사회공학기법을 이용한 피싱 공격 분석 및 대응기술

이동휘* · 최경호* · 이동춘** · 김귀남* · 박상민***

요 약

최근의 해킹 공격 양상은 급격히 변화하고 있으며, 사회공학적 기법을 이용한 피싱 공격은 정보 사회를 위협하고 있다. 사회공학적 기법을 이용한 피싱 공격은 기술적으로 취약한 시스템을 해킹하는 것 이외에도 사용자를 기만하여 개인 및 기업의 내부 정보 및 중요 정보를 획득하는 수단이 되고 있다. 따라서 본 연구에서는 사회공학적 기법을 이용한 피싱 공격에 대해 국내외의 사례 분석 및 통계 분석을 통하여 향후 위협의 방향성을 찾고, 이에 대응하는 기술들을 분석하여 국내 실정에 맞는 모델을 제시하고자 한다. 이를 통해 향후 미래에 발생할 사회공학적 기법을 이용한 해킹 공격으로부터 개인 및 기업을 보호할 수 있으리라 판단된다.

Intelligence Report and the Analysis Against the Phishing Attack Which Uses a Social Engineering Technique

Dong Hwi Lee* · Kyong-ho Choi* · Dong Chun Lee**
Kuinam J. Kim* · Sang Min Park***

ABSTRACT

The hacking aspect of recent times is changing, the phishing attack which uses a social engineering technique is becoming the threat which is serious in Information Security. It cheats the user and it acquires a password or financial information of the individual and organization. The phishing attack uses the home page which is fabrication and E-mail, and acquires personal information which is sensitive and financial information. This study proposes the establishment of National Fishing Response Center, complement of relation legal system, Critical intelligence distribution channel of individual and enterprise.

Key words : Phishing, Social Engineering Thechnique

* 경기대학교 정보보호학과
** 호원대학교 국방과학기술대학
*** 인천대학교 산업경영학과

1. 서 론

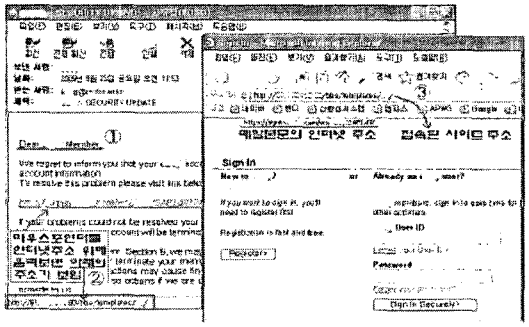
최근 정보화 사회의 진전과 더불어 유비쿼터스 환경의 진입으로, 21C 네트워킹의 활성화는 엄청난 경제적 가치를 창출하고 있다. 하지만, 인터넷 뱅킹 해킹사고, 개인 및 공공 · 민간 부문에서의 중요정보 유출사고, 다양한 변종의 웜과 바이러스의 등장 등에서 볼 수 있는 바와 같이, 정보사회의 발전과 병행하여 다양한 정보화 역기능도 증가하고 있는 것이 현실이다. 더욱 심각한 것은 최근의 사이버 공격에서 금전적인 피해를 유발하는 사이버 범죄가 차지하는 비중이 크게 증가하고 있으며, 사이버공간의 위기를 발

생시키는 공격들이 점점 통합화 · 지능화 되어 가고 있다는 점이다.

이러한 양상의 변화는 사회공학적 기법이 이용된 피싱 또한 마찬가지이며, 이에 따라 대응수단도 보다 더 체계적이어야 하고 통합화되어야 함을 요구한다. 본 논문에서는 변화하고 있는 사이버공간에서의 위협을 살펴보고, 이중 사회공학적 기법이 적용된 피싱 공격에 대한 국내외 사이버범죄 통계자료를 수집한다. 보다 더 구체적이고도 세부적인 보안 요구사항을 분석하기 위해서 실제로 발생한 사회공학적 기법을 이용한 피싱 공격의 사례들을 수집한다. 또한 세부적 기술들을 파악하기 위해서 국내외에서 시행하고 있는 기술적인 대응 방법들을 조사하여 국내에 맞는 피싱 대응 방안을 제안하였다.

