JDCS
디지털콘텐츠학회논문지
Journal of Digital Contents Society
Vol. 19, No. 1, pp. 193-198, Jan. 2018

보이스피싱에 대한 경찰의 대응방안에 관한 연구

김 덕 용*
*충북보건과학대학교 경찰행정과

A Study on Voice Phishing Countermeasures of the Police

Duck-Yong Kim*
*Department of Police Administration, ChungBuk Health & Science University, Chungbuk, Korea

[요 약]

우리나라는 인터넷과 전화 및 스마트기기 보급률이 세계 최고 수준에 이르고 있다. 이러한 인프라를 악용한 사이버금융범죄는 지속적으로 발전하고 있다. 2006년 5월에 국내 최초로 보이스피싱 범죄가 발생한 이후, 10년이 지난 현재까지 보이스피싱 범죄는 지속적으로 발생하고 있다. 보이스피싱이란 피해자에게 허위의 내용으로 전화를 걸어, 피해자의 계좌번호 및 패스워드 등을 알아내어 금전을 편취하는 범죄이다. 이러한 보이스피싱은 그 수법이 날로 진화 · 발전하여 수사에 어려움을 격고 있다. 보이스피싱의 대부분은 중국 등 동남아시아에 그 본거지를 두고 활동하는 국제조직범죄의 형태로써 국제협력수사에 의하지 않고는 근절이 쉽지 않다. 이에 본 연구는 보이스피싱 범죄에 대한 발생실태와 사례분석을 하고, 경찰의 보이스피싱에 대한 대응방안을 살펴본 후, 이에 대한 개선점을 제시하고자 한다.

[Abstract]

In Korea, the penetration rate of Internet, telephone and smart devices is reaching the highest level in the world. Cyber financial crimes that exploit such infrastructures continue to evolve. Since the first Voice Phishing crime in May 2006, ten years later, there has been a constant occurrence of Voice Phishing crime. Voice Phishing is a crime in which a victim is phoned for false information to figure out the victim's account number and password. This method of Voice Phishing evolves day by day, and it is difficult to investigate. Most of Voice Phishing is a form of international organized crime that is based in Southeast Asia such as China, and it is not easy to eradicate by international cooperation investigation. The purpose of this study is to investigate the actual situation and case analysis of Voice Phishing crime, and to propose the countermeasures against police Voice Phishing counterplan.

색인어 : 개인정보유출, 보이스피싱, 사이버금융범죄, 신종사기, 전화사기

Key word : Data Spill, Voice Phishlng, Cyber Financial Crime, New Fraud, Phone Fraud

http://dx.doi.org/10.9728/dcs.2018.19.1.193

Received 21 November 2017 ; **Revised** 23 January 2018
Accepted 29 January 2018

***Corresponding Author;** Duck-Yong Kim

Tel: +82-010-3427-1912
E-mail: dykim@chsu.ac.kr

Ⅰ. 서 론

현대 사회는 교통과 통신의 발달로 인하여 국,내외를 자유로이 드나드는 것은 물론, 통신의 발달로 인하여 전세계는 지구촌 시대라고 일컬을 만큼 긴밀한 관계를 유지하고 살고 있다. 특히 우리나라는 세계 최고 수준의 IT인프라를 바탕으로 IT최강국으로 자리매김 하고 있다. 특히 최근 첨단 정보통신기술이 경제·사회 전반에 융합되는 4차 산업혁명이 도래하고 있다. 형사법 분야에서도 이에 따른 영향을 받아 지능범죄, 동기범죄 등이 증가하고 있다[1][1]현재의 과학기술정보통신부(구, 미래창조과학부)에서 실시한 2015년 인터넷이용 실태조사에 의하면, 인터넷접속률이 전체 가구의 98.8%에 이르고, 만 6세 이상 인구의 82.6%가 스마트기기를 보유하고 있는 것으로 조사되고 있다[2]. 이러한 인프라를 악용한 사이버금융범죄는 지속적으로 발생하고 있으며, 최근에는 랜섬웨어, 이메일 무역사기 등 신종범죄의 확산도 가속화 되고 있다. 2015년 사이버 범죄는 총 144,679건이 발생하였고, 그중 사이버금융범죄가 14,686건(약 10.1%)이며, 사이버범죄는 전년대비(110,109건) 31.4% 증가했다[3]. 위와 같은 사이버금융범죄 중에서 2006년 5월 18일에 국내 최초로 인천의 우리은행 간석동지점에서 국제전화금융사기범죄(이른바, 보이스피싱)가 발생한 이래(국세청은 2005년 11월 14일 국세청을 사칭하는 환급사기사건이 최초라고 주장하고 있다), 현재에 이르기까지 지속적으로 발생하고 있다[4]. 일명 '보이스피싱(Voice Phishing)'이라고 부르는 전화금융사기는 주로 해외에서 범행이 시도되며, 인터넷전화(VoIP, Voice over Internet Protocol)와 현금자동입출금기(ATM, Automated Teller Machine) 등 사회적 인프라가 잘 갖추어져야 범행이 가능한 선진국형 범죄이다[5]. 보이스피싱(Voice Phishing)이란 용어의 피싱(Phishing) 이라는 출처에 대하여는 통상 개인정보(Private Data)와 낚시(Fishing)를 합성한 신조어라는 주장이 있고, 다른 주장으로는 비밀번호의 낚시(Password Fishing) 혹은 세련된 절도기법(Sophisticated Fishing)의 약어라는 주장이 있다[6].

