

# **보이스피싱 척결 대책 사전 브리핑**

2020.6.23(화) 15:00, 권대영 금융혁신기획단장(금융위원회)

<권대영 금융위원회 금융혁신기획단장>

디지털 혁신이 금융과 통신의 융합인 것 같습니다.

금융위에서 제가 나왔고 또 과기정통부에서 또 홍진배 국장님이 나오셔서요. 제가 전반적인 이야기를 말씀드리고 통신 분야에 특화된 부분은 국장님께서 추가 설명을 하겠습니다.

제가 전체적인 흐름을 설명을 드리겠습니다.

정부는 중대한 반사회적 민생침해 범죄인 보이스피싱을 척결하기 위해 전방위적인 예방·차단시스템 구축, 강력한 단속과 엄정한 처벌, 실효성 있는 피해구제 등을 담은 종합방안을 마련하여 시행하기로 하였습니다.

다음 쪽 추진 배경입니다.

디지털 기반 혁신성장의 이면에는 디지털 신기술을 악용한 신종수법에 따른 보이스피싱 범죄가 심각한 상황이고, 특히 스마트폰 사용이 대중화됨에 따라 대포폰, 악성앱 등 통신서비스 부정사용도 증가하고 있습니다.

보이스피싱은 개인뿐만 아니라 한 가정을 파괴하고, 나아가 금융·통신 인프라에 대한 신뢰를 저해하는 반사회적 범죄입니다.

그동안 보이스피싱 피해 규모가 감소추세이지만, 여전히 범죄수법·

수단이 지능화·고도화되고 있어 종합적이고 지속적인 강력한 대응이 필요한 상황입니다.

6월 22일 대통령께서도 반부패정책협의회에서 보이스피싱과 같은 민생침해 범죄에 대해 초기부터 강력하게 대응하고, 부처 간 공조를 강화하여 신속하게 대책을 마련할 것을 지시하셨습니다.

이에 관계부처 기관 합동으로 보이스피싱 종합 척결방안을 마련하여 신속히 집행·시행하고자 합니다.

3쪽 내일 장관님들 행사계획은 생략하도록 하겠습니다.

4쪽입니다.

보이스피싱 척결 종합방안은 하단에 있는 그림과 같이 첫째, 전방위적인 차단 시스템 구축, 단속과 처벌의 실효성 확보, 그다음에 종합적인 피해구제 강화, 관계부처의 상시 협업 체계 강화, 국민들의 경각심 환기입니다.

주요내용을 하나하나 설명드리겠습니다.

5쪽입니다.

첫째, 보이스피싱 범죄 시도가 성공하지 못하도록 통신과 금융 분야에서 전방위적인 예방·차단 시스템을 구축하겠습니다.

먼저, 통신서비스에 대한 강력한 부정사용 방지·차단대책을 마련하

였습니다. 휴대폰의 ‘개통-이용-중지’ 전 단계에 걸쳐 명의도용, 전화 번호 거짓표시 등 통신수단이 보이스피싱 범죄에 이용되는 자체를 사전에 방지하고, 한국인터넷진흥원 등에서는 보이스피싱·스미싱에 이용된 전화번호·악성앱·사이트 등을 보다 신속하고 철저하게 차단해 나갈 것입니다.

한편 금융회사의 경우에도 보이스피싱 의심거래를 적극 모니터링을 할 수 있도록 ‘FDS’라 하는데요. 이상금융거래 탐지시스템 구축을 의무화하고 고도화해 나가기로 하겠습니다. 이 과정에서 빅데이터나 AI 등 신기술을 적극 활용하도록 하고, 금융유관기관 간의 정보 집중과 공유를 강화해 나갈 것입니다.

또한, 금융회사와 통신업자의 책임과 의무도 강화해 나가겠습니다. 금융회사는 FDS를 통해 의심거래에 대한 모니터링을 강화하도록 하고, 통신업자도 통신서비스의 부정사용 예방활동을 강화하도록 할 것입니다.