2. 피싱의 정의 및 유형

최근 이슈가 되고 있는 피싱은 사용자를 속인다는 측면에서 사회공학 기술의 대표적인 사례이다. 피싱은 개인정보(private data)와 낚시(fishing)을 합성한 조어이다. 이의 대표적인 예로는 사용자에게 E-mail을 보내서 진짜 사이트처럼 보이는 가짜 사이트로 접속하게 만든 후 사용자 정보의 업데이트가 필요하다는 식의 내용을 통해 사용자의 ID와 비밀번호를 입력하게 만드는 방법이 있다.



(그림 1) 피싱 메일과 위장 홈페이지 예(1)

피싱은 공격자가 은행 등과 같은 국내외 유명기관을 사칭하여 메일을 보내고, 이를 통해 위장된 홈페이지에 접속하여 개인정보 및 중요정보를 입력하도록 유도한 뒤, 수집한 정보를 악용하는 신종 금융사기 수법이라고 정의할 수 있다. 이때 수집된 정보는 직접적으로 금융사기나 다른 범죄에 악용될 위험성이 크다.

국내외에서 발생한 피싱 사례에서 나타나는 메일이나 게시글의 주요 특징들은 다음과 같다.

① 메일 수신자의 회원정보가 명확하지 않음
② 본문 상에 링크된 인터넷 주소로 접속하여 개인정보를 입력하도록 요구
③ 이벤트나 복권에 당첨되었다는 내용
④ 이용자에게 유리한 대출 유도

이러한 피싱 공격은 직접적으로 금전적인 피해를 유발시키고 있다. 이미 피싱 공격을 통해 개인의 금융정보를 획득하여 개인 금융계좌에서 현금을 인출하여 개인에게 금전적인 피해를 유발시킨 사고가 발생하였으며, 유명기관의 브랜드에 대한 고객신뢰를 이용하여 인터넷 사용자들에게 손해를

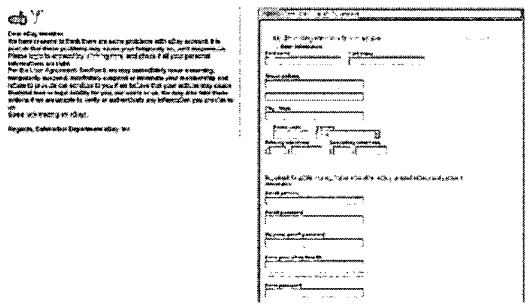
끼치기도 하였다. 이러한 피싱 공격들은 유명기관의 웹 사이트로 위장하면서 결국 기업의 인지도 손상을 초래한다. 이로 인해 e비즈니스에서 장기간에 축적한 브랜드 인지도가 단시간에 붕괴할 위험성이 있으며, 피해 기업은 이의 손상을 회복하는데 많은 시간과 비용이 소요될 것으로 판단된다.

피싱 공격의 양태는 급격히 변화하고 있으며 이의 위협도 다양하게 확산되고 있다. 최근에 발생하는 사회공학적 기법을 적용한 피싱의 주요 특징은, 기존의 기술적 취약점을 이용한 웜, 바이러스, 스파이웨어 등과 결부되어 발생한다는 것이다. 즉, 사용자 기만 뿐만 아니라 기술적인 보안 취약점을 악용하여 이를 응용하고 있는 것이다. 이렇게 사회공학적 기법을 이용한 피싱 공격은 그 대상을 일반적인 인터넷 사용자들까지 포함하여 광범위하게 확산시키고 있으며, 이를 통해 e비즈니스 전반에 걸쳐 신뢰에 관한 문제를 불러일으키고 있다. 또한 피싱 공격은 지속적으로 변화를 거듭하면서 대응책이 나올 때마다 이를 교묘히 피해나가는 새로운 공격기법이 개발되고 있으므로, 이에 대한 피해를 줄이기 위한 사회적인 대책 마련이 시급히 요구되고 있다. 이와 더불어 최근에는 고도의 숙련된 범죄 집단이 피싱을 이용하여 사기범죄를 수행할 가능성이 증대되어 가고 있으며, 조직적 범죄에 피싱 기법을 구현할 수 있는 IT 전문가가 개입되면서 피싱 수법이 고도화되고 사회적 피해도 확대되고 있음을 인식해야 한다.

