정 보 보 호 학 회 지
제23권 제6호, 2013. 12

피싱 금융사기 예방을 위한 이상거래탐지 분석 방법

김 정 선*

요 약

전자금융 사기범이 전화, SMS, 이메일을 통하여 통신회사, 경찰청, 검찰청 및 금융감독당국 등을 사칭하여 피해자로 하여금 사칭기관의 위장 홈페이지로 유도하여 피해자의 금융 정보를 불법적으로 취득하여 피해자의 금융자산을 인출해나가는 금융 분야에서 발생하는 특수 사기범죄의 피해가 줄지 않고 있다. 이에 대한 대책으로 금융감독당국과 금융회사는 지연인출제도, 카드론 취급 강화, 공인인증서 재발급 및 사용절차 강화, 대포통장종합관리시스템 구축 및 홍보 강화를 하고 있지만 이들 방법은 전자금융사고 피해가 추정되는 고객뿐만 아니라 그렇지 않은 대다수 정상적인 전자금융거래 이용자에 대한 전자금융거래의 불편을 야기하고 있으며 전자금융사고 발생중의 실시간 이상증후 탐지를 반영하고 있지 않다. 본 논문에서는 금융회사 홈페이지에서의 전자금융거래 이용자의 접속행위, 공인인증서 사용행위, 온라인 송금행위 측면에서 거래행위를 분석하여 전자금융사고 혐의 이상증후에 대해 금융회사의 실시간적이고 능동적으로 대응하는 방안을 제시한다.

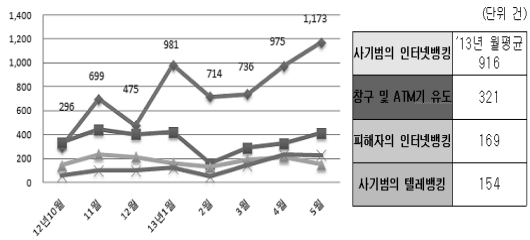
Ⅰ. 서 론

피싱(Phishing)이란 개인정보(Private Data)와 낚시(Flashing)의 합성어로 위장 홈페이지를 만든 뒤, 금융회사 홈페이지 이용자에게 금융기관, 경찰청, 검찰청, 금융감독당국, 통신회사 등으로 사칭하여 메일, 전화, SMS를 발송해 홈페이지로 접속하도록 현혹하여 신용카드 번호, 공인인증서 비밀번호, 금융회사 계좌번호, 보안카드 번호를 훔쳐 금융회사 이용자의 금융자산을 불법으로 인출해나가는 금융 사기 행위이다.

이러한 피싱 사기의 주요 경로에는 크게 보이스피싱, 피싱사이트, 파밍 등이 있으며 금융감독원에 따르면 2012년 10월 ~ 2013년 5월 기간중 발생한 11,439건의 피싱사기 중 전화를 활용하는 보이스피싱(Voice Phishing)에 의한 피해가 47.11%(5,390건)로 가장 많았고, 피싱사이트 31.4%(3,586건), 파밍 21.5%(2,463건) 순이며 특히, 최근 들어 피싱사이트, 파밍을 이용한 신▪변종 금융사기가 급증하는 등 범죄수법이 다양화▪지능화▪조직화 양상을 나타내고 있다. 또한 다음과 같이 타경로와 달리 사기범의 인터넷뱅킹에 의한 피해가 증가하고 있음을 나타낸다.

금융회사와 금융감독당국은 피싱 사기 피해예방을 위하여 300만원 이상 입금된 건에 대해 10분간 출금을 지연하는 지연인출제도('12년 6월), 카드론 취급 강화, 공인인증서 재발급 절차 등을 강화한 전자금융사기 예방서비스의 시범시행('12년 9월)과 더불어 금융감독당국은 홍보 강화를 위해 사례집 배포, 홈페이지 구축 및 단속에도 불구하고 피싱으로 인한 피해가 지속적으로 발생하고 있고 피싱사이트, 파밍 등 인터넷 기반의 고도화된 사기 수법에 의한 피해는 지속적으로 증가하고 있다.

이에 본 연구는 지속적인 제도강화, 홍보 및 단속에



〔그림 1〕 피싱사기범의 인터넷뱅킹에 의한 피해추이 및 타 경로와의 피해추이 비교

* 동양증권 IT보안팀 (ido666@hanmail.net)

도 줄어들지 않고 사회적으로 심각한 피해를 유발하고 있는 피싱사기의 피해사례를 분석하고 피싱 사기범에 의한 인터넷뱅킹의 비이상적 행위의 패턴을 도출하여 금융회사의 능동적이고 효과적인 대응방안을 제시하는 것을 목적으로 삼는다.