현재 정부기관에서는 '전화금융사기'라는 용어를 사용하고 있는데 반하여, 언론에서는 '전화사기', '전화금융사기', '보이스피싱 사기' 등의 용어를 혼용하고 있으며, 일반인들은 '전화사기'라는 용어를 사용하고 있는 것으로 보인다. 그러나 최근의 범죄양상을 보면 전화상으로 자녀를 납치하여 보호하고 있다며 협박하여 금전을 갈취하는 형태의 보이스피싱이 나타나고 있는데, 필자의 사견으로 이는 '전화사기범'이라기보다는 '전화공갈범'이라고 보여 진다. 어찌되었든 이러한 보이스피싱은 금융기관 등의 웹사이트나 거기서 보내온 메일로 위장해 개인의 인증번호나 신용카드번호, 계좌번호 및 패스워드 등을 불법적으로 알아낸 후 이를 범죄에 이용하는 사기수법으로써, 여기에 음성(Voice)을 더하면 전화를 통한 피싱사기, 즉 보이스피싱(Voice Phishing)을 일컫는 말이다[7]. 이러한 보이스피싱은 이미 일본이나, 중국, 대만 등지에서 발생하였던 것과 같은 양상으로 우리나라에서도 그대로 반복되고 있으며, 처음에는 세금환급금을 빙자하여 문자발송 형태의 사기 유형에서 시작하여 수사기관·금융기관·우체국 등 각종 기관사칭 유형 또는 자녀납치 빙자 유형 등의 수법으로, 최근에는 개인신상정보 수집을 통한 신뢰유형, 대출빙자 수수료 편취유형, 휴대폰 소액결재 악용을 통한 편취유형 및 허위 인터넷 사이트를 개설한 후 개인금융정보를 취득하여 인터넷 뱅킹을 통해 송금 편취유형 등 그 수법이 매우 다양해지고 있다. 보이스피싱의 발생은 2015년까지 총 59,690건, 피해액은 약 6,800억원에 이르고 있으며[8], 우리나라에서 발생하고 있는 보이스피싱의 경우 주범 및 콜센터는 주로 중국 내에서 활동하고 국내에서는 계좌개설팀·송금팀·인출팀 등 역할을 분담하여 점조직으로 활동하여 추적에 어려움을 겪고 있다. 또한 보이스피싱은 중국 내 조선족 등 우리말 구사가 가능한 사람들이 중국에서 우리나라의 부유층보다는 생업에 바빠 전화금융사기에 대한 범죄정보에 상대적으로 취약한 서민, 노인, 가정주부 등에게 피해가 집중되고 있다. 그런데 최근에는 중국을 벗어나 태국 및 베트남 등지로 범위를 넓혀 활동하는 등 보이스피싱이 발생한지 10여년이 넘도록 꾸준히 진화·발전하고 있다.

이에 본 연구는 우리나라에서의 보이스피싱의 발생실태를 분석하고, 그에 따른 경찰의 대응방안을 살펴본 후 이에 대한 개선점을 제언 및 결론을 제시하여 보이스피싱을 근절하는데 일조 하고자 한다.