3. 피싱의 피해사례 및 통계분석

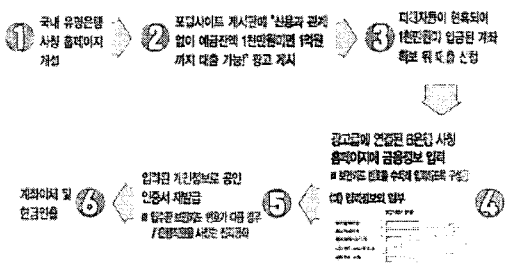
3.1 국내외 피싱 피해 사례

2003년 eBay 사건은 대표적인 해외 피싱 피해 사건이다. 피의자들은 eBay를 사칭해 "보안 위험으로 계정이 일시 차단되었으니 첨부된 링크를 클릭해 eBay 홈페이지를 통해 재등록하라"는 메일을 무작위로 발송하였고, 메일을 받은 사용자들은 신용카드번호, 사회보장번호 등을 입력하여 개인정보를 도용당한 사건이었다.



(그림 2) e-Bay를 사칭한 피싱 사건 사례(2)

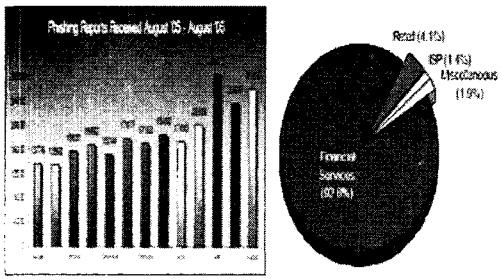
국내에서는 대출을 미끼로 한 금융사기 사건이 있었다. 피셔들은 국내 유명 포털사이트 게시판에 신용과 관계없이 '예금잔액 1,000만원 이상 있는 고객에게는 1억까지 대출가능'이라는 게시물을 올려놓고, 연락해오는 사람들에게 신용확인을 해야 한다고 속여 미리 만들어 놓은 위장사이트로 접속하도록 유도하였다. 피해자들은 자기가 거래하는 은행 홈페이지와 비슷한 화면이 나오자 별 다른 의심 없이 개인정보를 입력하였으며, 만약 보안카드 번호가 틀린 경우 은행직원을 사칭해 전화로 확인하는 등의 수법으로 모두 12명의 계좌에서 1억 2천여 만원이 인출되는 사고가 발생하였던 것이다.



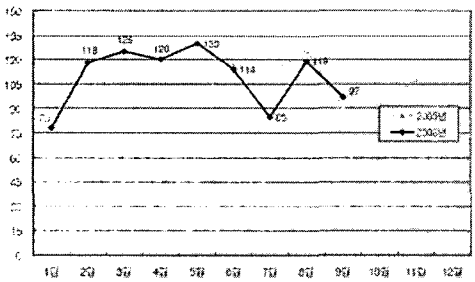
(그림 3) 대출을 미끼로 한 금융사기(1)

3.2 국내외 피싱 사고 통계

안티피싱그룹(APWG)에 따르면, 전세계 피싱 사고 접수 건수는 2004년 10월 6,957건에서 2006년 8월 26,150건으로 지속적인 증가추세를 보이고 있다. 피싱 공격이 발생하는 사업부문은 금융기관이 92.6%로 가장 많았으며, ISP가 1.4%, 소매부문이 4.1%를 차지하고 있다.



