피싱에 대한 분석 및 대응방안에 대한 연구

강현중*

요 약

유선전화로 시작된 피싱 사기는 스미싱, 파밍 등으로 계속 진화하고 있다. 우리가 유·무선 통화, 문자, 이메일, 온라인 뱅킹 등을 편리하게 이용하고 있는 만큼 그에 따라 해킹 및 피싱 사기 공격의 종류도 진화하고 다양해지고 있는 것이다. 본 논문에서는 그에 따라 피싱의 종류에 따른 공격방법을 살펴보고 그에 따른 일반적인 예방대책을 살펴본다. 그리고 사용자들이 직접적으로 느낄 수 있는 실질적인 예방대책과 정부에서 추진할 수 있는, 장기적인 대책을 제시하였다. 계속 진화하는 피싱 사기를 단기간 내에 박멸하기는 어려우며 정부의 장·단기적인 대책과 기술개발 그리고 지속적인 홍보 등이 해결책이 될 것이다. 물론 SNS를 비롯한 인터넷상의 매체들도 홍보에 큰 도움이 되고 있다. 아울러 새로 개발되는 서비스 기술들은 보안상의 허점이 없도록 다시 한번 살펴서 기술개발이 이루어져야 할 것이다.

A Study of the Analysis and Countermeasure about the Phishing Scam

Kang Hyun Joong*

ABSTRACT

Phishing scans through wired telephones have been evolving into smissing and pharming. While we use wire or wireless telephones, text messages, e-mails, and online-banking conveniently, the ways of hacking and phishing attacks are getting developed and various. This paper investigates the various aspects of attacks depending on the kinds of phishing and suggests general prevention measures. In addition, the user-oriented practical preventive measures and government-driven long term measures are proposed in this paper. Technological developments, short or long term preventive measures proposed by the government, and continuous public relations could be solutions since in a short time, it could be difficult to eradicate phishing scams evolving continuously. Besides, the internet media as well as SNS are great helps in promoting the preventives against phishing and smissing. Finally this paper asserts that the newly developed service technology should be made carefully without security problems.

Key Words : Social Engineering, Voice Phishing, Smishing, Pharming

접수일(2014년 9월 17일), 수정일(1차: 2014년 9월 26일), 게재확정일(2014년 9월 29일)

* 서일대학교 인터넷정보과 교수

Ⅰ. 서 론

우리는 최근 수십년 간에 걸친 유선전화, 휴대폰, 스마트폰, 인터넷상의 각종 인프라 및 서비스, SNS 등, 이루 다 나열할 수 없는 유·무선 통신과 서비스들의 급속하고도 획기적인 발전으로 인하여 편리함과 행복함을 만끽하고 있다. 이러한 인프라는 물론 우리나라의 인터넷보급률 및 속도가 세계의 상위권이기 때문에 가능한 일이기도 하다. 그러나 이렇듯 인터넷을 기반으로 우리의 삶을 편안하고 행복하게 만드는 인프라만 늘어나는 것이 아니라 우리를 속이고 괴롭히는, 정신적인 피해는 물론 심지어는 금전적인 피해까지 입히는 일들이 발생하고 있으며 점점 지능화되고 있다. 전화사기로 시작된 피싱은 휴대폰 문자, 악성코드가 포함된 파일을 첨부한 이메일, 휴대폰에 URL이나 악성코드가 포함된 앱 설치 등으로 계속적으로 진화하고 있다.

본 논문에서는 이렇듯 계속적으로 진화·발전하고 있는 피싱 기술들을 분류, 분석하고 적절한 대응 방안들을 제시하고자 한다. 2장에서는 관련연구로써 그동안의 피싱사 기 공격기술에 대해 정의하고 그에 대한 일반적인 대응방안들을 살펴본다. 3장에서는 이들 피싱 사기 공격들을 막을 수 있는 보다 실질적이고 합리적인 방안을 제시하고 4장에서는 정부에서 추진해야 되는 장·단기적인 대책을 제시하고 5장에서 결론을 맺고자 한다.

Ⅱ. 관련연구

본 장에서는 피싱 관련 용어와 해당 사기 혹은 공격 형태를 소개하며 아울러 알려져 있는 예방 대책에 대해 소개한다.

2.1 사회공학기법

피싱 사기의 시초는 1960~70년대의 '사회공학'이라는 용어로 거슬러 올라가야 한다. 위키백과에 따르면 "사회공학(社會工學, 영어: Social Engineering)은 보안학적 측면에서 기술적인 방법이 아닌 사람들 간의 본적인 신뢰를 기반으로 사람을 속여 비밀 정보를 획득하는 기법을 일컫는다."로 서술되어 있으며 아울러 "컴퓨터 보안에서 인간 상호 작용의 깊은 신뢰를 바탕으로 사람들을 속여 정상 보안 절차를 깨트리기 위한 비기술적 침입 수단. 우선 통신망 보안 정보에 접근 권한이 있는 담당자와 신뢰를 쌓고 전화나 이메일을 통해 그들의 약점과 도움을 이용하는 것이다. 상대방의 자만심이나 권한을 이용하는 것, 정보의 가치를 몰라서 보안을 소홀히 하는 무능에 의존하는 것과 도청 등이 일반적인 사회 공학적 기술이다. 이 수단을 이용하여 시스템 접근 코드와 비밀번호를 알아내 시스템에 침입하는 것으로 물리적, 네트워크 및 시스템 보안에 못지 않게 인간적 보안이 중요하다"로 부연 설명되어 있다[1]. 현재 우리는 PC(Personal Computer)를 주로 사용하고 있지만 상용컴퓨터가 개발되기 시작한 1960~70년대에는 개인이 컴퓨터를 사용하기는 그리 자원이 넉넉하지 않았다. 사용컴퓨터의 초기 모델인 마크 I, 유니백(UNIVAC), IBM 701 등은 그 운영체제가 UNIX로 시분할방식에 의한 병렬처리 시스템이다. 따라서 하나의 대형컴퓨터에 여러 명의 사용자가 단말기로 접속하여 아이디와 비밀번호로 관리되며 순서에 따라 일정한 시간간격(Time Slice)으로 나누어 사용하였다. 따라서 아이디는 모든 이들에게 부여되지 않았으며 대학의 경우에 일부 교수나 대학원생들에게만 부여되었다. 따라서 컴퓨터를 반드시 사용하고 싶은 이들(해커 : 이 당시는 열심히 컴퓨터를 공부하는 사람들)은 본의 아니게 아이디 소유자들과 대화를 나누면서 아이디와 비밀번호를 슬쩍 알아내는 방법을 취했는데 그것이 바로 사회공학 기법인 것이다.