Ⅱ. 국내 피싱 전자금융사기 대응 현황

본 장에서는 국내 피싱 전자금융사기에 대한 금융감독당국과 금융기관의 대응 현황에 대해 설명한다.

2.1. 카드론 지연입금 제도

금융감독당국과 카드업계는 보이스피싱 피해방지 대책으로 다음과 같은 카드론 지연입금제도를 2012년 5월 17일 ~ 21일부터 시행하였다.

카드론을 최초 이용한 경우가 카드론 보이싱피싱 피해의 대부분(87%)을 차지하고 피해자의 72%가 2시간 이내에 피해 사실을 인지함에 따라 카드업계는 카드론 최초 이용자가 300만원 이상 신청한 경우 승인 후 2시간 지연입금을 하였다.

2.2. 지연인출제도

금융감독당국과 은행 등 금융회사는 공동으로 보이스피싱 피해 방지를 위해 다음과 같은 지연인출제도를 2012년 6월 26일부터 시행하였다.

정상 이체거래의 대부분(91%)이 300만원 미만인데 반해, 보이스피싱으로 인한 피해사례의 경우 총 이체건수의 84%가 300만원 이상이었다. 따라서, 300만원 이상 현금입금(송금, 이체 등)된 통장에서 자동화기기(CD/ATM기 등)를 통해 현금카드 등으로 출금할 경우 10분간 출금을 지연시키는 제도이다. 이는 피해금 인출의 75%가 10분 이내에 발생한 것에 기초한 것이며 보이스피싱 사기범이 피해금을 인출하기전에 사기범 통장에 대한 지급정지를 용이하게 하기위한 제도이다.

2.3. 전자금융사기 예방서비스

금융감독당국과 은행업계는 공인인증서 재발급 및 인터넷뱅킹을 통한 전자자금 이체시 본인 확인 절차를 강화하는 전자금융사기 예방서비스를 은행권역에 2012년 9월 25일부터 시범 시행하였다.

전자금융사기 예방서비스를 신청한 개인 고객에 대해서 ① 공인인증서를 재발급받거나(유효기간 내 갱신은 제외) 타행(기관) 발급 공인인증서를 등록하는 경우와 ② 인터넷 뱅킹을 통해 1일 누적 300만원 이상 이체하는 경우에 대해서 본인확인 절차를 강화하는 것이다. 고객은 지정된 단말기에서만 공인인증서 재발급 및 전자자금이체가 가능하며 본인확인 방법은 ① (보안카드 또는 OTP) + 휴대폰 SMS 인증, ② 2채널 인증, ③ 영업점 방문이다.

Ⅲ. 최근 피싱사기에 의한 피해현황과 피싱사기수법

3.1. 피해현황 분석

본 장에서는 2011년 12월 ~ 2013년 5월 기간중 피해금이 일부 환급된 32,996건의 피싱 전자금융사기에 대한 금융감독당국의 피해현황에 대해 설명한다.

3.1.1 피해연령대와 성비

전체 피해자 중 74.5%(11,560명)가 경제활동 계층인 30대 ~ 50대에서 발생한 반면, 60대 이상, 20대 이하 피해자도 각각 18.9%(2,943명), 6.6%(1,203명)에 달한다. 피해자의 성비는 여성이 51%(7,916명)로 남성(49%, 7,610명)과 거의 비슷한 수준으로, 우리나라의 남성 사회참여비율 58% 여성 사회참여비율 42% 등을 감안할 때 여성이 사기피해에 보다 많이 노출된 것으로 판단된다.

3.1.2 피해발생 시간대와 요일

피해자의 일과시간대이며 금융회사의 주영업시간대인 09시 ~ 16시가 68.4%(10,639명)로 피해자를 금융회사 창구·ATM기로 유인하거나 금융거래 정보를 편취하기 위해서는 동 시간대가 용이하기 때문이다. 또한, 월 ~ 금요일이 전체 피해의 93.2% (14,488명)에 달하며, 토, 일요일은 전체의 6.8%(1,063명)에 불과하다.

3.2. 피싱사기 주요 수법

본 장에서는 2012년 10월 ~ 2013년 5월 기간중 발생한 11,439건의 피싱 전자금융사기 주요 수법에 대해 설명한다.