(그림 4) 국내외 피싱 통계(3)



(그림 5) 국내 피싱 통계(4)

Krcert/cc의 통계에 의하면, 국내 피싱 피해 접수건수는 2005년에 총1,087건 이었으며, 2006년은 9월까지 986건에 도달하였다. 동년 9월에 발견된 피싱 사이트만도 97건으로 집계되었다.

피싱 피해 규모는 금융기관의 공식적인 피싱 피해 발표 회피 및 피해 상황에 대한 인식 미흡 등으로 인해 조사기관에 따라 많은 차이를 발생하고 있다. Ponemon은 피싱 사고로 인한 금전적인 피해규모가 미국에서만 약 5천억 규모에 이를 것으로 추정하고 있으며, 가트너 그룹은 2004년 한해에 만 240만 인터넷 이용자들이 피싱 피해를 입었으며, 그 피해액은 약 1조원으로 추정하고 있다. APWG은 매달 피싱 공격 증가율이 50%에 이르고 있으며, 피싱 공격의 지능화로 피싱 메일에 5%의 이용자가 응답할 것으로 예상하고 있다[2]. 이러한 피해사례와 각종 통계들에 비추어 볼 때, 피싱에 대한 위협은 나날이 증가하고 있으나 인터넷 이용자들의 피싱 방법의 지능화와 피싱에 대한 인식 수준은 여전히 미흡하여[5, 6] 피싱으로 인한 피해가능성이 매우 높은 것으로 판단된다.

국내외 통계현황들에서는 지속적으로 피싱 사고가 증가하고 있는 추세이며, 또한 이러한 문제는 어느 한 국가만의 문제가 아니라는 것을 보여준다. 피싱 공격의 초기에는 영문 E-mail을 이용한 사례가 많아, 국내 피싱 피해 사례가 적었다. 그러나 최근에는 각국의 언어로 작성된 사이트들이 피싱 공격에 이용되는 사례들이 발생하고 있으므로[7], 이의 위협이 전세계적으로 확산되는 추세임을 인지하고, 이에 대한 대비책을 마련해야 한다.

4. 피싱 대응 기술

피셔들은 다양한 기술과 기법을 이용하여 피싱 공격을 성공시키려 하고 이를 통해 인터넷 이용자의 정보 유출을 시도하고 있다. 이들은 보통 기술적인 기법과 사회공학적인 사용자 기만, 즉 속임수를 병행하여 사용하고 있다. 최선의 피싱 방어를 위한 기술적인 방어 매커니즘은 사용자 측면에서의 방어와 서버 측면에서의 방어이다.

4.1 사용자 측면에서의 방어

일반 사용자 측면에서, 피싱 공격에 대한 대응은 매우 취약하다. 이는 피싱 공격 위협에 대한 인식 부족 및 대응방안 확보 미흡에서 기인한다. 이에 각국의 보안기관 및 사회단체에서는 각종 대응

기술 제공과 교육 등을 통해 사용자에게 피싱 공격에 대한 경각심을 일깨우고, 피해를 방지하려 한다. 이때 사용되는 방법들은 아래와 같다.

- 인터넷 브라우저에서의 차단 기능
- 광고 홍보성 메일 차단 기능
- 피싱 피해 사례 및 통계 제공
- 이메일의 전자서명 첨부 기능
- 일반적 보안 준수 사항 고지

4.2 서버 차원에서의 방어

사이버 공간에서 직접적으로 인터넷 서비스를 제공하는 기업 및 조직들이 자신들이 관리하는 자원에 대한 피싱 방어기술 구현을 위해 피싱 위협에 대한 교육과 피싱의 원인을 제거하는 내부적 업무 지침 및 기술 개발에 노력하고 있다. 이때 사용되는 방법들은 아래와 같다.