Ⅱ. 보이스피싱의 발생실태 및 분석

2-1 보이스피싱의 발생실태

1) 지난 10년간의 발생실태

표 1. 10년간 보이스피싱의 발생현황
Table 1. Present condition of Voice Phishing Crime by 10 years

년 도	2006년	2007년	2008년	2009년	2010년
발 생	1,488건	3,981건	8,454건	6,720건	5,455건
년 도	2011년	2012년	2013년	2014년	2015년
발 생	8,244건	5,709건	4,765건	7,635건	7,239건

위 표에서 보면, 2006년에 발생된 1,488건은 경찰청 통계가 시작된 이래 2006년 6월부터 12월까지의 피해발생 건수를 산출한 것이며, 보이스피싱이 발생한 이래 10년이 흐른 2015년까지의 보이스피싱의 발생 건수는 총 59,690건으로 산출되고 있다. 위 자료를 보면 2008년 발생 건수가 8,454건으로 2007년 3,981건 대비 112%가 상승하였고, 2009년에는 전년도 대비 21% 감소하였고, 2010년에는 전년도 대비 19% 감소하였다가, 2011년에는 8,244건으로 전년도 대비 51% 상승하였다. 이후 2012년에는 전년도 대비 31% 대폭 감소세를 보였으며, 2013년에는 전년도 대비 17% 감소하였지만, 2014년에는 전년도 대비

약 65% 급성장 하였고, 2015년에는 전년도 대비 약 5% 정도의 감소함으로써 그 추세가 유지되고 있다. 이처럼 3년 주기로 급격한 발생과 감소를 반복하고 있다고 볼 수 있다.

2) 보이스피싱의 피해사례

보이스피싱의 피해사례를 검토하면 크게 세 가지 형태로 대별되는데, 첫 번째 형태는 여러 가지 수단과 방법을 이용하여 현금인출기로 피해자들을 유인 한 후, 보안번호설정을 새로이 해야한다며 피해자들을 속여서 계좌번호와 비빌번호를 입력하게 한 후 이를 계좌이체 받아 편취하는 형태로써, 이는 전형적인 보이스피싱(전화금융사기)이다. 그리고 두 번째 형태로 자녀 등을 납치하고 있다고 피해자인 가족들을 협박하여 금전을 송금하지 않으면 풀어주지 않겠다고 협박을 하여 공갈범의 형태를 띠는 차명계좌송금형 범죄가 있다. 마지막으로는 피해자에게 직접 현금을 인출하게 한 후 인출한 현금을 사기수법 혹은 절도 등의 수법으로 현금을 편취 또는 절취하는 형태이다. 이하에서는 위 세 가지 형태의 보이스피싱의 사례에 대하여 살펴본다.

(1) 보안번호설정 등을 빙자한 계좌이체 형태

보안번호설정 등을 빙자한 계좌이체 형태는 2006년 최초의 범죄 이래 현재에 이르기까지 자행되고 있는 전형적인 보이스피싱의 사례로써, 이른 바 환급금, 연체금, 카드명의 도용빙자, 사건연루 빙자 등 다양한 형태의 공공기관 혹은 금융기관, 통신회사 등의 직원임을 사칭하여 보이스피싱을 통해 금전을 편취하는 형태이다. 사례를 살펴보면 ①국세청, 연금관리공단, 건강보험관리공단의 직원이라고 사칭하여 과·오납된 세금 혹은 연금, 보험금 등을 환급 또는 납부하라고 유인한 후, 현금인출기에 현금카드 혹은 신용카드를 넣고 전화로 불러주는 기관의 인증코드를 입력하라고 속여 계좌이체를 하도록 유도한 후 이를 인출하거나, 혹은 직접 계좌번호와 비밀번호를 입력하도록 유도하여 송금하도록 한 후 이를 편취하는 형태이다. 이러한 형태는 범인들이 피해자들에게 개인정보나 계좌정보를 알려주어 범인들이 그 정보를 악용하는 것이 아니라, 피해자들이 직접 계좌이체에 필요한 정보를 입력하도록 유도하여 이체가 되는 형태로써, 피해자들이 입력하는 정보가 해당 기관의 인증번호라고 착오를 일으키기 때문에 계좌이체를 해준다는 사실을 쉽게 알아차리지 못하는 경우가 대부분이다[9]. 또 다른 사례로는 ②은행, 신용카드사, 금융감독원, 은행연합회 직원 등을 사칭하여 카드대금이 연체되었다고 피해자들을 속여 개인정보가 유출되어 보안설정을 새로 해야 한다며 현금인출기로 유인한 후, 보안설정코드를 입력하라고 속여 계좌이체를 하도록 한 후 이를 편취하는 유형이다. 이러한 유형은 위에서 살펴 본 환급금 빙자 전화사기형과 유사한 방법으로 금전을 편취하는 수법이다. 이러한 유형이 발전된 형태로 금융기관 직원을 사칭하는 것을 벗어나, 검찰이나 경찰 등 혹은 통신회사의 직원임을 사칭하여 편취하는 등 다양한 직업군을 악용하여 전화사기 범죄를 저지르고 있다. 이와 유사한 사례로 ③수사기관을 빙자하여 피해자 명의계좌가 사기사건과 연관되어 있어 이를 보호해 준다는 명목으로 현금인출기로 유도한 후, 예금보호 설정번호를 입력하라고 계좌이체를 하도록 하여 편취하는 유형이 있다.