3.2.1 피싱사기의 주요 경로

보이스피싱(피해자의 창구, ATM기 유도 등)에 의한 피해가 47.1%(5,390건)로 가장 많고, 피싱사이트 314.%(3,586건), 파밍 21.5%(2,463건) 순이다. 특히, 최근 들어 피싱사이트, 파밍을 이용한 신·변종 금융사기가 급증하는 등 범죄수법이 다양화·지능화·조직화 양상을 보이고 있다.

3.2.2 사칭기관

개인정보 편취에 의한 피싱사기의 경우 공공기관(경찰, 검찰, 우체국, 법원, 전화국, 금감원 등) 사칭이 49.5%(5,657건), 금융회사 사칭이 34.3%(3,918건) 등이었다. 이는 보안승급, 보안인증 등 공공기관 및 금융회사에서 수행하지 않은 업무를 빙자하여 피해자의 인식부족으로 손쉽게 기망이 가능하였다.

3.2.3 기망·공갈유형

보안인증 등을 가장한 금융거래정보 편취가 83.1%(9,511건)로 가장 많고, 지인사칭·협박이 15.6%(1,790건)를 차지하였다. 피해자의 74.8%(8,561건)는 개인정보유출 방지 64.6%(7,394건), 사건연루조사 10.2%(1,167건) 등을 빙자한 기망행위로 인해 금융거래정보 등을 사기범에게 편취당했다.

Ⅳ. 피싱사기범의 이상증후 행위분석과 대응방법 제안

4.1. 피싱사기범의 이상증후 행위

본 장에서는 피싱사기범이 피싱사기 피해자로부터 탈취한 개인 금융정보를 이용하여 금융회사 홈페이지 접속 이후 행위에 대해서 분석 내용을 보여준다.

4.1.1 피해자의 공인인증서 재발급

피싱사기범은 반드시 피싱사기 피해자의 공인인증서를 재발급 받는다. 이는 피싱사기범이 피해자를 피싱사이트로 유도하여 피해자의 개인 금융정보(공인인증서 비밀번호, 계좌번호, 계좌비밀번호, 보안카드번호 등)만을 탈취하였고 악성코드의 백도어를 통해 피해자의 컴퓨터에서 직접 공인인증서 폴더 자체를 복사하는 추가적인 노력이 필요 없고 기 탈취한 금융정보로 공인인증서를 충분히 재발급 받을 수 있기 때문이다.

4.1.2 금융회사 홈페이지 접속

피싱사기범은 피해자의 개인 금융정보를 탈취하고 피해자의 금융자산을 이체하기 위해 금융회사 홈페이지에 반드시 접속을 시도한다. 피싱사기범이 피해자 컴퓨터에서 직접 접속하지 않기 때문에 피싱사기 피해자의 계정으로 금융회사에 홈페이지에 접속하는 컴퓨터는 피해자가 과거에 접속한 피해자 컴퓨터의 MAC Address, IP Address와 일치하지 않는다.

4.1.3 피싱 피해자와 피싱사기범의 대포통장과의 관계

피싱사기범은 불특정 개인에게 접근하여 피싱사기를 하므로 상식적으로 피싱사기범과 피싱사기 피해자와는

〔그림 2〕 피싱사기 피해자와 거래가 없는 수취 계좌로 불법 이체된 내역

서로 아는 사이가 아니다. 그에 따라 피싱사기범과 피시사기 피해자간의 금융회사 전자금융 거래는 존재하지 않는다. 즉, 피싱사기 피해자의 송금 계좌번호 내역에는 피싱사기범의 대포통장 수취 계좌번호가 존재하지 않는다.

4.1.4 대포통장 이체금액

피싱사기범은 피해자가 피싱사기를 인지하기 전에 피싱사기 피해자로부터 탈취한 개인 금융정보를 이용하여 피해자의 금융자산을 피싱사기범의 대포통장으로 이체하는 것을 목적으로 한다. 그러한 방법으로 금융감독당국과 금융회사가 시행하는 지연인출제도를 우회하기 위해 300만원 미만 금액으로 다건을 이체한다.

4.1.5 대포통장 이체 횟수

피싱사기범은 피해자의 전체 금융자산을 피싱사기범의 대포통장으로 빠른 시간동안 이체를 하려고 한다. 하지만 300만원 지연인출제도를 피하기 위해서 300만원 미만 금액으로 이체를 한다. 따라서, 299만원 이하 금액으로 동일 대포통장 수취계좌로 2회 이상 이체를 해야지만 피해자의 금융자산을 이체할 수 있다. 즉, 동일 수취명의 대포통장으로 2회 이상 불법 이체가 발생한다.

