사이버공격의 국가 경제적 손실분석 - 보이스 피싱을 중심으로

신진*

Analysis on National Economic Loss of Cyber Attack: Voice Phishing Case

Jin Shin*

이 논문은 2012년도 단국대학교 대학연구비를 지원받았음

요 약

보이스 피싱은 해독능력이 약한 노인과 약자를 대상으로 사회공학적인 방법을 이용하여 경제적 피해를 유발시킨다. 최근 인접국과 연계조직에 의한 보이스 피싱이 많은 국민에게 경제적 손실과 정신적 파탄을 야기하였고 대한민국 전체로 보더라도 보이스 피싱으로 인한 국가경제손실 및 정신적 피해는 매우 크다. 최근 정부와 관련기관들이 보이스 피싱을 막기위한 보안시스템과 금융보안장치를 강화하고 있으나 보안효과가 얼마나 큰가는 검증하기 쉽지 않다. 본 논문에서는 보이스 피싱으로 인한 대한민국의 경제적손실과 보안장치강화에 따른 보안효과의 경제성에 관하여 살펴본다. 우리나라의 보이스 피싱 피해의 직접 피해액은 1,100억 원으로 나타나고 있으며 철저한 보안에 따는 잠재적인 경제적 효과는 연간 3,500억 원 규모에 이른다고 볼 수 있다.

ABSTRACT

Voice phishing against the old or weak persons have used the methods which are social engineering in the object and financial structure and function. Until recently Voice phishing from Chaina caused economic devastation and the economic loss by phishing grows with the South Koreans in the whole. Korean government and public organizations involved have been strengthening protection system and a financial security devices. But it is not easy to verify how much effects of security measures are. In this paper I will study the economic loss caused by voice phishing and potential economic effects of security measures and security device reinforcements of the Republic of Korea. Direct costs are reported about 100 million dollars and potential economic effects of voice phinshing secure measures may be around 320 million dollars.

키워드

보이스 피싱, 경제적 손실, 보안효과, 경제적 효과

Key word

voice phishing, economic loss, security effect, economic effect

* 종신회원 : 단국대학교 교양기초교육원(korjin@empas.com)

접수일자 : 2012. 10. 05
심사완료일자 : 2012. 10. 25

Open Access http://dx.doi.org/10.6109/jkiice.2012.16.11.2341

Ⅰ. 서 론

개인정보(private data)와 낚시(fishing)를 합성한 신조어인 피싱(phishing)은 금융기관 등의 웹사이트나 거기서 보내온 메일로 위장하여 개인의 인증번호나 신용카드번호, 계좌정보 등을 빼내 이를 불법적으로 이용하는 사기수법이다. 피싱 공격자는 그림 1처럼 보안이 취약한 홈페이지에 대한 관리자 권한 등을 해킹한 후, 가짜 홈페이지를 만든다. 다음으로 은행이나 쇼핑몰, 온라인게임 등 유명 기관을 사칭해 가짜 홈페이지 주소가 들어있는 e-mail을 보내고 가짜 홈페이지에 개인정보를 입력하도록 유도한 뒤 수집한 정보를 악용하는 신종 금융사기 수법이다. 피싱의 경우에는 주로 e-mail 등의 사회공학적 방법을 이용해 부주의한 사용자를 비정상적인 방법으로 위장된 피싱 사이트로 연결시켜 사용자의 정보를 빼내는 방법이 사용되고 있다.

그림 1. 피싱 사고 발생도
Fig. 1 Phishing Attack Flows

보이스 피싱(voice phishing)은 '(전화)음성을 통해 개인정보를 낚아 올린다'는 뜻이다. 이는 전기전자통신수단을 이용한 비대면 접촉을 통하여 남을 속여 금전을 편취하는 방법으로 특히 금융 분야에서 발생하는 사기 범죄이다.

보이스 피싱은 2000년대 초반 대만에서 시작되어 중국, 일본, 한국, 싱가포르 등 주로 아시아 지역으로 확산되었다. 한국에는 2006년 중반에 보고된 후 피해자가 기하급수적으로 늘어났다. 지난 7월 말까지 6년 동안 약 4만여 명이 피해를 입었는데, 보고된 피해 금액만 약 4천억 원에 달한다.

보이스 피싱은 피해자에게 경제적 손실을 가져올 뿐 아니라 사회적 불신을 조장하고 사람들을 공연히 불안하게 만들어 직접적으로 피해를 당하지 않은 일반국민들이 겪는 정신적인 피해 또한 막대하다. 본 논문에서는 보이스 피싱이 경제에 미치는 손실에 대한 연구 자료를 토대로 분석하여, 국가 보안효과의 경제적 효과를 연구하고자 한다.