- 피싱 피해 사례 및 교육자료 배포
- 미연의 사고 방지를 위한 자사 정책 안내
- 업체간 정보유통 경로 사전 검증
- 전자서명 및 E-mail 검증
- 보안을 고려한 웹 응용프로그램 개발
- 강력한 인증 시스템 사용
- 라우터 및 게이트웨이 보호
- 도메인 관리

현재 사회공학적 기법을 이용한 피싱 공격에 대한 방어 기술들은 구체적으로 웹 사이트 인증, 메일 서버 인증, 전자 서명 메일 등이 이용되고 있으며, URL 스푸핑을 이용한 피싱 공격의 방어를 위한 매커니즘도 이미 특허가 공개된 상태이다. 또한 세계적으로 많이 알려진 구글, G메일, Microsoft社 등도 자사의 고객들을 피싱 위협으로부터 보호하기 위한 수단들을 제공하고 있다.

그러나 이러한 피싱 방어 노력에도 불구하고 해결해야 할 문제점들은 여전히 많이 남아 있다. 첫째, 일방적인 사건 사례 및 통계현황의 전달이다. 일반적인 인터넷 사용자에게 사회공학적 기법이 이용된 피싱 공격에 대한 인식은 현재도 매우 낮은 것으로 평가되어 있으며, 이는 공공기관 및 보안업체에서의 교육 또는 홍보활동이 미흡함을 시사한다. 또한 각국의 인터넷 사용 환경이 다른 만큼, 사회공학적 기법을 이용한 피싱의 양태도 다르며, 이에 따른 세부적인 대책을 세우기 위한 사례 분석이 필요하다.

둘째, 일반사용자들이 쉽게 사용할 수 있는 클라이언트 기반의 보안 프로그램 개발이 필요하다. 현재는 정보사회를 기반으로 하고 있으나, 일반 사용자에게는 사이버공간의 광범위성과 비대면성, 익명성을 이해하기는 어렵다. 이러한 상황은 인터넷 사용자적 입장에서 운용할 수 있는 안전한 웹 서핑을 위한 프로그램을 필요로 한다. 이를 통해 보안정책 및 지침을 중앙에서 고지하는 수준이 아닌, 이용자가 쉽게 인지하고 정보를 획득할 수 있는 환경을 구축해야 한다.

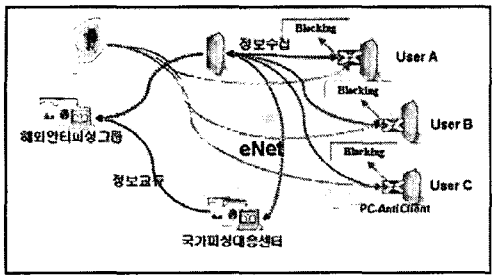
이러한 기술의 개발은 향후 사회공학적 기법을 이용한 해킹 공격이 피싱 뿐만 아니라 파밍, XSS, ActiveX, 비싱 등과 같이 확대되었을 때에도 안전한 사이버 공간을 유지할 수 있게 할 것이다. 특히, 향후 사회공학적 기법을 이용한 해킹 공격들이 기존의 기술적인 보안 취약점을 이용함으로써 더욱 확산되리라 예상되는 이 시점에서는 더욱 절실히 요구된다.

5. 향후 기술적 대응방안

5.1 National Phishing Response Center

사회공학적 기법을 이용한 피싱 공격들은 다양한 피싱 방어 기술들이 개발됨에도 불구하고 새롭게 나타나고 있다. 이러한 역동적인 변화 속에서 사이버안전에의 위협은 점차 확대되고 있으며, 이를 National Phishing Response Center의 통합관

제 서비스를 통해 차단해야 한다.