4.2. 피싱사기 피해방지 대응방법 제안

본 장에서는 분석한 피싱사기 이상증후를 기반으로 피싱사기 피해방지를 위한 탐지 기준과 대응 방법을 제안한고자 한다.

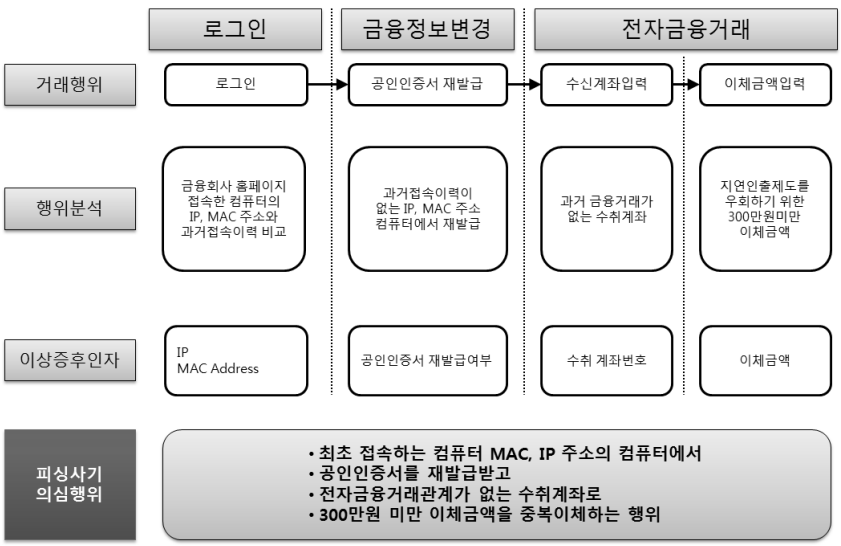
4.2.1 피싱사기 피해방지를 위한 피싱사기 의심행위 개요

금융회사에서의 금융거래는 로그인, 금융정보 변경, 전자금융거래의 3가지 단계를 거쳐 이뤄진다.

로그인 업무에서의 구체적인 행위는 컴퓨터의 IP, MAC 정보로 접속을 한다. 고객의 특별한 상황이 아니면 일반적으로 기존에 거래했던 컴퓨터에서 접속을 하게 된다. 그에 따라 금융회사에서는 고객의 IP, MAC 정보에 일관성이 존재한다.

금융거래에서는 공인인증서 인증이 필수적이다. 공인인증서의 유효기간 만료 또는 비정기적인 금융거래를 제외한 일상적인 거래에서 과거에 미접속한 IP, MAC을 가진 컴퓨터에서 공인인증서 발급/재발급을 하지 않는다.

전자금융거래에서의 마지막 단계는 수취계좌로의 이체이다. 생애 최초로 이체하는 수취계좌가 있다 하더라도 그 계좌로 300만원 미만으로 동일 수취계좌로 복수건을 이체하는 경우는 고객이 1회 이체 한도를 축소한 경우를 제외하곤 발생할 수 없다.



〔그림 3〕 피싱사기 피해방지를 위한 피싱사기 의심행위 개요

위 행위기반을 [그림 3]과 같이 도식화하였다.

4.2.2 거래행위분석 기반 이상증후탐지 순서도

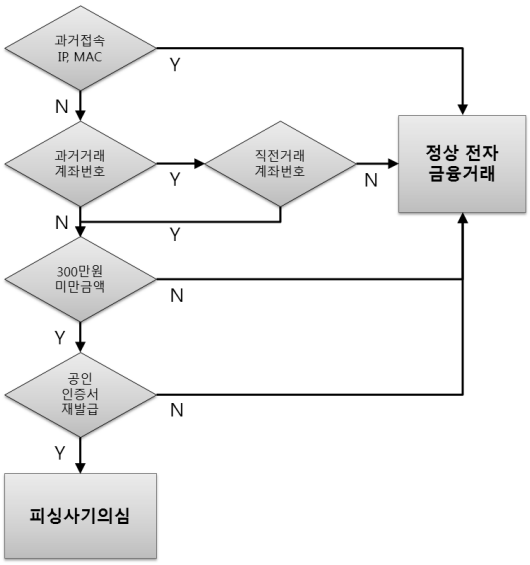
IP 주소, MAC 주소, 공인인증서 재발급 여부, 수취 계좌번호, 이체금액 등의 개별 이상증후 인자 하나만으로는 정상적인 금융회사 이용자와 피싱사기범을 판단하기는 쉽지 않다. 대다수의 정상적인 금융회사 이용자들의 불편을 최소화하면서 피싱사기범으로 의심되는 이상증후 행위를 한 거래에 대해서만 SMS 인증, 투 채널 인증 등을 해야 한다. 따라서, 아래 그림과 같은 업무 프로세스의 금융회사 대응 방법을 제안한다.