Ⅱ. 보이스 피싱 공격과 사이버 보안의 경제적 효과

2.1. 보이스 피싱 확산의 배경

보이스 피싱은 2000년대 중반부터 전자금융활용이 급속하게 확산되면서 기승을 부리기 시작하였다. 현재는 일부 노년층을 제외한 우리나라 국민의 대다수가 금융기관의 창구를 통한 거래보다는 편의성이 높은 인터넷뱅킹을 선호하며 나아가 모바일 거래가 급격하게 증가하고 있다. 보이스 피싱 공격자들은 공격대상들이 상황을 냉정하게 판단하고 확인하는 시간을 배제하기 위하여 다양한 전략을 구사하며 전자금융이 그 환경을 제공하고 있다. 2011년도의 전자금융이용금액은 1경 7,043조 원에 달하며 이 중 인터넷뱅킹이 1경 5,544조 원에 달한다.

표 1. 전자금융 취급실적(자료: 금융감독원)
Table. 1 Electronic financial transactions(data: Financial Supervisory Service)

	2010 (조 원)	2011 (조 원)	증감률 (%)
인터넷뱅킹 (모바일)	14,358 (134)	15,544 (225)	8.3 (68.6)
CD/ATM	715	798	11.7
폰뱅킹	693	701	1.3
전자금융합계	15,765	17,043	8.1

전자금융거래는 거래의 편의성, 신속성, 낮은 수수료 등의 장점이 있는 반면 정보유출, 불법거래, 위변조

에 의한 사고가 발생될 수 있다. 따라서 전자금융거래 보호장치와 개인적인 대처방법 숙지가 필요하다. 보이스 피싱의 경우에는 일반적인 전자금융의 보호조치와 더불어 공격상황에 따른 침착하고 냉정한 대응이 요구된다[1].

2.2. 보이스 피싱 범죄조직시스템

보이스 피싱 조직은 대개 콜센터와 국내현지조직으로 나누어 볼 수 있다. 콜센터는 중국의 동북3성 등 인접국에 전산팀, 시나리오팀, 텔레마케팅팀의 3팀 체제로 운영된다. 전산팀은 자동 통화 프로그램을 개발하거나 운용한다. 전산팀은 해킹 등을 통해 '개인정보'를 수집하기도 한다. 시나리오팀은 한국의 상황과 금융 시스템의 구조 등을 분석하여 어떤 내용으로 전화를 걸 것인지 여러 상황을 설정하고 고도의 심리 테크닉도 개발한다. 국내 사정에 밝은 한국인이나 조선족이 담당하고 있다. 중국 공안은 최근 랴오닝 성 등 5개 성에서 대규모 보이스 피싱 조직을 적발했는데, 조직원 2백 35명 중 한국인 51명이 포함되어 있었다고 한다. 이들은 대부분 시나리오팀 조직원들이다. 상황 설정이 완료되면 시나리오를 만들어서 '텔레마케팅팀'으로 넘긴다. 이들은 우리말을 유창하게 구사하며 고도의 심리전을 펼친다. 조직원들은 근무시간이 보통의 회사와 유사하며 월급 형태로 급여를 받고 일의 성과에 따라 추가 성과급이 지급된다.

보이스 피싱 조직은 한국에 지부 성격의 조직을 구축한다. 국내 조직은 통장 모집팀 등 4팀으로 구성되는데 각 팀에는 팀장급의 관리자를 임명해 하부 조직원들을 피라미드식으로 관리한다. 한국 조직은 통장 모집팀, 배달팀, 현금 인출팀, 송금팀 등 4개팀으로 점조직으로 운영된다. 별도의 사무실을 두지 않고, 통칭 선불폰이나 대포폰 등을 이용해 연락을 주고받는다. '통장 모집팀'은 범죄 자금을 송금받을 통칭 대포통장을 모집한다. '배달팀'은 통장 모집팀이 대포통장을 모집하면 현금 인출팀에게 전달하는 역할을 한다. '현금 인출팀'은 피해자가 대포통장에 입금한 자금을 찾는다. '송금팀'은 인출한 현금을 통칭 환치기를 통해 세탁한 후 본부로 보낸다[2].

2.3. 보이스 피싱 피해와 경제적 효과

'노턴 사이버 범죄 보고서 2011'을 요약한 표 2에 의하면 세계적으로 빈발하고 있는 사이버범죄의 비중을 살펴보면 컴퓨터바이러스/악성프로그램, 온라인 사기, 피싱순으로 나타나고 있다[1]. 또한 24개국의 사이버범죄의 희생자수는 총 4억 3천 백만명으로 나타났는데 이는 조사대상 24개국의 성인 중 69%가 지금까지 가상범죄에 노출되었으며 이중 65%가 지난 12개월간 가상범죄의 희생양이 되었다는 것을 말한다[3].