(2) 사기 또는 협박을 통한 직접 송금유도 또는 강요 형태

위와 같은 유형 이외에도 피해자에게 전화하여 피의자의 자녀가 먼 타지에서 교통사고가 발생했다며, 피해자를 속인 후 지금 즉시 수술을 해야 하는데 우선 수술보증금을 송금해 달라고 요구하여 피해자가 직접 송금을 하도록 유도하는 형태 및 신용불량자 등 대출이 어려운 사람들에게 대출해주겠다며 신용조정비용 등 각종 수수료 명목으로 현금을 송금 받는 형태가 있으며, 다른 형태로는 피해자의 자녀에 대한 개인정보를 사전에 입수한 후, 피해자에게 전화하여 자녀를 납치하여 데리고 있다고 속인 후 돈을 송금해 주지 않으면 자녀를 해치겠다고 거짓협박을 하여 대포통장으로 금전을 송금하게 하여 편취하는 유형이 있다. 이러한 유형은 피해자 혹은 피해자 주변 가족의 신상정보를 사전에 입수한 후 특정한 사람을 대상으로 한다는 점에서 차이를 보이고 있다[10].

(3) 피해자가 직접 인출한 현금을 사기 또는 절도 형태

최근 새로운 형태의 보이스피싱으로 각종 제도개선으로 대포통장의 수급이 원활하지 않게 되면서, 피해자에게 보이스피싱을 통하여 직접 현금을 인출하게 한 후, 피해자를 직접 만나 위조한 신분증·공문서를 보여주며 해당기관의 직원임을 사칭하여 돈을 건네받는 사기형태가 있으며, 또는 집안의 안전한 장소나 냉장고·세탁기 등에 현금을 보관하게 한 후 피해자가 집을 비운 사이에 돈을 절취하는 수법의 현금절도 유형이 있다[11].

2-2 보이스피싱의 발생실태 분석

1) 보이스피싱의 일반적인 특징

보이스피싱의 주범과 유인책이라 할 수 있는 콜센터는 대부분 중국 또는 대만 등지에 위치하고 있으며, 최근에는 태국, 베트남 등지로 그 본거지를 확대하고 있다. 이들 외국인들은 주로 유인책 혹은 현금의 인출, 송금 등을 담당하고 있으며, 내국인들은 대부분 범죄에 이용된 계좌를 만들거나, 인출, 송금하는 것을 분업화 하여 범행을 자행하고 있다. 이는 오늘날의 범죄가 국제화 되고 있는 추세에 발맞추어 내, 외국인을 가리지 않고 국제적으로 조직화 하고 있다고 볼 수 있다. 즉, 위와 같은 보이스피싱은 한국과 중국 등 동남아를 활동 영역으로 하면서 내, 외국인이 각각의 범행 역할을 분담하면서 범행하는 국제조직범죄의 형태를 띠고 있다. 또한 국내에 입국한 유학생들이 예금계좌를 개설해 주거나, 불법체류자들이증가하

면서 보이스피싱범죄조직과 연계되어 현금인출 및 중간 연락책 등의 역할을 수행하는 경우도 있다.

또한 보이스피싱의 범행장소를 살펴보면, 위에서 보는 바와 같이 국내를 벗어나 중국 전역을 넘어 동남아시아까지 확대되어 범행이 자행되고 있는 점에 비추어 보아 범인검거에 상당한 어려움을 초래하고 있는 것으로 분석되어 진다.

그리고 범행의 수법에 있어서 초기에는 기관의 직원임을 사칭하여 현금인출기로 유인한 후, 보안설정변경 등의 단순한 거짓말로 계좌번호를 입력케 하여 금전을 편취하는 형태의 범행수법에서, 그 후에는 유출된 개인정보를 이용해서 특정인에게 보이스피싱을 통한 금융사기범죄로 그 수법이 진화되고 있으며, 최근에는 보이스피싱을 통하여 피해자가 직접 인출한 현금을 사기수법으로 편취하거나, 집안에 보관케 한 후 절취하는 수법 등 날로 그 방법이 교묘해지고 진화하고 있으며, 보이스피싱이 일명 대포통장을 이용한 차명계좌를 이용하고 있어서 수사기관에서는 수사의 어려움을 겪고 있다[12].