6쪽입니다.

제도적으로는 안전하면서도 편리하게 계좌를 개설하고 국민들께서 금융거래를 이용할 수 있도록 디지털 신기술, 편리성, 안전성 등을 종합 고려하여 ‘금융분야 인증·신원확인 제도혁신 방안’을 3분기 중에 마련할 것입니다.

한편, 과기정통부 등 관계부처에서는 보이스피싱 예방에 디지털 신기술 개발·활용을 촉진할 수 있도록 시범사업 및 R&D 등을 지속 추진해 나갈 계획입니다.

둘째, 보이스피싱 범죄에 가담할 유인 자체를 없앨 수 있도록 보이스피싱 단속과 처벌의 실효성을 확보해 나가겠습니다.

먼저 관계부처 합동으로 연말까지 보이스피싱 등 민생침해 금융범죄를 일제히 집중·단속하여 나갈 것입니다. 수사당국은 국제적인 공조수사를 통해 허위 피해구제 사건은 엄정하게 수사하는 한편, 최근 증가하고 있는 메신저 피싱, 중계기 밀수, SIM박스라 그러는데요. 중계기 밀수 및 불법이용 등에 대해서도 집중 단속해 나갈 것입니다.

과기정통부에서도 통신사업자의 통신서비스 부정사용에 대해서도 일제히 점검하여 위법사항 적발 시 제재해 나갈 계획입니다.

보이스피싱 범죄에 대해서는 일반 사기범죄보다 훨씬 더 무겁게 처벌해 나가도록 하겠습니다. 관계부처와 협업을 통해 법정형을 강화하는 한편, 보이스피싱 조직에 대한 자금전달 등 관련 범죄행위에 대해서도 보다 명확하게 처벌할 수 있도록 관련법을 개정하겠습니다.

7쪽입니다.

금융회사 등의 배상책임을 대폭 강화하여 금융회사 등이 스스로 사전예방 조치를 적극적으로 수행할 수 있도록 하여 피해구제도 강화하고 소비자들도 두텁게 보호할 것입니다.

금융회사 등이 금융인프라 운영기관으로서 기본적인 책무를 다 하는 원칙을 확립하겠습니다. 금융소비자인 이용자의 고의·중과실이 없는 한 금융회사 등이 원칙적으로 배상책임을 지도록 하겠습니다. 다만, 이용자의 도덕적 해이 방지, 손해의 공평한 부담원칙 등을 고려하

여 금융회사 등과 이용자 간의 피해액이 합리적으로 분담될 수 있도록 하겠습니다. 현재 연구용역을 추진 중에 있으며 금융권과 충분한 의견수렴을 거쳐 구체적인 방안을 마련하도록 하겠습니다.

또한, 보이스피싱 피해를 보상할 수 있는 다양한 보험상품을 개발하여 통신대리점이나 은행창구 등에서 보다 간편하게 가입할 수 있도록 하겠습니다.

넷째, 보이스피싱 대책이 실효성 있게 집행되도록 관계부처 간 상시 협업체계를 구축해 나가겠습니다.

청와대 반부패비서관실 주관 T/F를 통해 금융위원회, 과기정통부, 수사당국, KISA, 금감원, 금보원, 금융회사, 통신사 등이 협업하여 대응하겠습니다. 이를 통해 금융과 통신사의 협업 그다음에 신종수법에 대한 효과적인 대응, 특히, 허위 피해구제의심 사건을 신속히 수사하여 피해구제를 가장한 악의적인 피해 신고도 수사당국이 방지할 계획입니다.

마지막으로 보이스피싱에 대한 홍보를 강화하여 국민들께서 보이스피싱을 당하지 않도록 경각심을 환기해 나갈 것입니다.

특히, 금융회사들은 100만 원 이상 입금 시 30분 인출이나 이체가 지연되는 지연인출제도, 지연이체서비스 등을 24시간 운영하고 있습니다. 국민들께서 이 서비스를 많이 활용할 수 있도록 계속 안내해 나가겠습니다.