2.2 전화사기 (Voice Phishing)

피싱(phishing)은 '개인정보(private data)'와 '낚시(fishing)'를 뜻하는 영어를 합성한 조어로서 전화를 통하여 상대방의 신용카드 번호 등의 개인정보를 불법으로 알아낸 뒤 이를 범죄에 이용하는 전화금융사기 수법을 말한다. 처음에는 국세청 등 공공기관을 사칭하여 세금을 환

급해준다는 빌미로 피해자를 현금지급기(ATM) 앞으로 유도하는 방식이었으나, 이같은 수법이 널리 알려진

뒤에는 피해자가 신뢰할 수 있도록 하기 위하여 사전에 입수한 개인정보를 활용하는 등 다양한 수법들이 등장하였다 [2].

< 표 1> 보이스 피싱의 유형 [2-3]

순서	사칭	사기 및 요구 내용
1	국세청, 국민연금관리공단	세금, 연금 등을 환급한다고 유혹, ATM기로 유인하여 계좌이체유도
2	신용카드사, 은행, 채권추심단	연체대금입금, 카드나 계좌번호 등의 개인정보탈취, 고액 유료결제 ARS 이용유도
3	국제전화	국제전화 수신자요금부담
4	검찰, 경찰, 금융감독원 직원, 시군관계자	출두, 벌금입금, 범죄연루를 빌미로 개인정보탈취
5	가전회사나 백화점	경품이벤트 당첨을 빌미로 당첨상품 세금부담, 개인정보탈취
6	납치범, 병원, 행인	자녀가 납치 혹은 사고를 당했다며 부모에게 돈을 요구
7	동창회, 종친회	동창회·종친회 명부를 입수하여 회비를 송금하도록 요구
8	택배회사, 우체국	우체국 방문, 우편물이나 택배물건이 계속 반송된다는 구실로 개인정보 요구
9	대학	대학입시에 추가로 합격을 빌미로 등록금 입금 요구
10	부동산소개소	내놓은 매물을 높은 가격으로 팔고 싶으면 정보지에 광고를 내라고 유도, 광고료 탈취

그 유형들을 표로 정리하면 <표 1>과 같이 다양하며 이러한 유형들은 크게 분류한 것이고 보다 다양하게 파생되기도 한다. 한국인터넷정보원(KISA)은 이로 인한 피해를 예방하기 위하여 다음과 같은 '보이스 피싱 예방 10계명'을 정하여 발표하였다.

① 미니홈페이지나 블로그 등 1인 미디어 안에 전화번호 등 자신과 가족의 개인정보를 게시하지 않는다.
② 종친회·동창회·동호회 사이트 등에 주소록 및 비상연락처 파일을 게시하지 않는다.
③ 자녀 등 가족에 대한 비상시 연락을 위하여 친구나 교사 등의 연락처를 확보한다.
④ 전화를 이용하여 계좌번호·카드번호·주민등록번호 등의 정보를 요구하는 경우에 일체 대응하지 않는다.
⑤ 현금지급기를 이용하여 세금 또는 보험료 환급, 등록금 납부 등을 하여 준다는 안내에 일체 대응하지 않는다.
⑥ 동창생 또는 종친회원이라고 하면서 입금을 요구하는 경우 반드시 사실 관계를 재확인한다.
⑦ 발신자 전화번호를 확인하여 표시가 없거나 처음 보는 국제전화 번호는 받지 않는다.
⑧ 자동응답시스템(ARS)을 이용한 사기전화를 주의한다.
⑨ 본인의 은행계좌에서 돈이 빠져나가는 것을 바로 인지할 수 있도록 휴대폰 문자서비스를 적극 이용한다.
⑩ 속아서 전화 사기범들 계좌에 자금을 이체하였거나 개인정보를 알려준 경우에 즉시 관계 기관에 신고하고, 거래 은행에 지급정지를 요청하고 금융감독원이나 은행을 통하여 개인정보 노출자 사고예방시스템에 등록하여 추가 피해를 최소화한다.

전화사기는 한동안 급속하게 퍼졌으나 그에 따라 방송통신위원회는 2012.6.28에 “보이스피싱 피해예방을 위한 발신번호 조작방지 가이드 라인”을 마련하였고 금융감독원은 2011.9.29에 전화금융사기 피해금 환급제도 시행“을 발표하였으며 2011.11.30에 ”경찰청 112 센터를 통한 보이스 피싱 피해금 지급정지 신청제도“를 마련하기도 했다. 이러한 기관들과 신문, 방송 그리고 인터넷 등에서의 보도, 예방홍보, 사례소개 등으로 이제는 그 피해가 많이 줄어졌으며 그에 따라 다른 형태의 신종 사기로 변형되어가고 있다 [4].