표 2. 세계의 주요 사이버 범죄 비중(%)
Table. 2 Global Major Cyber Crime(%)

	24개국	미국	일본
컴퓨터바이러스/악성프로그램	54 (58)	56 (61)	23 (41)
온라인사기	11 (52)	18 (45)	
피싱	10 (53)	14 (60)	5 (44)
기타			12 (88)

( )내의 수치는 사이버 범죄 피해자 중 조사기간인 2011년 2~3월 기준으로 최근 12개월간 해당 범죄를 경험한 비율이다.

국민권익위원회가 운영하는 110 정부 민원 안내콜센터는 2012년 1월~8월에 접수된 보이스 피싱 관련 상담내용을 분석해 발표했다. 분석결과를 살펴보면 보이스 피싱을 통해 사칭하는 기관은 「검찰과 경찰 등 수사기관」이 25.5%로 가장 큰 비중을 차지했으며 「공공기관」도 6.7%로 지난해 1.7%에 비해 큰 폭으로 증가했다.

이와 같이 「수사기관·공공기관 사칭」은 전체 보이스 피싱의 32.2%를 차지해 전년도에 비해 50.5% 증가한 것으로 나타났고, 이에 반해 전년도 까지 16.1%로 가장 큰 비중을 차지했던 「은행사칭」은 9.2%로, 지난 3년간 꾸준히 증가했던 「자녀납치 사칭」은 전년도 9.9%에서 5%

1) 노턴사이버 범죄보고서(2011)은 2011년 2월 6일부터 3월 14일까지 24개국의 성인 12,704명을 포함한 19,636명을 대상으로 인터뷰를 수행한 결과를 바탕으로 작성되었다. 조사대상 24개국은 호주, 브라질, 캐나다, 중국, 프랑스, 독일, 인도, 이탈리아, 일본, 뉴질랜드, 스페인, 스웨덴, 영국, 미국, 벨기에, 덴마크, 네덜란드, 홍콩, 멕시코, 남아공, 싱가포르, 폴란드, 스위스, 아랍에미레이트연방이다.

로 감소했다. 2008년 전체의 44%를 차지할 정도로 주요 사칭유형인 「우체국과 택배사칭」은 전년도 8.8%에 이어 올해 5.2%로 계속 감소하고 있다.

이와 같이 과거에는 특정 유형이 주를 이뤘으나 최근에는 다양한 유형들이 고른 비중을 차지하고 있다.

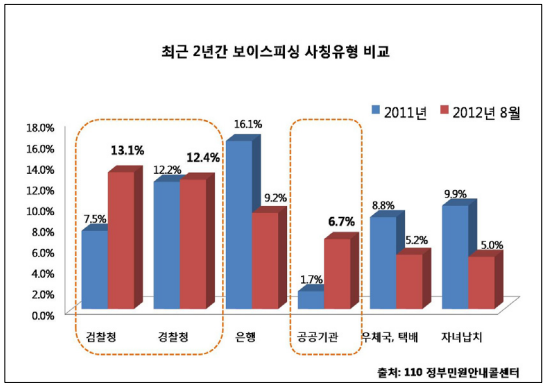

그림 2. 보이스 피싱 사칭유형
Fig. 2 Voice Phishing Types Ratios

그림 2처럼 최근 3개월('12.6~8)간 보이스 피싱에 가장 빈번히 사용된 발신번호는 서울지방검찰청 (02-6953-6844)과 경찰청 금융 범죄과 (050-7788-5003), 대검찰청 (02-3484-9688), 법무부(02-6304-0058) 등 수사 관련 기관으로 나타났다. 상담 사례를 살펴보면, 최근 급증하고 있는 검찰·경찰 등 수사기관을 사칭한 보이스 피싱은 주민등록번호와 연락처 등 개인정보를 파악하고 전화를 걸어오는 경우가 많고 단순한 기관 사칭이 아닌, 실제 은행 인터넷 사이트와 흡사한 가짜 피싱 사이트를 제작하고 접속을 유도해 개인정보등도 빼내는 사례와 연금·보험 관련 기관인 국민연금공단, 국민건강보험공단 등을 사칭해 환급금을 돌려준다고 현혹해 개인정보를 빼내 또 다른 범죄에 활용하는 경우도 있어, 보이스 피싱 수법은 나날이 더 다양해지고 정교해지고 있다는 것을 알 수 있다[4].