또한, 보이스피싱 방지를 위한 전국민 대상 경고 문자를 긴급재난 문자와 같이, 수준으로 지속적으로 발송해 나갈 생각입니다.

마지막으로 국민 여러분께 드리는 말씀입니다. 이번 보이스피싱 척결 방안으로 디지털 기반 혁신성장의 이면에 나타나고 있는 보이스피싱 등 금융·통신을 이용한 범죄를 효과적으로 예방하고, 피해는 좀 좀히 구제할 수 있게 됨에 따라 국민들께서는 금융과 통신서비스를 보다 안전하고 편리하게 이용할 수 있는 디지털 경제의 신뢰 기반이 조성될 것으로 기대하고 있습니다.

국민들께서도 보이스피싱 등 금융사기·사고, 휴대폰 명의도용·악성코드 감염 등 정보보호·보안에 대해서 늘 특별한 경각심을 가지고 정보유출·재산상의 피해 등이 발생하지 않도록 지연인출·이체제도 활용 등 스스로를 지켜나가기를 간곡히 당부드리겠습니다. 이상 브리핑을 마치겠습니다.

하나 끝나고 나서 말씀드리고 싶은 내용은 이 대책 중에서 의미 있는 것은 통신 분야의 대책인데 국장님께서 곧 발표할 텐데, 상당히 저희는 의미 있다고 보고 있습니다. 그 분야가 추가 설명을 들으시면 될 것 같고요.

금융위 측면에서는 이 금융인프라를 국민들이 안심하고 이용할 수 있게 보이스피싱이 발생되면 원칙적으로 금융회사가 좀 스스로 이렇게 책임지는 그런 환경을 만들어야지, 금융회사가 FDS 시스템을 고도화한다든지 이런 피해방지를 노력하는 측면이 있습니다.

물론 국민들께서 보이스피싱을 알면서도 이렇게 송금을 했거나 그런 경우에는 구제가 되지 않겠지만, 가급적 금융기관들이 보상할 수 있는 그런 체계를 만들도록 하겠습니다. 또한, 처벌을 대폭 높였던 측

면, 그다음에 내일부터 연말까지 집중단속을 하는 그런 부분이 중요하고, 특히 어쨌든 이 부분은 국민들께서 스스로 지키는, 그래서 보이스피싱 10계명이라든지 특히 자연이체·인출제도를 언론에서 충분히 같이 홍보해서 대한민국에 보이스피싱이 발붙일 수 없는 그런 환경을 정부, 민간, 언론이 같이 만들어나갔으면, 그런 생각이요.

하나로 참고 말씀드릴 것은 이런 내용들이 하다 보면 국민들이 좀 불편해질 수가 있습니다. 그래서 또 혁신은 해야 되고 편리해야 되지만 또 이렇게 국민들의 재산을 지키고 보호를 하자면 또 절차가 번거로워지는 그런 측면에서 정부의 고민도 있기 때문에 저희가 이런 안전과 편리를 균형 있게 하는 그런 노력을 같이 기울여나가겠습니다. 언론인께서도 많은 이해와 협조를 당부드리겠습니다.

이상입니다.

<홍진배 과학기술정보통신부 통신정책관>

감사합니다. 과기정통부 통신정책관 홍진배입니다.

앞서 설명드렸듯이 지금 보이스피싱 관련해서 수법들이 굉장히 고도화되고 지능화되고 있습니다. 지금 금년에는 피해액이 좀 줄었습니다만, 지난 몇 년간을 분석해 보면 매년 한 2,000억씩 계속, 6,000억대까지 피해액이 증가하였고 금년 상반기에 좀 준 것은 사실 코로나19로 인해서 중국에서 활동하는 보이스피싱 조직들이 위축되었던 영향으로 보여지고 있고요. 지금 중반기부터는 다시 한번 예의주시해 봐야 되지 않을까, 그런 생각이 듭니다.