2.3 이메일 사기 (E-mail Phishing)

두산백과에서 정의한 것에 의하면 “금융기관 등의 웹사이트나 거기서 보내온 메일로 위장하여 개인의 인증번호나 신용카드번호, 계좌정보 등을 빼내 이를 불법적으로 이용하는 사기수법이다. 대표적인 수법으로 이메일의 발신자 이름을 금융기관의 창구 주소로 한 메일을 무차별적으로 보내는 것이 있다. 메일 본문에는 개인정보를 입력하도록 촉구하는 안내문과 웹사이트로의 링크가 기재되어 있는데, 링크를 클릭하면 그

금융기관의 정규 웹사이트와 개인정보입력용 팝업 윈도가 표시된다. 메인윈도에 표시되는 사이트는 '진짜' 이지만, 팝업 페이지는 '가짜'이다. 진짜를 보고 안심한 사용자가 팝업에 표시된 입력란에 인증번호나 비밀번호, 신용카드번호 등의 비밀을 입력·송신하면 피싱을 하려는 자에게 정보가 송신된다. URL에 사용되는 특수한 서식을 이용하여, 마치 진짜 도메인에 링크되어 있는 것처럼 보이게 하거나, 팝업 윈도의 어드레스 바를 비표시로 하는 등 교묘한 수법을 이용하고 있어 피해자가 속출하고 있다" [5].

그에 따라 최근 정보통신부가 발표한 피싱 대응요령을 보면 다음과 같다.

① 은행, 카드사 등에 직접 전화를 걸어 이메일에서 안내한 사항이 사실인지를 확인한다.
② 이메일에 링크된 주소를 바로 클릭하지 말고, 해당 은행, 카드사 등의 홈페이지 주소를 인터넷창에 직접 입력해 접속한다.
③ 출처가 의심스러운 사이트에서 경품에 당첨됐음을 알리는 경우, 직접 전화를 걸어 확인하고 사실인 경우에도 가급적 중요한 개인정보는 제공하지 않는다.
④ 피싱이 의심되는 메일을 받았을 경우 해당 은행, 카드사 및 한국정보보호진흥원 등에 신고한다.
⑤ 은행, 신용카드, 현금카드 등의 내역을 정기적으로 확인한다 [5].

전화사기는 유선전화기가 각 가정에 1대씩은 대부분 보급되어 있고 휴대폰 역시 초등생부터 노인층에 이르기까지 대다수 보급되어 있기 때문에 그 공격대상이 폭넓고 다양했다. 그러나 이메일 사기는 이메일을 주로 사용하는 즉, 컴퓨터로 업무나 연락 등을 취하는 사람들에게만 공격되므로 전화사기보다는 그 공격대상이 좁은 편이며 따라서 그 피해도 작은 편이다.

2.4 문자 사기(Smishing)

위키백과에서 정의한 것에 따르면 "문자메시지 피싱(SMS phising, 스미싱, Smishing)은 문자메시지를 이용한 피싱이다. 스미싱은 SMS(문자메시지)와 피싱(Phising)의 합성어이다. 신뢰할 수 있는 사람 또는 기업이 보낸 것처럼 가장하여 개인비밀정보를 요구하거나 휴대폰 소액 결제를 유도한다. 최근 들어 스마트폰 이용자들이 늘어남에 따라 돌잔치, 결혼 청첩장 등이 도착하였다고 하면서 링크를 걸어 안드로이드 애플리케이션 설치파일인 apk 파일을 설치하도록 유도하여 휴대폰 내의 정보를 빼가는 수법이 늘고 있다 [6]."

일반 휴대폰만 이용하던 시기에도 문자 사기는 존재했지만 그 피해는 미미했다. 단순히 우체국에 등기 혹은 택배가 도착했다는 문자, 경찰 혹은 검찰청에 출두하라는 등의 장난 문자가 대부분이었다. 그러나 스마트폰의 대중화되면서 문자 사기는 다양해지고 현재도 진화하고 있으며 금전적인 피해도 커지고 있다. 이는 스마트폰이 작은, 휴대용 PC이어서 문자에 포함되어 있는 URL을 클릭하면 악성코드가 설치되며 스마트폰에 저장되어 있는 개인정보를 빼내가 스마트폰 소액결제가 이루어질 수 있기 때문이다. 스미싱의 유형을 살펴보면 위의 <표 2>와 같다.

< 표 2> 스미싱의 유형

순서	사칭	사기 및 요구 내용	비교
1	돌잔치, 결혼청첩장, 회갑연 등	행사를 알리며 궁굼증을 유발시키고 URL 클릭시 개인정보 유출, 소액결제	
2	각종 무료쿠폰, 할인권, 교환권, 상품권	공짜, 할인, 무료 등으로 UR 클릭을 유도하여 개인정보 유출, 소액결제	
3	은행, 우체국, 금융기관	개인정보 유출(보안승급), 계좌에서 출금 등을 빌미로 URL을 누루게 하고 계좌번호, 비밀번호, 보안카드 등을 입력유도	
4	성적, 자극적 문자	성적이며 자극적인 문자로 URL 클릭을 유도하여 소액결제	고전 방법
5	택배사나 기사	배달주소가 틀리거나 택배조회를 알리며 URL 클릭을 유도	구정, 추석
6	승인번호 알림 구매통보	발신번호로 전화하면 취소하려면 승인번호를 알려달라고 하여 결제가 이루어짐	승인번호를 알려줌
7	통신사	통신 미납금 안내, 이용내역 확인, 데이터 초과 사용요금 청구서 등으로 유도	
8	인터넷 쇼핑몰, 카드사	상품결제 혹은 카드결제가 성공했다는 등으로 유도	
9	경찰	귀하의 차량이 과속카메라, 불법주차 단속 적발 등으로 유도	
10	예비군, 민방위 훈련	예비군 혹은 민방위 비상소집 훈련일정확인을 유도	

문자에 포함되어 있는 URL 링크를 클릭하면 악성코드가 설치되며 한도 30만원 미만의 소액결제가 이루어지게 된다. 소액결제를 위해서는 문자로 인증번호를 받아 이를 다시 결제화면에 입력해야 하지만 설치된 악성코드가 이를 가로채, 입력하여 스마트폰 사용자도 모르게 결제가 이루어지게 된다. 사용자는 월말에 휴대폰 이용료 명세서를 받은 후에 피해 사실을 인지하게 되기 때문에 신고 등의 사후 처리도 쉽지 않게 된다. 이에 대한 피해 예방법을 살펴보면 다음과 같다.

