피싱(Phishing)의 현황과 국내 대응방안 연구

박소영[a], 이병남[b], 박웅[c]

[a]한국전자통신연구원
305-350, 대전시 유성구 가정동 161번지
Tel: +82-42-860-3827, E-mail: bubble@etri.re.kr

[b]한국전자통신연구원
305-350, 대전시 유성구 가정동 161번지
Tel: +82-42-860-6636, E-mail: b.n.lee@etri.re.kr

[c]한국전자통신연구원
305-350, 대전시 유성구 가정동 161번지
Tel: +82-42-860-4941, E-mail: wungp@etri.re.kr

Abstract

피싱(Phishing)이란 '위장 홈페이지를 만들어 불특정 다수의 이메일 사용자에게 메일을 보내는 수법으로 수신자의 개인정보를 빼내 금융범죄에 악용하는 행위'를 말한다. 기존의 스팸메일 등과 달리 피싱은 이메일 사용자에게 금융, 신용 피해를 줄 수 있어 개인에게 미치는 피해가 심각한 경우가 발생할 수 있다. 이에 대응하여, 미국에서는 'SB California SB 1386' 등의 법안을 제정하고, 'Coalition on Online Identity Theft' 등의 조직을 결성하는 등 피싱으로 인한 피해 예방 및 대처를 위해 적극적으로 노력하고 있다. 국내에서도 금융기관과 기업에서의 주의 메일 발송, 홈페이지에의 피싱 주의 안내문 게시 등의 방법으로 대응하고 있으나, 피싱으로 인한 피해를 예방하기에는 미진한 것으로 여겨진다. 이에 본 고에서는 미국을 중심으로 한 피싱에 대한 피해•대응현황과 국내 대응방안에 대해 살펴본다.

1. 피싱의 등장

피싱(Phishing)이란 실제 금융기관이나 기업이 보낸 것처럼 보이도록 위장한 이메일을 통하여, 신용카드 번호 등의 개인 정보를 훔치는 행위를 말한다. 이 단어는 일반적으로 개인정보(private data)를 낚시(fishing)하듯 낚아챈다'는 뜻에서 유래되었다고 인식되고 있다. 피싱 메일은 '긴급보안통지', '메일의 요청을 무시할 경우 귀하의 계좌가 잠정적으로 정지될 수 있음', '업그레이드 된 인터넷뱅킹 기능 사용을 위해 링크된 홈페이지로 즉시 접속할 것', '경품 당첨, 계좌잔액증가, 거래내역 변경 등의 내용으로 홈페이지 접속을 요구' 등의 내용을 담은 이메일을 보내, 이메일 수신자가 개인 정보를 공개하도록 유도한다. 잘 알려진 기업의 웹사이트를 가장한 위조사이트로 링크를 하여 개인정보를 입력하도록 유도하는 경우도 많다.

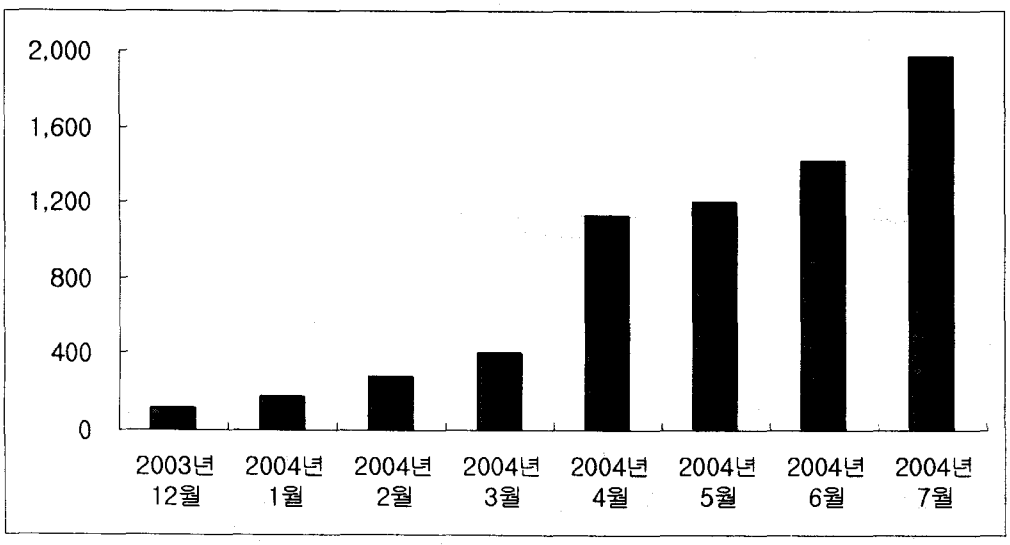
피싱을 시도하는 사람(피셔, Phisher)은 일반적으로 메일의 송신자 주소를 유명 기업의 이름