저희 자료는 통신사용 부정사용방지 대책인데요. 별첨2를 봐주시면 될 것 같습니다.

보이스피싱이 계속 이렇게 지능화, 고도화되고 있기 때문에 그간의 대책에 대한 보완과 함께 이번에는 AI나 빅데이터를 활용한 기술적 대책을 강화해서 병행 추진하는 데 중점을 두었습니다.

먼저, 그간의 대책에 대한 보완입니다.

첫 번째로, 대포폰이 보이스피싱의 시발점이기 때문에 악용 가능성이 높은 사망자라든지 폐업법인·외국인 명의의 휴대폰을 조기 정리하려고 합니다.

지금 현재는 약 5,900만 회선을 전수를 저희가 매년 2회를 하고 있습니다. 그것을 주기를 4개월로 단축해서 매년 3회로 강화하고, 법무부와 특히 협의를 마무리했는데요. 협조를 해서 단기 외국인 관광객이 출국 시에도 그 사람들이 썼던 선불폰이라든지 이런 것들을 즉시 정지시켜 놓을 수 있도록 그렇게 조치를 하겠습니다.

그리고 본인확인이 상대적으로 취약한 선불폰 등에 대해서 관리점을 강화하겠습니다. 주로 비대면 온라인 개통을 통해서 알뜰폰들이 많이 개통하고 있는데요. 이 선불폰 같은 경우에는 동일인 명의로 통신사를 바꿔가면서 또 대량 개통하는 사례도 발생하는 경우가 있습니다.

그래서 이에 대해서 비대면 개통 시 신분증, 그냥 플라스틱 신분증이 아니라 관련법상으로 정해놓은 수단들이 있습니다. 신용카드라든지 인증서라든지 이런 것을 통해서 본인확인 할 수 있도록 다시 한



번 가이드를 주고, 현장점검을 강화해서 그거를 위반하고 있는 업체들 같은 경우에는 제재할 수 있도록 그렇게 하겠습니다.

그리고 사용기간이 크게 도과된 선불폰들이 있습니다. 이런 것들에 대해서는 관련 업체와 협의해서 주기적으로 검증을 해서 정리해 나가도록 하고요.

그리고 단기간에 다회선이 개통되는 경우에는 가이드라인을 마련해서 이통3사를 통해서 자사 망에 팔려 있는 알뜰폰들이 있습니다. 적게는 수 개에서 많게는 한 10여 개씩 팔려 있는데, 그들의 알뜰폰에도 적용을 통합 관리해서 대포폰으로 악용되는 여지를 좀 더 차단해 나가도록 하겠습니다.

다음 페이지입니다.

공공기관이나 금융기관 전화번호 사칭 방지 노력을 강화하도록 하겠습니다.

현재 공공기관이나 금융기관 전화번호 사칭을 막기 위해서 저희가 위·변작 금지목록, 일명 화이트리스트를 만들어서 관리하고 주요 10개 통신사에다 그 DB를 나눠줘서 해외에서 유입되는 공공기관이나 금융기관 번호를 차단하는 그런 조치를 해오고 있는데요.

지금 현재는 여기에 홀이 있는 것이 주로 대표번호 위주로 DB가 작성돼서 공유가 되고 있는데, 이것을 일단은 저희가 주요 공공기관이나 금융기관의 경우에는 모든 보유 번호를 대상으로 해서 위·변작 금지목록을 만들고, 그 만드는 주기도 거의 실시간성으로 협업 체제

를 만들어서 진행해 나가려고 하고 있습니다.

네 번째로는 보이스피싱으로도 많이 사용되는 것이 해외에서 발신되는 인터넷전화의 국내전화 그리고 거기서 010번호로 변작돼서 나타나는, 허위 표시돼서 나타나는 것들이 많습니다.