① 사용하고 있는 스마트폰의 통신사의 고객센터 홈페이지를 통하여 소액결제 서비스를 차단 요청을 한다. (혹은 소액결제액을 0원으로 설정)
② 스마트폰용 백신 프로그램을 설치하여 주기적으로 악성코드를 검색, 삭제한다.
③ 출처가 확인되지 않는 웹 어플리케이션이 설치되지 않도록 보안설정을 강화시킨다.
④ '무료', '조회', '공짜' 등의 문구를 스팸 차단으로 등록하여 문자 수신을 차단한다.
⑤ 유료 웹 어플리케이션을 무료로 사용하기 위하여 인터넷에서 apk 파일을 다운받아 설치하지 않도록 한다.

스미싱 사기는 계절별, 유행별로 변화하기도 하는데 가족행사가 많은 5월에는 <표 2>의 1번과 같은 문자가, 구정과 추석 등을 앞두고는 2, 5, 8번의 문자가 기승을 부리기도 한다. 또 독도관련 서명참여를 유도하거나 월드컵 응원유도를 하는 등의 스미싱 사기도 이벤트성으로 뿌려지기도 한다.

2.5 파밍 사기(Pharming)

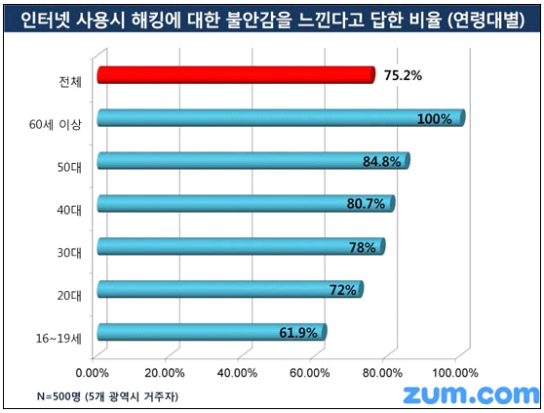
매일경제용어사전에 따르면 파밍 사기의 정의는 "합법적으로 소유하고 있던 사용자의 도메인을 탈취하거나 도메인 네임시스템(DNS) 또는 프락시 서버의 주소를 변조함으로써 사용자들로 하여금 진짜 사이트로 오인하여 접속하도록 유도한 뒤 개인정보를 훔치는 새로운 컴퓨터 범죄 수법이다. 해당 사이트가 공식적으로 운영하고 있던 도메인 자체를 중간에서 탈취하는 수법으로 '피싱(phishing)에 이어 등장한 새로운 인터넷 사기 수법이다. 사용자가 아무리 도메인 또는 URL 주소를 주의 깊게 살피더라도 늘 이용하는 사이트로만 알고 아무런 의심 없이 접속하여 개인 아이디(ID)와 암호(password), 금융 정보 등을 쉽게 노출시키게 된다. 따라서 피싱 방식보다 피해를 당할 우려가 더 크다. 피해를 방지하기 위해서는 브라우저의 보안성을 강화하고, 웹사이트를 속일 수 있는 위장기법을 차단하는 장치를 마련해야 한다. 또 전자서명 등을 이용하여 사이트의 진위 여부를 확실하게 가릴 수 있도록 해야 하고 사용하고 있는 DNS 운영 방식과 도메인 등록 등을 수시로 점검해야 한다 [7].

파밍 공격에 대한 예방법으로는 다음과 같은 것이 있다.

① 송신자가 불분명한 이메일의 첨부파일이나 출처가 의심스러운 파일(동영상, 음악파일 등)을 열거나 다운로드받지 않는다.
② 백신 프로그램을 설치하여 주기적으로 악성코드를 검색, 삭제한다.
③ 인터넷뱅킹 서비스 이용 시에 정상적인 은행사이트라면 보안카드의 시리얼번호와 코드표 전체의 입력을 요구하는 일은 없으니 절대 입력을 하지 않도록 주의한다.
④ 파밍캅 프로그램을 다운로드받아 백신과 같이 이용한다. 파밍캅은 악성코드가 감염시킨 hosts 파일의 감염된 사이트 내용을 수정하여 정상 사이트로 접속하도록 유도해준다.

Ⅲ. 현실적인 예방 대책

2014년 8월 6일, 데이터넷의 "보안 우려하며 인터넷 사용습관 안고쳐"라는 기사에 따르면 "인터넷 사이트와 스마트폰을 통해 악성코드가 유포돼 사용자들의 개인정보와 금융정보가 탈취되거나 실제 금전적인 피해를 입게 된 사례가 급증하고 있어 사용자들이 사이버 보안에 많은 우려를 나타내고 있다. 그러면서도 보안에 취약한 인터넷 사용습관을 거의 개선하지 않는 모순된 모습을 보이고 있다.