2) 보이스피싱의 년도별 증감에 대한 분석

보이스피싱에 대한 년도별 발생상황을 분석해 보면, 2006년에 처음으로 발행한 보이스피싱은 2007년 3,981건에서 2008년8,454건으로 급등세를 보이다가, 2009년 6,720건, 2010년 5,455건으로 전반적인 감소세를 보이고 있는 바, 이는 경찰의 강력한 단속활동과 2009년 5월부터 시행된 국제전화 식별번호 표시 및 국제전화 안내문자 서비스시행, ATM기 이체한도 축소 및 지급정지시행, 공익광고 등 각종 홍보활동 등의 종합대책으로 감소세를 보였다. 또한 2009년 7월경 중국내부에서 활동 중이던 대만계 보이스피싱 콜센터 조직의 검거로 활동이 위축된 것으로 분석된다.

그 이후 보이스피싱 발생건수가 2011년 8,244건으로 급등하였다가, 2012년 5,709건, 2013년 4,765건으로 감소세를 보이고 있는 바, 이는 보이스피싱범죄조직이 카드론 및 피싱사이트와 같은 신종 수법으로 변신함과 아울러, 국제전화 발신번호를 변작하여 국내전화번호로 변경하여 발신함으로써 이에 속은 피해가 급등한 것으로 추정할 수 있으나, 상시단속의 강화 및 10분 지연인출제도의 시행 및 홍보강화 등으로 감소세를 보이고 있는 것으로 분석된다.

그러나 보이스피싱은 2014년 7,635건, 2015년 7,239건으로 증가추세를 보이고 있는 바, 이는 범죄수법이 지속적으로 진화하여 증가세를 보여주고 있는 것으로 추정되고 있다[13].

Ⅲ. 경찰의 보이스피싱에 대한 대응방안

우리나라 경찰에서 추진하고 있는 보이스피싱에 대한 대응방안을 살펴보면, 첫째 우리경찰은 2015년부터 보이스피싱의 척결을 위해 본청에 전화금융사기 T/F를 설치 및 각 지방청에 전담수사체계를 구축하여 연중 · 상시 단속을 실시하고 있다. 특히 각 지방청의 지능범죄수사대를 설치하여 광역 수사체계를 구축하고, 경찰수사역량을 총동원하여 강력단속을 시실하고 있다고 한다. 그리고 중국, 태국, 베트남 등 외국 경찰과의 공조 수사를 통해 사사권역을 확대시키고 있음을 알 수 있다.

둘째, 경찰은 과학기술정보통신부, 금융위원회, 금융감독원 등 관계기관과의 협력을 강화하여 보이스피싱 피해예방을 위한 각종 금융 · 통신제도를 개선하고 있다. 2005년 1월에는 전자금융거래법 개정을 통하여 통장양도자(이른바 차명을 이용한 대포통장 양도행위)의 처벌을 강화하고, 과거 지연인출제도의 지연시간을 '300만원 이상 이체시 10분 경과'에서 '100만원 이상 이체시 30분 경과'로 골든타임을 확보하였다. 이러한 금융제도의 혁신을 통해 2015년에 총 8,668건의 정지요청 건이 있었다.

셋째, 발신번호를 변작한 경우 전화번호 발신의 차단조치 및 국외 발신표시조치, 그리고 변작된 전화번호 발신회선에 대하여 전기통신역무제공을 중지하는 조치를 하였다. 이에 따라 해외 콜센터에서 해외에서 국내 피해자에게 전화를 할 경우 '국제전화'임을 알리는 문자를 화면에 표시토록 하였다.

넷째로는 보이스피싱에 대한 대국민 홍보를 단발성이 아닌 수요자대상 종합적 홍보방안을 마련하여 체계적으로 실시하였다. 이에 따라 보이스피싱의 취약계층인 노인, 여성, 청년, 학교, 종교, 금융기관 등 수요자별, 단계별로 세분화한 특성에 따라 신문, TV, 라디오, 인터넷 등을 통하여 홍보를 강화하였다[14].

Ⅳ. 경찰의 대응방안에 대한 개선점 제안

위와 같은 경찰의 보이스피싱 근절을 위한 대응방안에 대하여 개건할 점에 대한 제안을 살펴보자면 아래와 같다.