특히, 회선설비를 임대하는 영세사업자를 통한 변작들이 많이 발생했었는데요. 저희가 영세사업자를 대상으로 해서 계도도 하는 한편, 집중 단속도 병행해 나가도록 하겠습니다.

그리고 문자발송 사업자들이 있습니다. 문자발송 사업자들이 한 650여 개가 있는데, 이들에 대해서 문자발송을 신청하는 사람들에 대해서 번호가 변작됐는지 이것을 집중적으로 확인하도록 저희가 의무를 강화하고 점검해 나가도록 하겠습니다.

그리고 이런 것들을 위반하는 사업자에 대해서는 과태료를 지금 현재 3,000만 원인데 5,000만 원으로 대폭 상향하도록 하겠습니다.

그리고 중요한 것이 국내에서 인터넷전화를 개통을 해서 해외로 가지고 가서 발신하는 경우가 있습니다. 주로 소위 얘기하는 070 번호를 가지고 중국이나 다른 데 가서 발신을 해서 마치 국내에서 발신하는 것으로 오인토록 하는 그런 것들인데요. 여기에 대해서는 국외 발신을 표시할 수 있도록 기술적 조치를 주요 사업자부터 취해 나가도록 하겠습니다.

다섯 번째로는 보이스피싱 등 범죄이용 전화번호에 대해서 신속한 이용 중지를 하도록 하겠습니다.

지금 전기통신사업법에 보이스피싱에 사용된 전화번호는 중지할 수 있도록 되어 있습니다마는, 여러 행정기관을 거치는 과정에서 한 3~4일 정도가 소요되는 것으로 저희가 파악하고 있습니다.

여기에 대해서는 저희가 절차 간소화라든지 자동적인 시스템 구축을 통해서 최대 1일 이내로 처리할 수 있도록 저희가 최대한 노력하겠다는 말씀드리겠습니다. 물론 상황에 따라서는 그리고 사업자에 따라서는 하루 정도 더 소요될 수는 있겠습니다마는 저희가 최대한 단축해서 추진을 해 나가도록 하겠습니다.

그리고 이용 중지된 전화번호는 타 사로 번호이동을 하는 경우에도 이용을 할 수 없도록 저희가 조치를 하고, 이용중지 기간, 소위 애기하는 에이징 기간이라고 합니다. 그 번호를 사용하지 못하도록 하는 건데 그 기간을 1년에서 1년 6개월 이상으로 좀 늘려서 그 번호들이 오랫동안 사용될 수 없도록 이렇게 조치하도록 하겠습니다.

다음 3페이지입니다.

다음은 기술적 대응에 대한 강화입니다. 그간에는 이런 제도적 대응 위주로 보이스피싱에 대한 대응을 해 왔는데요. 이 기술적 대응을 잘 활용하는 경우에는 좀 더 효과적으로 조금 더 발전된 대응을 할 수 있지 않겠느냐는 생각을 좀 해서, 저희가 빅데이터 시범사업을 통해서 정보에 대한 통합분석과 보이스피싱에 대한 음성 문맥에 대한 기계학습을 저희가 지원을 해서 이런 기반이 되는 기술을 지속적으로 고도화를 해 나갈 계획입니다.

그래서 음성패턴이나 이런 것들을 음성지문이라고 하는데, 그런 것들을 그 DB를 꾸준히 축적해서 스타트업이라든지 관련 기업들이 이것을 활용해서 피싱탐지앱이라든지 그것을 방지하는 예방적·기술적 조치를 취할 수 있도록 그렇게 하고요. 이를 은행의 FDS하고도 연계해서 실질적 피해예방에 기여할 수 있도록 하겠습니다.

이렇게 개발된 기술이나 알고리즘 같은 경우에는 일반에도 당연히 공개를 해서 관련 기업들 활용이라든지 스타트업들이 활용할 수 있도록 그렇게 하도록 하겠습니다.

다음 4페이지입니다.

이런 단기적인 빅데이터 기반의 시범사업뿐만 아니라 능동적·선제적 예방을 위한 R&D 작업도 추진을 하려고 하고 있습니다.