(그림 1) 인터넷 사용시 해킹 불안감의 연령대별 통계 [8]

줌닷컴(zum.com)이 모바일 리서치 업체인 오픈 서베이를 통해 7월 한 달 동안 전국 5개 광역시에 거주하는 500명의 인터넷 사용자들을 대상으로 실시한 'PC·모바일 이용행태 및 보안인식에 관한 조사'에서 이같이 나타났다고 1일 밝혔다. 인터넷 이용자의 75.2%가 인터넷 보안위험을 느끼며, 나이대가 많을수록 인터넷 사용시 해킹의 위험에 대한 불안을 크게 느끼는 것으로 나타났다. 인터넷 서핑 시 보안에 대한 불안함이 있다고 응답한 응답자는 16세~19세의 경우 61.9%, 20대가 72%, 30대가 78%, 40대가 80.7%였으며 50대는 84.8%, 60세 이상은 100%로 나이가 들수록 해킹 위험에 대한 불안도가 커지는 경향을 보였다. 남성의 69.2%, 여성의 81.2%가 해킹 등에 대한 불안감을 느낀다고 답해 여성이 보안에 대한 불안을 더 느끼는 것으로 드러났다.

이는 나이가 들수록 최신 정보나 뉴스 그리고 최신 기술에 따른 컴퓨터(스마트폰 포함) 사용에 어려움이나 불편함이 따르기 때문인 것으로 추측된다. 특히 여성들은 남자들에 비해 컴퓨터 등의 기기들에 대한 사용상의 두려움이 다소 높기 때문인 것으로 사료된다.

"응답자들이 해킹방지 대비책으로 가장 많이 꼽은 것은 1위가 백신프로그램 사용(56%), 2위가 OTP사용하거나 모르는 URL 클릭 자제(26%) 였으며, '아무것도 하지 않는다'가 8.9%로 3위를 차지했다. 반면, 경찰청 파밍캅 등 해킹방지 프로그램 사용(5.5%), 해킹 피해 보상서비스 가입(3%)등 적극적인 방어 및 구제책을 이용한다고 답한 응답자는 8.5%에 불과해 상대적으로 적었다. 해킹 방지 조치를 취하지 않는 가장 큰 이유로는 '모르기 때문'이 1위로 꼽혔다. 응답자의 51.7%가 어떤 조치를 취해야 할 지 몰라서 보안 무방비 상태에 있다고 답했다. 그 뒤를 이은 2위가 '귀찮아서'(23.3%), 3위가 '해킹이 불안하지만 실제 발생 가능성은 낮아 보여서'(16.7%)로 나와 안일한 태도 때문에 보안 대비를 미루는 경우도 상당한 것으로 드러났다 [8]."

이 조사에 따르면 아직도 많은 사람들이 해킹방지 대책을 모르고 있거나 알고 있더라도 구체적으로 모르는 것으로 파악된다. 또한 해킹을 당하는 것을 남의 일이라 생각하고 나에게는 벌어지지 않으리라 생각하고 있는 것 같다. 따라서 이 장에서는 앞에서 소개된 일반적인 예방대책보다는 현실적인 예방 방안을 소개하고자 한다.

3.1 전화사기에 대한 예방책

앞에서도 언급하였듯이 전화사기는 언론 및 인터넷 등의 뉴스와 사고 사례 등이 소개되고 예방방법들이 홍보되면서 점차 예방이 되었으며 그에 따라 전화사기도 줄어들고 있다. 여기에서는 앞에서 소개한 전화 사기의 예방책과도 다른 각도에서의 예방 방안을 제시하고자 한다.

<집이나 회사에서 유선전화로 받았을 경우>

① 일반적으로 유선전화기는 상대방, 즉 발신자의 전화번호가 표시되지 않으므로 지인이나 자주 통화하던 사람이 아니면 신뢰하지 않는다.

② 모르는 사람이 어려운 부탁이나 이해가 잘 안되는 이야기를 할 때는 다시 전화해달라고 하거나 전화를 나중에 할테니 전화번호를 알려 달라고 한다. (혼자인 경우)

③ 모르는 사람이 어려운 부탁이나 이해가 잘안되는 이야기를 할 때는 다른 사람에게 통화하도록 한다. (혼자가 아닌 경우) --> 역시 어려우면 ②의 방법을 취한다.

④ 114나 인터넷 검색을 통하여 발신전화번호를 확인하여 확실한 번호면 응답 전화를 하고 그렇지 않으면 사기전화로 판단한다.

⑤ 혼자인데다가 ④의 방법이 여의치 않는 사람은 대

면이나 전화 등으로 다른 사람에게 물어보고 전화 응답을 결정한다.

<휴대폰으로 받았을 경우>

① 일단 발신자가 모르는 사람인 전화는 경계하여 전화받는 것을 결정한다. 특히 발신자표시제한 전화는 절대로 받지 않는다.
② 일단 전화를 받지 말고 부재중 전화번호를 인터넷으로 검색하여 확인을 해본 후에 응답 전화를 한다.
③ 부득히 전화를 받았다면 통화를 하는데 모르는 사람이 어려운 부탁이나 이해가 잘안되는 이야기를 할때는 지금 운전중 혹은 회의중이거나 병원에 있다는 등으로 나중에 통화하자고 유도한다. 그리고 ②을 이용한다.
④ 전화 수신시에 스팸 전화번호인지를 알려주는 앱을 이용하는 것도 좋다.

아무리 급하고 사소한 일이라도 혼자서 결정하기보다는 주위 사람에게 문의를 해보는 것이 중요하다. 특히 혼자 살거나 낮에 혼자 있는 노인들이 사기에 당하기 쉽다. 노인이 전화사기에 속아 은행에서 계좌이체를 하려는 것을 은행직원이 막은 사례도 보고되고 있다. 독거노인에 대한 교육 및 홍보도 필요하고 낮에 혼자계시는 노인들에 대한 교육 등의 가족의 관심도 필요하다.