으로 변경하여 상대가 믿도록 유도한다. 다음으로, 정보 입력용의 웹사이트를 만들고 이를 기업의 웹사이트와 동일하게 보이도록 위장하며, 메일의 내용에 실제 기업을 가장한 위조 사이트로의 링크를 만들어 두고, 메일 수신자를 유인한다. 대부분의 경우, 피셔는 정보 입력용의 웹사이트를 실제 기업의 웹사이트와 구별하기 어렵도록 만든다. 또한, 실제 기업의 회사명과 위조 사이트의 URL이 무관하다는 것을 간파 당하지 않도록 하기 위해 URL까지 실제사이트와 같아 보이도록 조치를 취한다. 흔히 사용되는 수법으로, 허위 사이트에 접속할 때 웹 브라우저의 주소 막대를 표시하지 않도록 하는 방법과, 실제로 접속하고 있는 사이트의 URL과 다른 URL을 브라우저의 주소 막대에 표시하는 방법이 있다. 이 외에도 피싱의 수법에는 여러 가지가 있으며, 인간 심리를 이용한 교묘한 수법들이 새롭게 생길 가능성이 높다.

2. 피싱에 의한 피해 현황

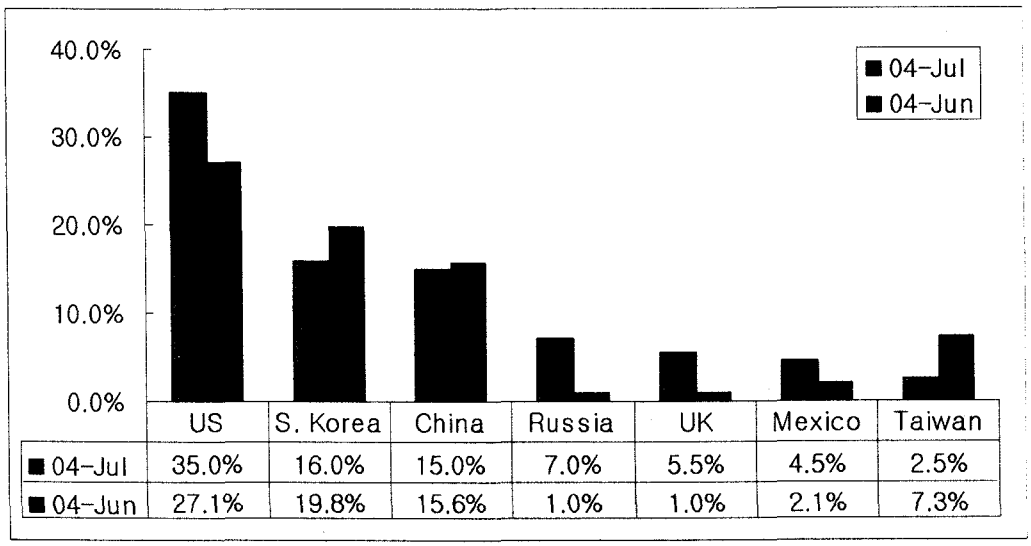
APWG(Anti-Phishing Working Group)는 이메일 사용자로부터 보고된 피싱 관련 정보를 집계하여 매월 발표하고 있다. 2004년 7월에 발간된 보고서에 따르면, 최근 7개월 동안의 피싱보고 건수의 월평균 증가율은 50%에 달하고 있다. 이에 따라, 2004년 7월에는 하루 평균 63.7건의 피싱 사례가 보고되었으며, 이러한 증가 추세는 계속 이어지고 있는 상황이다.