이미 저희가 R&D 기획예산을 저희가 확보를 해서 내년도에 수행할 수 있도록 금융위나 경찰청으로부터 기술개발 수요를 지금 받아서 기술개발 로드맵을 마련하려고 하고 있습니다.

주요 기술의 예시로는 해킹이나 바이러스를 통한 그런 것들과 연계된 신·변종 보이스피싱에 대한 능동적 대응기술이라든지, 아까 SIM박스 문제가 나왔습니다마는 SIM박스에 대한 어떤 패턴분석을 통해서 보이스피싱을 추적해 나가고 차단할 수 있는 그런 기술개발들을 기술적 대책부터 마련하도록 하겠습니다.

기타는 통신과금 서비스, 휴대폰 소액결제라고 하는데요. 이것에 대한 내구제 대출 같은 것들이 청년층이나 저소득층에서 문제가 되는

경우가 있습니다. 이것에 대해서도 통신사나 PG사의 고객이력관리를 시스템적으로 연계하고, 부정이용자에 대한 정보 공유를 강화해서 대응해 나갈 계획이고요. 그리고 저신용자나 미납이력자의 경우에는 이용한도를 하향해서 조치할 수 있도록 그렇게 하겠습니다.

다음으로 5페이지입니다.

휴대전화 도난방지기술이라고 혹시 '킬스위치(Kill Switch)'라고 혹시 들어보셨는지 모르겠습니다. 아마 지금 휴대폰에 보시면 환경설정 에 가시면 '내폰찾기'라고 많이들 되어 있는데요. 그게 굉장히 사실 유용한 기술임에도 불구하고 활용을 잘 못 합니다.

그게 아마도 2014년경에 우리나라 폰에 다 대부분 도입됐었는데 당시에는 굉장히 사용하기가 좀 어려웠습니다. 제조사에 따로 가서 자기 고유번호를 다 등록을 하고 나중에 폰을 잃어버렸을 때 조치를 할 수 있는 그런 것인데, 이 킬스위치 기능을 활용을 하게 되면 내 폰을 잃어버렸을 때 어디로 갔는지 찾을 수도 없는 상황이 됐다고 가정을 했을 때는 이 킬스위치를 operation할 수 있는 사이트, 지금은 구글이나 애플에서 많이 제공해주고 있는데요.

거기 안드로이드나 애플 ios 사이트에 들어가셔서 나에 대한 정보를 입력하게 되면 원격제어해서 자기 정보를 다 밀어버릴 수가 있습니다. 그래서 거기 안에 있는 사진 정보라든지 주소록, 모든 정보를 남들이 볼 수 없게 다 원격에서 다 제거를 할 수 있거나 아니면 잠금을 해버릴 수도 있거든요.

그런 것들을 그때 도입 당시에는 홍보를 많이 해서 사람들이 알았

었는데 그 당시에는 사용하기가 좀 불편했고, 지금은 환경설정에서 사실은 다 디폴트값으로 사용할 수 있도록 설정돼서 나옵시다만 사람들이 폰을 잃어버렸을 때 몰라서 못 쓰는 경우가 좀 많은 것 같습니다. 그래서 이것들도 저희가 이용이 미흡한 측면이 좀 있어서 통신사 유통망이라든지 관련 협회 등을 통해서 이용법에 대한 안내라든지 이런 것들을 강화해 나갈 계획입니다. 언론에서도 관심을 가져주시면 좋을 것 같고요.

그리고 분실·도난 폰 같은 경우에는 외국으로 나가서 사실 활용되는 경우가 좀 많습니다. 왜냐하면 국내에서는 분실폰이나 도난폰은 휴대폰을 개통할 수 없도록 저희가 막아놨기 때문에 국내에서 사용은 못하고 밖으로 나가서 쓰는데, 이것들도 GSMA 세계이동통신사업자 협회들하고 협력을 해서 해외에서 적어도 여기에 가입된 사업자들에게서는 개통이 안 되도록 저희가 좀 노력을 해나가겠다, 이런 생각을 갖고 있습니다.