우리나라의 경우 사이버범죄유형별 발생빈도를 보면 표 3처럼 해킹사고는 2009년까지 증가하다가 주춤하고 있으나 악성코드 피해와 피싱 피해 규모는 증가하고 있다.

표 3. 해킹사고 및 악성코드피해 신고 건수
(자료: 한국인터넷진흥원)
Table. 3 Hacking and Malware Damage Report
(data: KISA)

구분(년)	2008	2009	2010	2011
해킹사고	15,940	21,230	16,295	11,690
악성코드 피해	8,469	10,935	17,930	21,751

글로벌 정보통신기업 EMC의 'RSA 온라인사기보고서(Online Fraud Report)'에서 요약한 그림 2에 따르면 그들이 세계적으로 파악한 2011년의 피싱 공격 건수는 27만 9,580건으로 2010년에 비하여 37% 증가하였다. 월별 공격건수를 나타내는 그림 1에서 보면 2009년 9~12월 매월 1만 7,000건에 미치지 않던 것이 2012년 5월 이후 급격히 증가하여 2012년 7월 5만 9,406건으로 늘어나는 등 최근 들어 급격하게 증가하고 있는 것을 알 수 있다[5].

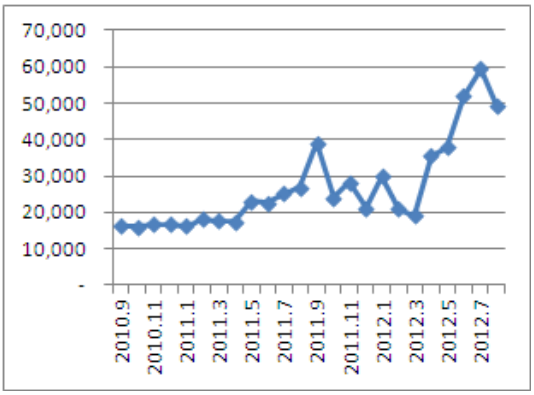

그림 3. 최근 3년 피싱 공격 건수(세계)
Fig. 3 World Phishing Attacks in Recent 3 Years

표 5처럼 우리나라의 2011년 보이스 피싱 신고건수는 8,244건으로 단순히 비교한다면 세계의 2.9%에 해당하는데 2011년에는 전년도에 비하여 51% 증가한 것으로 나타나 다른 나라들보다 가파르게 늘어나고 있음을 알 수 있다. 금액으로 보면 2011년 피해액이 1,019억 원으로 동기간 84%나 증가하였다. 건당 피해금액은 피해가 발생하기 시작한 2006년에는 약 700만 원에서 2011년에는 1,200만 원으로 증가하였다.

표 4. 우리나라 보이스 피싱 피해
(자료 : 방송통신위원회 국정감사 자료(2012))
Table. 4 Voice Phishing Damages
(data: KCC)

구분 (년)	2006	2007	2008	2009	2010	2011	2012 7월	합계
신고 건수	1,488	3,981	8,454	6,720	5,455	8,244	4,207	38,549
피해 금액 (억원)	106	434	877	621	554	1,019	460	4,071
건당 피해액 (만원)	712	1,090	1,037	924	1,016	1,236	1,093	1,056

표 5에 나타나듯이 우리나라에서 발생하고 있는 보이스 피싱 유형은 계좌안전조치빙자, 등록금빙자, 가족납치빙자, 메신저 피싱 등이 주종을 이루다가 최근에는 ARS를 통한 카드론 편취, 인터넷뱅킹을 연계한 예금 등의 편취, 상황극 연출 및 수사빙자 등이 갑자기 늘어나고 있다.

표 5. 보이스 피싱 유형과 피해규모(2011)
(자료: 경찰청, 금융감독원)
Table. 5 Types of Voice Phishing and Damage Scales (data: NPA, KCC)

유형		건수	금액 (억원)	비고
기존 유형	계좌안전 조치빙자	3,784	396	
	특이형태 사기	81	3	등록금 빙자등
	가족납치 빙자	1,536	144	
	메신저 피싱	(1,024)	(31)	
최근 유형	카드론편취(ARS)	826	154	
	카드론/예금등 편취(인터넷뱅킹)	1,005	240	피싱사이트 활용
	상황극연출	582	65	
	기타	430	27	수사빙자 등
합계 (메신저피싱)		8,244 (1,024)	1,019 (31)	

2011년 우리나라의 유형별 피해규모를 보면 금융계좌안전조치빙자가 3,800여건, 약 400억원으로 건수나 금액면에서 가장 많은 것으로 나타나고 있으며, 인터넷뱅킹관련 사기, 가족납치빙자가 다음을 잇고 있다. 2008년의 경찰청 자료에 의하면 피해금액 상위 20건중에 신용카드사 사칭과 관련된 건이 12건으로 건당 피해액이 최고 2억 천만원에서 6천백만원에 이른다[6].