출처: APWG, "Phishing Attack Report" (2004.7.)



<그림 1> 월별 피싱공격 보고건수 추이

피싱 사이트 호스트 수 현황의 경우, 2004년 7월 기준 미국이 35.0%로 그 수가 가장 많으며 한국의 경우 지난달보다 비율이 줄기는 하였으나, 16.0%의 비율을 보여 미국의 뒤를 잇고 있다. [1]



<그림 2> 피싱 사이트 호스트 수 현황

같은 보고서에 의하면, 7월 중에 나타난 피싱 공격에서 가장 빈번히 나타나는 위장 대상은 Citibank(682건), U.S. Bank(622건), eBay(255건), Paypal(147건) 순으로 나타났다. 대부분의 위장 대상은 금융권 기업으로 건수 또한 꾸준한 증가세를 보이고 있다. [1]

피싱 대상	2004년 1월	2004년 2월	2004년 3월	2004년 4월	2004년 5월	2004년 6월	2004년 7월
Citibank	34	58	98	475	370	492	682
U.S. Bank	2	0	4	62	167	251	622
eBay	51	104	110	221	293	285	255
Paypal	10	42	63	135	149	163	147
Fleet	2	9	23	28	33	55	20
Lloyds	1	0	4	15	17	24	23
Barclays	1	6	11	31	15	19	17
AOL	35	10	10	9	17	14	41

<표 1> 피싱 공격의 대상 기업 (출처: APWG - Phishing Attack Report)

피싱과 관련하여 2004년 5월에 나온 Gartner의 보고서에 따르면, 5700만 명 가량의 미국인이 피싱 이메일을 수신한 적이 있고 이 중 약 19%는 이메일이 제시하는 링크를 클릭하였으며, 3%에 해당하는 사람들은 실제도 개인정보나 금융정보를 직접 입력한 것으로 나타났다. 이러한 피싱으로 의한 2003년 피해액은 약 12억 달러에 이르는 것으로 나타났다. [2] 그러나, 피싱 공격 또는 피싱으로 의심되는 공격의 76%가 과거 6개월 이전에 발생한 것으로 미루어 보아 앞으로 그 피해는 크게 증가할 것으로 예상된다.

3. 피싱 대응 법안의 제정

3.1 California Security Breach Information Act

2003년 7월 1일, 미국 캘리포니아 주정부는 프라이버시 관련 법인 'California SB 1386 (California Security Breach Information Act)'를 시행하기 시작하였다. 이 법에서는, 단 1명이라도 캘리포니아 주민을 고객으로 삼고 있는 기업은, 개인 정보가 유출될 위험이 있는 경우 보안 침해 전부를 개인에게 통지하는 것을 의무로 정하고 있다. 이를 소홀히 할 경우에는 민사적 처벌이 가해지거나, 고소를 당할 수 있다.

이 법은 위장 범죄나 데이터베이스 보안에 관한 의식을 환기시키는 역할을 하기 위해 제정되었으나, 현재까지는 이 법에 대한 인식이 저조한 상황이다. 또한, 연방 전체에 동일한 법률이 시행될 것이라는 예상과는 달리 아직 별다른 법안이 구성되고 있지 않다. [6] [7]

3.2 Identity Theft Penalty Enhancement Act

2004년 7월 14일, 미국 정부는 위장된 웹사이트를 이용해 인터넷 사용자들의 신용카드 번호, 은행계좌 정보, 사회보장번호 등을 불법적으로 취득하는 피싱에 대해 5년 이상의 징역과 25만 달러 이상의 벌금을 부과할 수 있는 법안인 ITPEA(Identity Theft Penalty Enhancement Act)을 통과시켰다.