그리고 마지막으로 아까 우리 금융위에서도 관계기관 간의 협력을 굉장히 강조를 해주셨는데, 저희가 이것을 어떤 기술적으로 핫라인을 만들어서 관계기관 간 협의체를 만들려고 합니다. 그래서 정책 협력뿐만 아니라 관련 정보나 수법 이런 것들이 좀 더 체계적이고 신속하게 공유될 수 있는 체계를 만들어서 보이스피싱 대응역량을 지속적으로 좀 강화해 나가겠다, 이렇게 말씀드리겠습니다.

이상 발표를 마치겠습니다. 감사합니다.

## [질문 · 답변]

※마이크 미사용으로 확인되지 않는 내용은 별표(\*\*\*)로 표기하였으니 양해 바랍니다.

<질문> 단장님께 두 가지 여쭙보고 싶은 게 금융사의 책임을 강화한다고 하는데 이 보이스피싱 피해자는 본인의 의지를 가지고 송금, 송금을 하게 되지 않습니까? 그러면 결국 금융사들은 이 사람이 피해자가 책임이 더 크다, 책임 소재는 서로가 더 떠넘기려고 할 건데 이것을 개략적으로나마 어떤 기준으로 해서 대체로 어느 정도 이상은 금융사가 책임을 지고 변제를 하게끔 하는 방향이 있는지 궁금하고요.

보험, 또 하나 여쭙보면... 보험 쪽 이야기하셨는데 여기 내용 보면 그 금융소비자가 자발적으로 보험을 가입하는 것으로 저는 이해를 했거든요. 그런데 이게 금융소비자가 그 보이스피싱 보험을 가입하는 게 맞는지 아니면 금융기관이 적극적으로 그런 보험제도를 만들어서 금융기관이 보험비용을 부담해서 이걸 대응해 나가는 게 맞는지, 이것에 대한 거 설명 좀 부탁드립니다.

<답변> (권대영 금융위 금융혁신기획단장) 책임이라는 것은 인프라에 대한 운영자로서의 기본적인 어떤 책무라는 그런 대원칙을 말씀드리는데 접니다. 구체적으로 가면 과실여부라든지 이런 부분을 좀 따져야 되겠지만 기본적으로 '아, 이 시스템에 대해서는 내가 좀 책임을 진다.'는 이런 금융기관의 그런 자세가 필요하다는 거고 구체적으로 소비자가 만약에 말씀대로 알고 '이거 보이스피싱입니다. 보내시면 안 됩니다.'라고 함에도 불구하고 보냈던 경우에는 금융기관이 극단적으로 책임질 이유는 없겠죠.

해외의 경우에도 이런 인프라 기관의 어떤 책무를 강화하는 그런 추세를 감안해서 저희가 현재 연구용역을 하고 있습니다. 그러한 연



구용역이 나오면 합리적인 어떤 기준과 원칙을 마련하고 금융권하고 소비자의 의견을 충분히 수렴하여 구체적인 방안을 마련할 생각이고, 제가 오늘 말씀드린 것은 큰 원칙에 대해서 말씀드렸고 그러한 원칙이 작동돼야지 국민들이 이 시스템을 안심하고 이용할 수 있고요.

또 금융회사는 반대로 아까 과기정통부에도 이야기했지만 신기술을 통한 또는 FDS를 통한 예방노력을 굉장히 할 것이고, 그렇게 함으로써 이 보이스피싱 자체를 이렇게 줄여나가는 효과가 있다고 판단을 하고 있습니다.

그다음에 보험은 제가 알기로는 아주 소액으로 알고 있습니다. 몇 백 원 정도 하는 것인데 당연히 우리 기자님 말씀대로 제가 좀 좋은 보험은 기본적으로 가입할 수도 있을 것이고요. 아니면 금융회사가 이것을 시스템을 이용하는 국민들을 위해서 아예 탑재를 해서 팔 수도 있는 것이고, 그것은 금융회사와 소비자가 결정할 이유고, 이유라고 이렇게 설명드리면 될 것 같습니다.

