 이용한 신종 보이스피싱 수법, 정상으로 위장한 QR코드 스캔을 통해 스마트폰 악성앱을 설치하고 금융 정보를 빼가는 신종 큐싱(Qshing) 수법 등이 등장함에 따라 더 이상 개인의 노력으로 디지털 범죄를 방지하기 어려움
- 이에 정부(과학기술정보통신부)는 보이스피싱 범죄자들이 AI 기술을 악용하지 못하도록 이에 대한 대응책을 추진 중

• 과기정통부가 최근 7월에 발표한 보이스피싱 대응 방안에는 범죄통화데이터 공개, 통화 문맥을 분석하여 피싱 여부를 판별하는 AI 기술 개발을 추진하고 있음

- 이와 함께 대국민 피해 예방을 위한 교육 강화, 불법 스팸 차단 및 대포폰 개통 방지와 같은 구체적인 대책이 포함되어 있으며 향후 디지털 생활 범죄 확산 억제와 디지털 환경 오염을 줄이는데 기여할 것으로 기대

• 더 나아가 민·관 간 협력을 확대하여 AI와 같은 신기술을 활용한 범죄 수법에 대해 선제적으로 대응 및 예방, 스팸 등 범죄 악용 계정 차단 등 기술 개발 및 국민 인식 제고를 위해 노력 필요

참고 자료(Reference)

- 과기정통부, 디지털 경제·금융의 신뢰 기반 조성을 위해 '보이스피싱 척결 종합방안' 마련, 2020.6.24.
- 국무조정실, 보이스피싱 등 대책 관련 관계부처 회의, 2024.4.11.
- 국무조정실, 이제 보이스피싱 신고는 '112'로…피해구제까지 원스톱 처리, 2023.9.27.
- 대한민국 정책브리핑, '보이스피싱' 대응 AI 기술·서비스, 민·관 협력으로 개발한다, 2024.6.3.
- 세계법제정보센터, 보이스피싱 범죄에 대한 세계 각국의 처벌규정, 2022.09.28.
- 연합뉴스, 中, 보이스피싱 등 범죄 4년새 1천배 급증…'젊은층 공범' 확산, 2023.07.23.
- 정책브리핑, 통신분야 사기전화(보이스피싱) 대응 방안 발표, 2024.7.8.
- BBC, Ofcom asks phone networks to block foreign scam calls, 2021.10.25.
- Bolster, 2024 State of Phishing & Online Scams: Statistics, Facts, Trends & Recommendations, 2024.3.12.
- CISA, Phishing Guidance: Stopping the Attack Cycle at Phase One, 2023.10.18.
- EOS-EU, Recommendations on the Future of Security Research Towards Framework Programme 9
- EU, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on fighting spam, spyware and malicious software, 2006.11
- Experian, What's the Difference Between Phishing, Smishing and Vishing?, 2022.3.20.
- FCC, Targeting and Eliminating Unlawful Text Messages Report and Order and Further Notice of Proposed Rulemaking, 2023.3.17.
- Gartner, The Future of Sales Follow-Ups: Text Messages, 2019.10.4.
- Identity Week, German BSI joins FIDO Alliance, 2015.10.16.
- Phishing Tackle, Phishing Tackle introduce world's first simulated smishing-as-a-service, 2021.10
- Proofpoint, 2024 State of the Phish, 2024
- Spacelift, Top 54 Phishing Attack Statistics & Latest Trends for 2024, 2024.8.6.
- TSL Magazine, 不正アクセス禁止法とは？規制対象となる行為・改正の概要・違反事例も解説, 2020.1.14.
- UK Home Office, Fraud Strategy: stopping scams and protecting the public, 2023.5
- 公安部, 中宣部公安部联合部署在全国开展"全民反诈在行动"集中宣传月活动, 2024.06.25.
- 法治日报, "七大反诈利器"有效防范电信网络诈骗, 2023.06.21.
- 央视网, 国家安全部揭露"钓鱼"邮件常用伎俩, 2024.03.17.

- 人民网， 公安部就《电信网络诈骗及其关联违法犯罪联合惩戒办法（征求意见稿）》面向社会公开征求意见，2023.11.13.
- https://business.bofa.com/en-us/content/what-is-smishing-how-to-prevent-it.html#1
- https://ironscales.com/guides/phishing-prevention/smishing-vs-phishing
- https://www.antiphishing.jp/
- https://www.bafin.de/EN/Verbraucher/Finanzbetrug/Datendiebstahl/datendiebstahl_node_en.html
- https://www.bsi.bund.de/EN/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Spam-Phishing-Co/spam-phishing-co_node.html
- https://www.cps.gov.uk/legal-guidance/computer-misuse-act
- https://www.fcc.gov/call-authentication
- https://www.fcc.gov/general/frauds-scams-and-alerts-guides
- https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/phishing
- https://www.ftc.gov/news-events/news/press-releases/2024/02/ftc-proposes-new-protections-combat-ai-impersonation-individuals
- https://www.gesetze-im-internet.de/stgb/
- https://www.gov.uk/government/collections/hmrc-phishing-and-scams-detailed-information
- https://www.legislation.gov.uk/ukpga/2006/35/contents
- https://www.ncsc.gov.uk/collection/phishing-scams
- https://www.npa.go.jp/bureau/cyber/countermeasures/phishing.html
- https://www.ofcom.org.uk/phones-and-broadband/accessibility/general-conditions-of-entitlement/

www.kisa.or.kr

KISA INSIGHT

2024 VOL. 07
2024. 10.

KISA 한국인터넷진흥원