첫째, 경찰이 현재 시행하고 있는 각 지방청에 지능범죄수사대를 두고 이에 기반한 광역수사체계를 구축하여 보이스피싱의 근절을 위한 대대적인 단속은 바람직한 것으로 보여지고 있으나, 이보다 더욱 세밀하게 일선 경찰서까지 포함한 유기적인 수사망 구축이 필요할 것으로 사료된다. 일선 경찰서에도 전담반을 두어 경찰청과 유기적으로 효율적인 수사활동이 필요할 것으로 보여 진다. 이웃 일본의 경우도 우리나라처럼 연금, 의료비 등을 환급시켜주겠다고 피해자를 속여 보이스피싱범죄를 저지르는 경우가 해마다 급증하고 있다. 이에 대한 근절책으로 매달 연금지급 시기에 ATM 기기 주변에 경찰인력을 집중배치하여 보이스피싱 피해 예방을 실시하고 있다[15]. 이러한 일본의 사례를 검토하여 우리나라도 정복을 착용한 경찰관이 수시로 ATM 기기 주변지역의 순찰을 강화하여야 할 필요성이 있다할 것이며, 이는 지방청과 일선 경찰의 유기적인 수사협력을 바탕으로 보이스피싱범죄가 우려되고 있다는 정황이 포착되면 협조수사를 통하여 범죄가 발생할 만한 ATM 기기 주변의 순찰을 강화할 필요성이 있다할 것이다.

둘째, 경찰은 과학기술정보통신부, 금융위원회 등 유관기관

과의 유대강화를 통해 보이스피싱의 근절을 위해 협력을 강화하고 있으나, 이는 사건 발생에 따라 일시적인 협력을 통해 이루어지고 있을 뿐이다. 미국의 경우 인터넷을 이용한 사이버 위협으로부터 국가적 차원에서 모든 국제금융사기에 대처하기 위해 국토안보부(Department of Homeland Security) 가 창설되었다. 미국은 9.11테러 사태 이후, 국 · 내외의 모든 테러공격을 예방하고 국민을 보호하기 위해 2003년에 국가적 차원에서 사이버보안 정책과 계획을 개발·조정하는 중앙기관을 창설하였다. 이는 미국의 22개 연방기관이 참여하는 거대한 규모의 재난대비 총괄기관으로서 그 산하에 정보분석단(ASIA)과 기반시설보호단(ASIP)을 두었다. 이 기관들이 미국의 사이버 및 물리적 임프라에 대한 위협평가 업무를 수행한다. 이는 연방경찰 및 각각의 기관에서 독자적으로 수행하여 왔던 대국민 사이버관련 위협 대응업무가 모두 위 국토안보부로 이관되어 일관적이고 통합적인 기관을 통하여 일사불란하게 효율적으로 업무진행이 되고 있다[16]. 우리나라도 이제는 과학기술정보통신부, 경찰청, 금융위원회 등 각 부처에 분산되어 있는 인터넷 및 정보통신 관련 국가적 위협에 대하여 일원화된 조직을 두어 보다 능동적으로 대처를 해야 할 것으로 사료된다. 이러한 점에 비추어 국민 · 기관 · 국가를 위협하는 모든 사이버범죄(인터넷 및 정보통신에서 발생할 수 있는 범죄의 모든 분야를 포함한 개념)에 능동적이며 일률적으로 대처할 수 있는 국가기관의 신설이 절실히 요청된다 할 것이다.

셋째로 경찰은 현재, 보이스피싱의 해외 콜센터에서 피해자에게 국제전화를 하는 경우 피해예방을 위하여 국제전화임을 표시하는 정책을 시행하고 있다고 하지만, 인터넷 전화의 경우에는 국내전화번호로 변작하여 발신하고 있는 바, 이에 대한 적극적인 대책이 추가적으로 필요하리라 사료된다. 이는 주관부서인 과학기술정보통신부에서의 기술적인 지원을 통하여 경찰청과 유기적인 업무협업을 통하여 해결할 수 있으리라 기대된다.

넷째로 보이스피싱범죄와 관련한 대국민 홍보에 있어서 현재도 다양한 매체와 다양한 방법을 총동원하여 시행하고 있다. 다양한 홍보방법에도 불구하고 보이스피싱에 노출되기 쉬운 서민층, 노인층, 농어촌 주민 등 포이스피싱범죄 취약계층에 대한 홍보의 질과 방법에 대하여 재고할 필요가 있다할 것이다. 위와 같은 범죄 취약계층에게 다양한 매체 중에서 신문, 라디오, 인터넷, SNS 및 홈페이지 등을 통한 홍보라든지, 전국마트, 야구장, 인기개그맨 등과 접촉할 수 있는 기회가 극히 드문 점을 감안 한다면, 피해자측면에서의 눈높이에 맞춘 효과적인 홍보활동이 필요한 바, 같은 TV홍보라 할지라도 대만의 경우처럼 정규 뉴스시간대 및 인기 드라마의 방영시간인 골든타임에 맞춘 홍보 등 맞춤 홍보를 통한 적극적인 홍보가 필요하리라 사료된다[17]. 또한 우리나라의 6세 이상 국민들 중 82% 이상이 보유하고 있는 스마트폰을 이용한 휴대폰 재난문자방송을 통한 보이스피싱 안내문자 발송홍보도 유용한 수단이라 사료되며, 범죄취약계층을 대상으로 한 현수막홍보 및 반상회, 노인정에 직접 방문하여 지속적인 홍보가 필요하리라 사료된다.