(그림 6) National Phishing Response System

National Phishing Response Center는 국내 인터넷 사용 환경 및 피싱 사례들을 분석하여 예측 가능한 사이버범죄 행위들을 차단하고, 네트워크 패킷 분석과 운영 중인 웹 서버들의 파일 변조 유무를 체크하여 네트워크 환경에서의 위협을 방어하는 역할을 수행해야 한다. 이와 더불어 위협에 대한 데이터베이스를 축적하고 개인정보 및 중요 정보에 대한 중점관제를 통해 실시간 사이버 위협 탐지, 조기대응 체제를 구축해야 한다. 여기서는 정보의 중앙 집중 및 위협 발생과 대응에 대한 시차를 줄이기 위해 Client의 Secure Program을 필요로 한다. 이는 최근의 피싱 위협이 아주 짧은 시간에 발생하여 피해를 입히고 사라지기 때문에, 이러한 경우를 대비하기 위함이다.

5.2 Client Secure Program

National Phishing Response System의 통합 피싱 관제 서비스를 위한 클라이언트 프로그램으로 개인 PC에 설치되어 National Phishing Response Center의 정보와 비교, 실시간으로 피싱 사이트 접속시 차단 및 자동신고가 가능한 프로그램이다. 이 두 가지 체계는 서로 연동되어 피싱 사이트의 가능성을 데이터베이스를 통하여 비교할 수 있으며, 이를 통해 실시간적인 위협 검출 및 사용자 방어를 수행할 수 있다. 또한 피싱 위협에 대한 자동 신고 기능을 수행하며, 인터넷 이용자를 위한 Secure 웹 서핑을 가능하게 해준다.

6. 결 론

최근에 나타나는 사회공학적 기법을 이용한 피싱 공격은 상상을 초월하는 속도로 지능화 · 다양화 되고 있으며, 급속하게 확산되는 피싱을 방치할 경우 e비즈니스의 근본이 흔들릴 수도 있다는 위기감을 인식하고, 이에 대한 대책 및 대응기술 확보에 주력해야 한다.

그러므로 본 연구에서 제안한 범정부 차원의 체계적인 대응방안 마련이 필요하다. 따라서 향후 상존하는 위협요소에 대한 위험(Risk)을 평가하고, 위험을 감소시키기 위한 정책 및 절차를 제공하며, 사고 탐지 및 신속한 신고, 대응 절차를 제공하는 프로그램의 개발이 필요하다.

참 고 문 헌

[1] 정보통신부 · 한국정보보호진흥원 · 금융감독원, "피싱예방가이드", 보호나라 배포자료.

[2] 한국정보보호진흥원, "새로운 사이버 위협 : 피싱", 2005.

[3] AWPG, "Phishig Activity Trends Report", August, 2006.

[4] 한국정보보호진흥원, 인터넷 침해사고 동향 및 분석 월보, 각월호.

[5] Demopoulos Associates, "User Phishing Awareness Survey", 2005.

[6] Princeton Survey Research Associates International, "Spyware Survey Final Topline", 2005.

[7] 안랩 스파이제로, '일본에서 발견된 피싱 사이트', http://auction.ahnlab.com/badcode_view.asp?seq = 7818.

이 동 휘

2000년 경기대학교 전자계산학과 (이학사)
2003년 경기대학교 정보보호기술 공학과(공학석사)
2004~현재 경기대학교 정보보호 학과(박사과정)

최 경 호

2003년 경기대학교 경제학과 (경제학 학사)
2005년 경기대학교 경제학과 (경제학 석사)
2005년~현재 경기대학교 정보보호학과 박사과정

이 동 춘

연세대학교 컴퓨터과학과 (공학박사)
현재 호원대학교 국방과학기술대학 학장
관심분야 : 이동/무선 통신, USN 및 보안

김 커 남

미국 캔자스대학 수학과(응용수학사)
미국 콜로라도주립대학 통계학과(통계학석사)
미국 콜로라도주립대학 기계산업공학과(기계·산업공학박사)
현재 경기대학교 정보보호학과 교수

박 상 민

1970년 한양대학교(공학사)
1983년 한양대학교(공학석사)
1990년 한양대학교(공학박사)
2002년~현재 동북아전자물류연구센터 소장
현재 인천대학교 산업경영학과 교수