이 법률은 범법 행위를 저지르기 위한 목적으로 타인의 신상 정보를 취득하는 자에 대한 처벌에 대해 다루고 있다. 이 법의 서명 이전에 부시 미국 대통령은 다음과 같이 언급하여, 가장 새로운 방식이면서 또한 전자상거래에 피해를 끼칠 수 있는 인터넷 사기범죄인 피싱을 방지하는 것이 이 법의 제정 배경이라는 것을 설명하였다. '신상정보 절취는 국가 경제가 기반을 두고 있는 신뢰를 손상시키는 행위이다. 어떤 사람이 보험에 가입하거나, 온라인으로 물건을 구매하거나, 계좌를 개설할 때에, 그 사람은 자신의 개인 금융 정보가 보호되고 소중히 다루어질 것이라는 신뢰를 가질 수 있어야 한다. 신상정보 절취는 피해자에 대한 직접적 피해뿐만 아니라, 신뢰를 잃어버리게 된 많은 기업과 고객들에게도 피해를 주게 된다.'

ITPEA의 제정에 따라 합법적인 허가 없이 타인의 신상정보를 '전송, 소유, 사용'할 경우 집행유예가 불가능한 2년간의 형을 선고 받게 된다. 또한, 항공기 파괴, 방화, 공항시설에서의 폭력, 주요 정부 관리자 납치 등의 테러리즘과 연계되기도 하는, 특정한 주요 범죄와 관련하여 신상정보 사기를 범할 경우 추가 5년 형을 받게 된다. [3] [4] [5] [8]

4. 피싱 대응조직의 결성

4.1 Coalition on Online Identity Theft

2003년 9월 2일, 미국의 IT 관련 단체인 ITAA(Information Technology Association of America)는 신상정보 절취 문제에 대응하기 위하여 'Coalition on Online Identity Theft'를 발족시켰다. 이 조직에는 Amazon.com (미국), eBay (미국), Microsoft 등의 온라인 서비스,

전자 상거래 기업이 참여하고 있다. 이 조직의 목적은, 신상정보 절취 문제에 대한 소비자 계몽 활동과, 참여기업과 정부기관 사이의 밀접한 협력을 위해 압력을 가하는 것이다.

이러한 취지와는 달리, 이 조직의 활동에는 또 다른 의도가 있는 것으로 파악되고 있다. ITAA는 기업에 있어 막대한 부담이 따르고, 고객들이 전자 상거래를 기피하게 되는 사태가 발생할 수 있다는 이유로 California SB 1386 시행에 반대하고 있는데, Coalition on Online Identity Theft는 이러한 ITAA에 의해 설립된 조직이다. 즉, ITAA의 주목적은 신상정보 절취에 대해 고객들에게 알리는 것임에도 불구하고, 소비자 본위보다는 기업의 이익을 대변하는 애매한 입장을 취하고 있다.

4.2 Anti-Phishing Working Group

2003년 11월, Tumbleweed Communications 社는 APWG이라는 조직을 결성하였다. 이 조직은 금융, 온라인 소매, 법률 제정, 소프트웨어 제조 분야의 업체와 ISP 등 250여 개의 다양한 기업으로 구성되어 있다. APWG의 역할은 피싱 문제와 관련하여 구성원들 간의 정보와 대책을 공유하고, 피싱관련 비용의 규모를 파악하고, 피싱에의 대응을 위한 소송 제기 등 문제 해결을 위한 업계 전체의 주의를 이끌어 내는 것이다. 피싱 공격과 이메일 사기는 많은 기업들에게 민감한 주제이기 때문에, APWG는 구성원의 기밀성을 유지하는 정책을 가지고 있다.

4.3 Trusted Electronic Communications Forum

2004년 6월 16일, 소매, 통신, 금융 서비스, 금융, 기술 등 다양한 업계의 기업들이 피싱 등의 사기 행위에 대항하여 'TECF(Trusted Electronic Communications Forum)'을 발족시켰다. TECF는 피싱, 스푸핑(Spoofing) 등 온라인 신원정보 절취 행위의 위험성 완화를 목적으로 한 단체이며, 소비자나 기업을 신원정보 절취로부터 보호하기 위한 국제표준 작업도 수행할 계획이다.