마지막으로 사후적 조치이기는 하지만, 피해자보호 차원에서 지급 정지된 대포통장계좌에서 피해자의 계좌로 신속하고 간소화된 방법을 통하여 환수조치가 이루어져야 할 것이므로 이를 위한 전담센터가 필요하리라 사료된다. 아울러 가해자들에 대한 강력한 형벌의 처단도 필요하겠지만, 현재 우리나라에서도 시행되고 있는 징벌적 손해배상제도와 유사한 징벌적 배상제도를 도입하는 것이 필요하리라 사료된다. 즉, 우리나라에서 몇 년 전부터 시행하고 있는 하도급거래공정화에관한법률 및 신용정보의이용및보호에관한법률, 정보통신망이용촉진및정보보호에관한법률 등에서 징벌적 손해배상제도를 도입하여 시행하고 있는 바[18], 보이스피싱과 같은 사이버금융사기범에게도 위와 같은 징벌적 손해배상제도와 유사한 징벌적 배상제도를 도입하여 가해자들에게 경각심을 고취하는 것이 필요하리라 사료된다. 위와 같은 제도를 도입한다면, 보이스피싱 범죄자들에게 범죄행위를 자제하게 하는 일반적 범죄예방효과가를 뿐만 아니라, 보이스피싱 피해를 미연에 방지할 수 있는 소기의 성과를 올릴 수 있을 것이다.

Ⅴ. 결 론

보이스피싱범죄는 2003년경 대만에서 시작되어 중국, 일본 등에서 자행되어 오다가, 2006년 우리나라에 상륙한지 10여년이 흘렀다. 경찰청 공식자료에 의하면 현재까지 약 60,000여건에 이르는 보이스피싱이 발생하고 있는 바, 몇 년을 주기로 증감을 반복하면서 국민들의 현금을 편취하는 신종사기 범죄로 자리잡고 있다. 보이스피싱이란 위에서 살펴 본 바와 같이 무작위 피해자 혹은 불법으로 정보를 취득하여 언어진 신상자료를 통한 특정한 피해자에게 전화 등을 통하여 현금인출기로 가도록 유도 한 후, 범인들의 계좌로 금전을 이체 받아 편취하는 수법의 신종 금융사기 범죄라고 할 수 있다. 이에 필자는 본 논문을 통하여 우리나라의 보이스피싱에 대한 발생실태를 분석한 후 경찰의 대응방안을 검토하였고, 나타난 문제점에 대한 개선점에 대하여 제안하여 보았다.

보이스피싱에 대한 발생실태를 살펴보면, 2006년 최초 발생이래, 2015년까지 경찰청에서 집계한 10년 동안의 발생건수는 총 59,690건 피해액의 규모는 약 6,800억 원에 이르고 있다. 보이스피싱의 피해사례는 세 가지 형태로 첫째 보안보호설정 등을 빙자한 계좌이체형태, 둘째 사기 또는 협박을 통한 직접 송금유도 또는 강요형태, 셋째 피해자가 직접 현금을 인출하게 한 뒤 사기 또는 절도를 통한 형태 등이다. 이에 대한 분석은 국제화되고 각자의 역할 수행이 수반된 조직적인 범죄라는 점, 초기에는 불특정 피해자에게 금융피해를 입혔으며, 그 후 정보수집방법이 발전하여 특정한 피해자를 대상으로 편취하고 있는 점, 보이스피싱의 발생이 경찰의 단속노력의 결과에 따라 몇 년을 주기로 증감을 반복하고 있으나 끊임없이 지속적으로 발전, 변화하고 있는 점 등으로 분석되어졌다.