3.2 이메일 사기

이메일을 통하여 업무나 연락을 취하는 사람은 어느 정도 컴퓨터를 사용할 줄 알고 있으며 온라인 금융거래를 하기도 할 것이다. 이메일을 통한 사기는 일단 이메일 내용의 URL을 클릭하도록 하여 해킹 사이트로 접속을 유도한다. 혹은 첨부파일을 통하여 악성코드를 PC에 감염시키고 금융기관 접속시에 다른 해킹 사이트로 접속을 유도하게 된다.

바이러스 백신 프로그램을 설치하고 항상 최신으로 업데이트하며 주기적인 검사를 하는 것만으로도 충분한 예방을 할 수 있는데 좀더 실질적인 예방법은 다음과 같다.

① 발신자가 불분명하거나 제목이 유혹적이거나 자극적인 이메일은 열어보지 않고 바로 삭제한다.
② 발신자가 분명한 이메일이라 하더라도 중요한 내용인 경우에는 그 내용을 그대로 믿지 말고 인터넷 포털에서 발신자의 전화번호를 검색하여 전화통화로 확인을 한다.
③ 발신자가 분명한 이메일이라 하더라도 이메일 내용에 링크된 주소를 바로 클릭하지 말고, 인터넷 포털 등에서 해당 링크를 검색하여 접속한다.
④ 은행거래와 신용카드 사용 시에 문자 안내를 받도록 등록하는 것도 좋은 방법이다.

3.3 문자 사기

문자는 일반 휴대폰과 스마트폰의 두 가지로 구분할 수 있다. 일반 휴대폰에 수신되는 문자는 URL이 포함되지 않으며 포함되더라도 소액결제로 이어지지 않으므로 응답전화나 괜한 헛걸음을 하지 않도록 조심하면 된다. 문제는 개인정보 탈취나 소액결제가 가능한 스마트폰에 수신되는 문자이다.

① 출처가 분명, 불분명을 가리지 말고 문자에 포함된 URL을 누르지 않는다.
② URL을 반드시 확인해야 하는 경우에는 PC에서 확인하도록 하여 악성코드에 감염되어 소액결제가 이루어지지 않도록 한다.
③ 스마트폰에 정식으로 허가된 앱을 정당한 댓가를 지불하여 설치하도록 한다.
④ 긴급이나 금전을 요구하는 데 발신인이 확실한 경우에는 전화 등으로 확인한다.
⑤ 계좌이체 등의 금융거래를 해야하는 경우에는 스마트폰과 별개의 컴퓨터 기기에서 하는 것도 좋은 방법이다.
⑥ 세상에 공짜는 없다는 생각으로 '무료', '할인', '대박', '공짜' 등의 유혹성 문구가 들어 있는 문자에 현혹당하하지 않도록 특히 조심한다.

3.4 파밍 사기

파밍 사기는 URL을 변조하는 사기 공격인데 처음에는 이메일에 포함된 URL을 통하여 이루어지다가 이메일 첨부파일을 통해 이루어지더니 동영상, 음악파일,

공개 소프트웨어 등에 포함되어 오기도 한다. 최근에는 ISP 서버 해킹을 통하는 등 더욱 교묘해지고 있다.

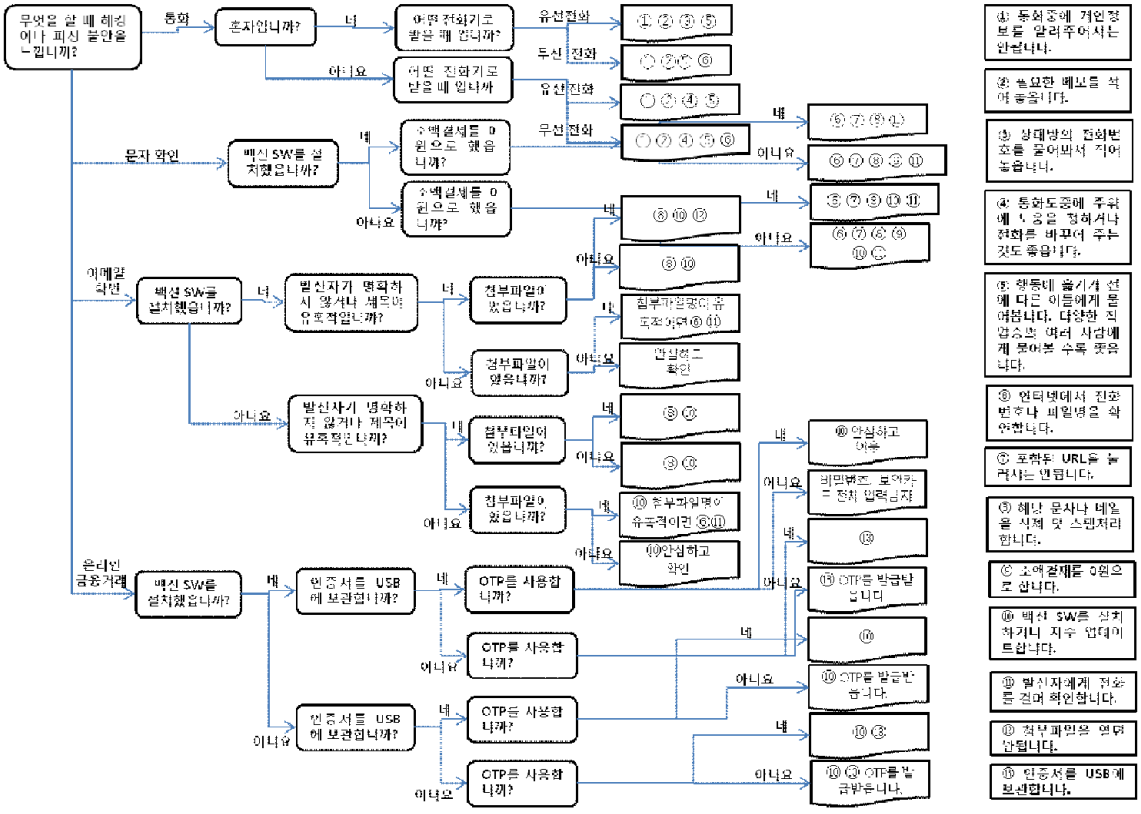
① 송신자가 불분명한 이메일의 첨부파일을 열지 않고 바로 삭제한다.
② 공개소프트웨어는 해당사의 홈페이지나 포털 사이트를 통해 다운로드 받는다.
③ 무료로 동영상, 음악파일 등을 제공하는 곳은 절대로 없으니 다운로드받으려 노력하지 않는다.
④ 인터넷뱅킹 서비스 이용 시에 OTP를 사용하도록 한다.
⑤ 계좌이체 한도(1회 한도, 1일 한도)를 가급적 작게 설정하는 것이 좋다.