이를 분석해 보면 보이스 피싱이 인접국가에 근거를 두고 대규모로 기업화할 뿐만 아니라 우리나라에 사정을 반영한 보이스 피싱 기법이 빠른 속도로 개발되고 있음을 알 수 있다. 최근 해외에서 공공기관을 사칭하거나 인터넷전화를 이용하여 해외에서 전화를 한다든지 발신번호를 변경하여 수사기관을 추적을 따돌리는 방법을 통해 더욱 교묘하게 보이스 피싱을 하고 있어 우리 국민들의 피해는 확대되고 있다.

보이스 피싱 유형과 사칭유형을 종합해 보면 검찰청, 경찰청등 수사기관과 금융기관, 공공기관을 사칭하여 전화하고 계좌안전조치, 가족납치 등을 빙자한 경우와 카드론 편취가 많다는 것을 알 수 있다.

'노턴 사이버 범죄 보고서 2011'에 의하면 사이버범죄의 시간손실비용은 경제적 비용의 2.4배에 이른다고 분석하고 있다. 이를 준용한다면 우리나라의 보이스 피싱 피해의 직간접비용은 연간 3,500억 원 규모에 이른다고 볼 수 있다. 이는 보이스 피싱 보안의 잠재적인 경제효과가 그 이상이 될 것이라는 것을 말해준다. 이에 더하여 직접적인 금전피해를 당하지 않았으나 사이버 피싱 공격에 노출당한 이들의 불안감과 일반국민들의 불안감은 그에 못지않다고 할 것이다. 간접피해의 경제적 효과도 향후 패널구성을 통한 설문조사나 간접 추정방식을 통하여 정밀하게 분석할 필요가 있다.

Ⅲ. 결 론

보이스 피싱은 암세포가 퍼져나가듯이 확산되고 국민들에게 고통이 되고 있다. 보이스 피싱 공격은 이에 노출된 국민 개개인에게 경제적 피해를 입히고 불안감과 상실감을 유발할 뿐 아니라 사회 불신을 조장함으로써 국민적 결속력과 사회적 유대감을 저해하는 커다란 해독이 된다. 우리나라의 보이스 피싱 피해의 직접 피해액은 1,100억 원으로 나타나고 있는데 철저한 보안에 따른

잠재적인 경제적 효과는 연간 3,500억 원 규모에 이른다고 볼 수 있다.

지금까지는 주로 보이스 피싱은 인접국에 근거를 둔 국제조직에 의하여 자행되고 있다. 이는 우리나라 당국만으로 해결이 어렵다는 말이다. 최근 국내자생의 피싱 조직도 등장할 것으로 우려되며 신종보이스 피싱 범죄 형태도 지속적으로 등장할 것으로 예견되고 있다. 따라서 국내적으로는 방송통신위원회와 법무부, 지식경제부, 인터넷진흥원, 금융감독원 등 관련기관들이 긴밀히 협력해 범정부차원의 대책을 마련하여야하고 나아가 중국, 대만등과의 공조협력체계의 구축이 절실하다.

향 후 국가 사이버안전을 위한 피싱 방어대책과 개선효과에 관한 정보의 수집체계를 수립하고 이를 바탕으로 보안의 경제적 효과에 대한 체계적인 연구가 필요하다.

감사의 글

이 논문은 2012년도 단국대학교 대학연구비를 지원받아 이루어진 것임

참고문헌

[1] 김인석, 전자금융과 정보보호에 관한 연구, 우정정보 66 pp. 39-58, 2006 가을

[2] 보이스 피싱 '악마의 목소리' 뒤에 누가 있나, 시사저널 1185호

[3] Norton Cybercrime Report 2011, http://www.symantec.com

[4] 110_보이스 피싱 상담현황분석, 국민권익위원회, 2012.9.17

[5] RSA Online Fraud Report, EMC, http://www.rsa.com

[6] 2008년 경찰청 국회제출자료

저자소개

신 진(Jin Shin)

1989년 Florida State University 대학원 경제학과 (경제학석사)

1991년 Florida State University 대학원 경제학과 (경제학박사)

2008년~2011년 호서대학교 벤처전문대학원 교수

2012년 단국대학교 교수, 한국산업기술평가관리원 이사

※관심분야 : 과학기술정책, 산업정책 등