그리고 현재까지의 경찰에서 시행하여 왔던 대응방안을 검토하였고, 그에 따른 개선점에 대하여 제시하여 보았다. 개선점으로는 첫째, 효율적인 수사를 위하여 일선경찰서와 광역수사체계와의 유기적인 협력이 필요하며, ATM기기 주변에 정복경찰관의 순찰활동의 강화의 필요성을 제시하였고, 둘째 경찰청, 과학기술정보통신부, 금융위원회 등의 기관은 대국민, 기관 및 국가에 대한 인터넷 및 정보통신관련 범죄에 대처하기 위한 단일화된 국가기관을 신설하여 종합적으로 대처할 것을 제시하였고, 셋째 국제전화의 전화번호 변작의 문제는 어느 정도 성과를 보이고 있지만, 인터넷을 통한 해외발신번호 변작행위에 대하여 관련기관에서 철저히 근절시켜야 할 것이며, 넷째 홍보방법에 있어서 TV의 정규뉴스 및 황금시간 대에 홍보에 집중할 것과, 보이스피싱에 대하여 휴대전화를 통한 긴급문자 발송 및 범죄취약 계층에 대한 선별적인 홍보를 제안하였고, 마지막으로 피해회복을 위한 전담센터의 설치 및 현재 우리나라도 도입하여 시행하고 있는 징벌적 손해배상제도와 유사한 징벌적 배상제도를 도입하면 어느 정도 범죄예방의 효과를 거둘 수 있을 것으로 사료되어 제안하는 바이다.

이상 살펴본 보이스피싱범죄는 지속적이고도, 교묘한 방법으로 변신을 거듭하여 향후에도 그 범죄가 근절되지 않을 수 있다고 판단된다. 이제는 정부 당국과 국민 모두가 각별한 관심을 가지고 지속적인 대응자세를 갖는 것이 필요하다. 향후 많은 연구가 이루어져 보이스피싱이 근절되었으면 하는 바람으로 이 글을 마친다.

참고문헌

[1] K. H. Park, “Crime Prevention by Using CPTED and Improvement”, Journal of Digital Contents Society, Vol. 18, No. 4, p. 734, 2017.

[2] Korea National Police Agency, Korea National Police Agency 2016 White Paper: Seoul, Korea, p. 151, 2017.

[3] Korea National Police Agency, Korea National Police Agency 2016 White Paper: Seoul, Korea, pp. 151-152, 2017.

[4] H. J. Lee, “A Study on Voice Phishing Victims and Countermeasures of the Police” Korean Journal of Victimology, Vol 17, No. 2, p. 219, 2009.

[5] Korea National Police Agency, Korea National Police Agency 2016 White Paper: Seoul, Korea, pp. 152-153, 2017.

[6] S. R. Kim, “Zur Strafbarkeit von Phishing”, IT & Law Research, p. 1, 2010.

[7] J. H. Choi, P. J. Lim, “A Study on Plausible Measures to Prevent the Phone Financial Fraud(aka Voice Phishing) Committed through the Virtual Private Network”, The Journal of Korean Police Studies, Vol 8, No. 2, p. 187, 2009.

[8] Korea National Police Agency, Korea National Police Agency 2016 White Paper: Seoul, Korea, p. 153, 2017.

[9] H. D. Cho, “Voice Pishing Occurrence and Counterplan”, The Journal of Korean Contents Association, Vol. 12, No. 7, p. 180, 2012.

[10] H. J. Lee, “A Study on Voice Phishing Victims and Countermeasures of the Police” Korean Journal of Victimology, Vol 17, No. 2, pp. 222-223, 2009.

[11] Korea National Police Agency, Korea National Police Agency 2016 White Paper: Seoul, Korea, p. 153, 2017.

[12] H. J. Lee, “A Study on Voice Phishing Victims and Countermeasures of the Police” Korean Journal of Victimology, Vol 17, No. 2, pp. 223-225, 2009.

[13] Korea National Police Agency, Korea National Police Agency 2015 White Paper: Seoul, Korea, pp. 145-146, 2016.

[14] Korea National Police Agency, Korea National Police Agency 2016 White Paper: Seoul, Korea, pp. 154-155, 2017.

[15] Y. S. Chang, “ A Study on the Cyber Crimes – Focused on the Internet Frauds from the Perspective of the Criminal Law – M. A. Yonsei University, Seoul. p. 109, 2009.

[16] Y. S. Chang, “ A Study on the Cyber Crimes – Focused on the Internet Frauds from the Perspective of the Criminal Law – M. A. Yonsei University, Seoul. pp. 106 - 107, 2009.

[17] H. J. Lee, “A Study on Voice Phishing Victims and Countermeasures of the Police” Korean Journal of Victimology, Vol 17, No. 2, p. 239, 2009.

[18] W. Choung, “A Study on the Current Issues and Countermeasures of Cybercrime” Hongik Law Review. Vol. 17, No. 3, pp. 21-22, 2016.

김덕용(Duck-Yong Kim)

1987년 : 청주대학교 법과대학 대학원 (법학석사)

1998년 : 청주대학교 법과대학 대학원 (법학박사- 형사법 전공)

1994년～2000: 청주대학교, 국립교통대학교, 주성대학 외래교수

2000년～현재: 충북보건과학대학교 경찰행정학과 교수

※관심분야 : 형사법, 의료형법