그럼에도 불구하고 이러한 예방 및 대응 방법을 이해하기 어려운 사람을 위하여 <그림 2>에 유형별 피싱 사기에 대한 예방 및 대응 방법을 도식적으로 표현해 보았다. “네‘, ’아니오‘를 쫓아가면 해당하는 대응방법을 찾을 수 있다. 화살표 맨 오른쪽의 원번호들은 맨 우측에 위치한 블록들 중에서 해당하는 원번호의 조치사항을 준수 및 수행하도록 한다.

Ⅳ. 장기적인 대응책

이러한 유형별 대응책에도 불구하고 근원적이며 장기적이고 국가적인 대응 및 예방책도 필요하다.

① 앞의 기사에서도 언급되었지만 우리나라는 지나치게 한 개의 인터넷검색기만을 사용하고 있다. 익숙해져서도 그럴 수 있지만 해커들은 그럴수록 해당하는 인터넷검색기를 통한 공격을 더욱 시도하게 된다. 인터넷검색기만 바꾸어도 해킹이나 피싱 사기가 현저히 줄어들 것이다. 아울러 개발사들은 해당 인터넷검색기에 부가 서비스를 충분히 개발하여 사용자들이 부가 서비스가 충분치 않아 사용하지 않는 문제를 해결해야 한다 [8].
② 계좌이체를 신청하면 실제 은행에서 하루나 이틀 정도 후에 실제 계좌이체가 이루어지는 방법도 사기 피해를 줄일 수 있다. 이체 지연시간 동안에 해킹이나 피싱인지 여부를 파악할 수 있고 긴급조치를 취할 수 있기 때문이다. 그러나 빨리 이체되기를 기다리는 사람에게는 답답함을 줄 수도 있다. 이 방법은 어느 정도의 여론 수렴이 필요하며 은행에서의 계좌이체 처리절차의 수정을 필요로 한다.
③ 각 개인의 PC에 바이러스 백신 프로그램 설치 및 사용을 의무화하는 방법도 제기되어 있다. 기관 및 회사등의 조직에서는 이러한 방법을 이미 사용하고 있으며 매월 특정일을 “내 PC 지키미의 날”로 정하여 PC에 대한 검사를 실행하고, 백신을 업데이트하며 이 사실을 기록하여 남기기도 하고 있다. 그러나 각 가정의 PC는 그렇지 못한데 그러기 위해서는 ISP 사업자가 해당 가정의 PC들을 리모트 컨트롤할 수 있어야 하며 그에 따라 사생활 침해소지가 있어 법적으로 제정되지 못하고 있다. 결국 바이러스 백신 프로그램을 설치하거나 업데이트하지 못하는 PC들은 해킹이나 피싱 사기의 목표가 될 수밖에 없으며 나아가서는 DDOS 공격의 좀비 PC 역할까지 하게 된다.
④ 스마트폰의 소액결제는 분명히 편리한 결제 서비스임에 틀림없다. 사용자의 신용등급에 따라 최대사용금액이 월 30만원까지 상향 조정될 수 있다. 본격적인 인터넷뱅킹 서비스가 아니고 소액을 결제하기 때문에 인증서를 사용하지 않고 문자로 승인번호를 받아 입력하도록 되어 있는 서비스이다. 그러나 해커는 이 간단한 서비스의 단점을 이용하여 여러 사람에게 악성코드를 심어 결과적으로 많은 돈을 갈취하고 있다. 스마트폰의 단말기 한 대에서 승인문자 수신과 소액결제창에 입력이 이루어지고 그것도 디지털데이터를 사용하다보니 가로채기를 통하여 사용자는 알지도 못하는 사이에 쉽게 무단 소액결제가 이루어지는 것이다. 각 사업자에서 운영하고 있는 이 서비스는 현재 한도를 사용자에게 공지해야하고 한도변경도 용이하도록 해야 한다. 아울러 추가적인 확인절차를 거쳐 결제가 이루어지도록 해야 한다. 추가적인 확인절차는 첫째, 디지털데이터가 아닌 아날로그 데이터를 사용하여야 한다. 간단한 그래픽 인증 화면 등도 좋을 것으로 사료된다. 둘째, 스마트폰에서 전화통화로 승인번호를 받아 입력하는 것도 좋은 방법이다.



(그림 2) 유형별 피싱 사기 대응 및 예방 방법

⑤ 전화나 문자 수신에 발신자가 확실하지 않으면 불안하고 수신이 꺼려지기도 한다. 그러다보니 중요한 전화나 문자를 놓치거나 무시하기도 한다. 현재 발신번호를 표시해주는 앱이 개발되어 사용되고 있는 상황이다. 따라서 이러한 앱의 사용 의무화나 스마트폰 출시 시에 장착하여 판매하는 것도 좋은 방법이다.