TECF 설립 기업으로는 네덜란드 ABN AMRO, 미국 AT&T Wireless, 미국 Best Buy, 미국 Charles Schwab, 미국 CipherTrust, 미국 DirecTV, 미국 E*Trade, 미국 Fidelity Investments, GE Access, 영국 HSBC, 미국 IBM, National City Bank, 미국 PostX, 영국 Royal Bank of Scotland, 미국 Siebel Systems 등이다.

APWG가 피싱 대응방침과 피싱 관련 문제를 정성적 또는 정량적 측면에서 규정하는 것에 주력하는 반면, TECF는 기술표준 책정과 정부에 대한 압력단체로서의 활동에 중점을 두고 있다.

5. 대응방안 및 결론

지금까지 살펴본 것처럼 전세계적으로 피싱 공격이 증가하고 있으며, 우리나라도 예외가 아니다. 우리나라의 경우 국내 고객 수가 많지 않은 Citibank 등의 외국 사이트뿐 아니라, 많

은 가입자를 가진 이동통신 사업자를 모방한 피싱공격이 발견되는 등 피싱에 의한 국내 피해규모 또한 작지 않을 것으로 생각된다. 그러나, 피싱의 예방 및 대처는 물론 국내 피싱공격 사례 조사 및 피해규모 파악조차 제대로 되지 않고 있다. 바이러스나 인터넷 웜과 같이 일반인들에게 알려져 있는 악성코드나 사이버 범죄의 경우, 피해자들의 신고를 통하여 현황을 파악하는 것이 용이하나, 피싱의 경우 이메일사용자들이 그 정체를 몰라서 심지어는 피셔에게 신용•금융정보를 전송하고도 피해 사실을 알지 못하는 경우가 많아, 피해 현황을 파악하기가 무척 어려운 상황이다. 이에 따라, 피싱으로 인한 피해를 막기 위해서는 기술적 측면, 법•제도적 측면, 대국민 홍보 측면에서의 대응방안 마련이 시급하다.

외국의 경우, 피싱수신을 막기 위한 기술 개발이 활발하게 이루어지고 있으며 다수의 상용 프로그램이 시장에 출시되어 있다. 그러나, 국내에서는 관련업체들의 기술개발 성과가 가시적으로 나타나지 않고 있다. 또한, 미국 등에서는 피싱에의 대응을 위한 법•제도를 마련하고 관련기구를 설립하는 등 적극적으로 대응하고 있으나, 국내의 경우 스팸메일 관련 정책이 이메일 관련 정책의 대부분으로, 이를 통하여 개인의 금융정보를 빼앗아가는 악질 사이버범죄인 피싱에 대응하는 것은 역부족이다. 대국민 홍보 또한 기술적, 법제도적 대응방안에 못지 않게 중요하다. 기술과 법제도가 정착하는 동안 피싱의 피해를 최소화하고, 장기적으로 인터넷을 통한 상거래의 신뢰를 잃지 않기 위해서는 하루 빨리 이메일 사용자들에게 피싱에 대응할 수 있는 교육을 시행하는 것이 필요하다.

참고문헌

[1] APWG, "Phishing Attack Trends Report", 2004.7.

[2] Gartner, "Phishing Victims Likely Will Suffer Identity Theft Fraud". 2004.5.

[3] http://www.theorator.com/bills108/hr1731.html

[4] http://www.ssa.gov/legislation/legis_bulletin_032603.html

[5] http://www.whitehouse.gov/news/releases/2004/07/20040715-3.html

[6] SearchCIO, http://searchcio.techtarget.com/sDefinition/0,,sid19_gci951441,00.html

[7] Watchfire, http://www.watchfire.com/legislation/sb1386.aspx

[8] ZDnet, http://zdnet.com.com/2100-1105_2-5270077.html