하나만, 제가 그... 계속 브리핑하는 것 때문에 장관님들 현장방문을 말씀 안 드렸는데요. 자료 3페이지에 보면 아주 좋은 사례가 시연이 있습니다. 그래서 아마 방송을 하실 때 그 부분을 내일 따시면 좋을 것 같은데, 여기 보면 3페이지 하단에 신한은행에서 한 것은 만약에 악성앱이나 원격제어앱이 설치되어 있으면 모바일뱅킹이 딱 중단되는 이런 것을 아마 시연해 줄 것이고요.

지금 예컨대, 전화 음성하고 범죄자의 음성을 DB로 분석하는 그런 탐지 시범 이런 것들이 내일 현장에서 시연될 것이고, 양 장관님들이 오시니까 아마 구체적인 국민들한테 도움 되는 사례는 내일 아마 현

장에서 취재하시면 될 것 같습니다. 이상입니다.

<질문> \*\*\*

<답변> (권대영 금융위 금융혁신기획단장) 예, 지금 저희가 연구용역 몇 월까지...

<답변> (이한진 금융위 전자금융과장) 정부입법... 지금 제일 마지막 페이지, 상세자료 마지막 페이지 보시면 저희가 이런 보이스피싱 종합 척결방안 중에 대체로 과기부에서 얘기하시는 통신서비스 부정사용방지대책이라든지 저희 지금 현행법 해서 할 수 있는 것은 즉시 추진을 하고 관련 T/F를 통해서 계속 청와대에서도 점검을 하실 계획입니다.

그런데 그 밖에 법 개정이 필요한 사항 중에 대표적인 게 기자님이 질의하셨던 지금 금융사 배상책임강화 같은 것들은 법 개정이 필요한 사항이고요. 그것을 정부입법으로 추진하기 위해서는 아시다시피 입법예고를 해서 의견수렴 과정도 거치고요. 그렇게 해서 2020년 말까지 국회에 제출하게 되니까요. 입법예고 전까지 저희 금융위에서 입법예고를 할 때 그때까지 정책 연구용역 결과를 마무리해서 반영해서 아마 발표될 것 같습니다.

<답변> (권대영 금융위 금융혁신기획단장) 제가 지금 이 부분이 좀 새로운 내용이고 생소할 수 있어서 아마 관심이 높고 '이게 뭐냐.' 이런 이야기가 있어서 조금 설명을 드리면, 보이스피싱은 자기가 잘 모르고 당할 수가 있거든요. 국민들이 노력하더라도 잘 모르고 당할 수 있기 때문에, 그런데 이 모든 책임을 그냥 개인의 책임으로 하기에는 이 인프라를 이용하는 국민들한테 기울어진 운동장인 것 같아요.

그래서 뭔가 좀 금융회사들이 조금 더 이렇게 열심히 할 수 있는, 그래서 예컨대 우리 카드 부정사용에 대해서는 카드사가 기본적으로 보상을 해주지 않습니까? 그러니까 국민들이 굉장히 안심하고 카드를 썼고 그렇게 함으로써 우리나라의 신용카드 시장이 굉장히 커졌거든요. 그런 최소한의 어떤 의무를 금융회사가 할 수 있는 그런 대원칙을 마련하자는 그런 내용이고, 구체적인 것은 지금 연구용역 결과를 가지고 공청회도 하면서 금융회사의 의견을 충분히 수렴하겠습니다.

아까 말씀드린 대로 도덕적 해이가 또 일어날 수 있는 부분이기 때문에 그 합리적인 수준을 결정하는 것이 우리에게 주어진 과제라고 생각하거든요. 그런 관점에서 이해를 부탁드립니다.

<끝>