⑥ 정부는 지난 국민은행을 비롯한 금융기관들의 고객 개인정보 대량 유출 사고 시에 그동안 선택이었던 은행거래시 확인문자서비스를 의무화시키려고 추진한 바가 있다. 그러나 각 은행들이 고객에게 모든 은행거래마다 문자를 주려면 막대한 비용이 발생하여 난색을 표시했고 일정 금액이상 거래에만 문자서비스를 제공하는 것으로 절충 중으로 알려져 있다. 어쨌거나 이러한 문자 서비스도 해킹이나 피싱 사기를 바로 파악할 수 있는 방법이기 때문에 의무적인 추진이 필요하다.

⑦ 그동안 은행사, 무선 사업자, 단말기 제조사마다 스마트폰에서 모바일 금융거래 서비스를 제공하고 있다. 그러나 그동안 금융사, 무선 사업자, 단말기 제조사별로 플랫폼이 상이해서 불편하기도 했다. 그런데 카카오톡은 메신저를 통하여 모바일 송금 서비스를 제공할 예정이다. 최대 50만원까지 충전해서 하루에 10만원까지 송금할 수 있는 서비스이다. 통일된 플랫폼에서 제공되는 서비스이기 때문에 그 파급력은 대단할 것으로 예상된다. 그에 따라 이에 대한 해킹 및 피싱사기도 급증할 것으로 우려되고 있다. 서비스 개발시에 보안상의 문제점에 대비한 기술이 철저히 준비되어야 할 것이다.

⑧ 스마트폰은 크게 아이폰과 안드로이드폰으로 구분할 수 있다. 아이폰은 앱개발시 개발자 등록 및 개발환경도 검증받도록 되어 있다. 그러나 오픈마켓을 지향하는 안드로이드 폰은 앱 개발환경은 물론 앱 개발자에 대한 확인을 거치지 않는다. 앱에 포함될

지도 모를 악성코드에 대한 법적 책임을 묻기 위해서는 적어도 앱개발자에 대한 확인이 필요하다.

V. 결 론

유선전화기만 존재하던 시대에서 급속적인 IT 기술이 발전하며 휴대폰, 스마트폰, PC, 노트북 등이 크게 상용화되고 그에 따른 인프라가 빠르게 발전하고 있다. 물론 유·무선 인터넷도 속도 및 대역폭도 크게 늘어가고 있다. 그에 따라 전화, 문자, 이메일, 악성코드, 컴퓨터 바이러스 등도 더불어 발전하며 사람을 괴롭히고 나아가서 정신적, 경제적 피해를 입히고 있다.

본 논문에서 제안한 방법과 기존의 방법들과의 차별성은 일반 고객들이 실제로 느낄 수 있는 실질적인 예방책을 본 논문에서 제안한 것이다. 또한 단기적인 대책과 장기적인 대책을 구별하여 제안함으로써 정부를 비롯한 관련 기관에서 선별적으로 장·단기적으로 구분하여 추진을 할 수 있으리라 판단한다. 아울러 <그림 2>을 통하여 컴퓨터를 비롯한 IT 기기 사용에 어려움이 있는 컴맹자라 하더라도 각 문항에 대한 질문에 '예'와 '아니오'로 따라가기만 해도 피싱에 대한 적절한 예방 방법을 찾을 수 있도록 되어 있다. 피싱에 대한 각종 보도나 사례를 듣고 막연하게 불안감을 느끼기 보다는 구체적인 분류와 그에 따른 적절하고도 실질적인 예방대책을 제시하였으며 그림을 통한 쉬운 접근을 통하여 본인에게 맞는 예방대책을 세울 수 있다.

피싱 사기는 워낙 다양하고 진화해서 단기간에 박멸하기는 어렵다. 그러나 정부의 지속적인 홍보, SNS 및 인터넷을 통한 알리기 그리고 장·단기 대책들을 마련함으로써 서서히 차단할 수 있으리라 판단한다.

참고문헌

[1] 이동휘 , 최경호, 이동춘, 김귀남, 박상민, "사회공학기법을 이용한 피싱 공격 분석 및 대응기술", 정보.보안 논문지 제6권 4호, 2006.12

[2] "보이스피싱 ," 두산백과, http://terms.naver.com/entry.nhn?docId=1348460&cid=40942&categoryId=31693.

[3] 한지선, "전화사기, 유형도 가지가지 ," 디씨인사이드뉴스, http://www.dcnews.in/news/view.html?no=22585&section=79, 2007.2.2.

[4] 정상욱, 김봉식, "국내보이스피싱(전화금융사기 현황 및 대응방안 검토 -통신분야 대책을 중심으로," 정보통신정책확회, 정보통신정책연구논문지 제24권 15호 통권 537호, pp50~69, 2012.8.16.

[5] 유재형, 이동휘, 양재수, 박상민, 김귀남, "피싱공격 차단을 위한 PSMS 설계 및 구현",정보.보안 논문지 제8권 제1호 , 2008.3

[6] "스미싱 ," 위키백과, http://ko.wikipedia.org/wiki/스미싱

[7] "파밍 ," 매일경제용어사전, http://terms.naver.com/entry.nhn?docId=19652&cid=43659&categoryId=43659.

[8] 김선애, "보안 우려하며 인터넷 사용습관 안고쳐 ," 데이터넷, http://www.datanet.co.kr/news/articleView.html?idxno=73908, 2014.8.1.

[저 자 소 개]

강 현 중 (Kang Hyun Joong)

1980년 2월 성균관대학교 학사
1986년 2월 연세대학교 석사
1996년 2월 성균관대학교 박사
1989년 3월 ~ 현재 서일대학교 인터넷정보과 교수

email : hjkang@seoil.ac.kr