금융감독기관과 금융회사가 가이드하고 있는 안전한 금융거래를 위해 단말기 지정 서비스, 투 채널 인증 서비스, OTP(One Time Password)를 사용하는 개인 고객과 법인 고객은 [그림 4] 의 순서도에서 제외한다.

4.2.3 피싱사기 피해방지를 위한 거래행위분석 기반 이상증후탐지 방법의 설명

(step 1)

금융회사는 전자금융거래법 제22조 (전자금융거래기록의 생성 및 보존), 전자금융거래법 시행령 제12조 (거래기록의 보존기간 및 방법 등) 1항 1호 나목에 따라 전자금융거래와 관련한 전자적 장치의 접속 기록을 보존하여야 한다. 그에 따라 금융회사는 이용자의 접속 기록 보존을 위해 IP 주소, MAC 주소를 이용자별로 저장하고 있다. 피싱사기범은 피싱사기 피해자의 금융정보를 탈취하였지만 피해자의 컴퓨터에서 직접 금융회사 홈페이지를 접속할 수 없다. 금융회사는 피싱사기 피해자의 과거 접속 이력 정보를 바탕으로 기존 컴퓨터에서 접속하는지 과거 접속이력과 상이한 IP주소, MAC주소를 가진 컴퓨터에서 접속하는지 판단할 수 있다.



〔그림 4〕 피싱사기 피해방지를 위한 이상증후탐지 순서도

(step 2)

피싱사기범은 피싱사기 피해자의 금융정보를 기반으로 피해자의 금융자산을 대포통장으로 이체를 위해 수취 계좌번호를 입력한다. 피싱사기범의 수취 계좌로 사용되는 계좌번호는 수사기관의 수사를 피하기 위해 대포통장, 휴면계좌를 사용한다. 따라서 피싱사기 대포통장 계좌 소유주와 피싱사기 피해자와의 관계는 타인관계이며 설령 피싱사기 피해자의 거래관계에 있었던 상대 계좌의 소유주 이름이 같을 수 있지만 상대 계좌의 금융기관, 상대 계좌의 계좌번호 등은 같은 경우는 상당히 희박하다. 따라서, 피싱사기범이 피싱사기 피해자의 금융자산을 이체하기 위한 용도로 사용되는 수취 계좌번호는 피싱사기 피해자와 일체의 거래관계가 없었던 계좌번호이다.

(step 3)

금융감독기관과 금융회사는 2012년 6월 26일부터 지연인출제도를 시행하고 있다. 1회 300만원 이상 현금 입금(송금, 이체 등)된 통장에서 자동화기기(ATM/CD기기 등)에 출금할 경우 10분간 지연하는 제도이다. 피싱사기범은 이러한 제도를 역이용하여 피싱사기 피해자의 금융자산을 피싱사기범의 수취 계좌로 이체할 때 1회 300만원 미만 금액으로 이체 금액을 입력한다. 피싱사기범의 입장에서는 피싱사기 피해자가 피싱에 이용되었음을 인지하기 전에 피싱사기 피해자의 금융자산을 최소한의 시간으로 현금 인출할 필요성이 있기 때문이다.

(step 4)

피싱사기범은 피싱사이트를 통해서 피싱사기 피해자의 금융정보를 탈취하였지만 공인인증서 비밀번호를 안다고 해도 금융회사 홈페이지에서 피해자의 금융자산을

이체할 수 없다. 피싱사기범이 별도의 해킹을 통해서 피싱사기 피해자의 컴퓨터에서 직접 공인인증서 폴더를 복사하지 않는 한 탈취한 피싱사기 피해자의 금융정보(계좌번호, 주민번호, 보안카드번호 일체 등)를 통해 공인인증서를 재발급할 수 밖에 없다. 공인인증서를 재발급받는 컴퓨터 역시 피싱사기 피해자가 과거에 접속하지 않은 IP주소, MAC주소를 가진 컴퓨터이다.

(step 5)

피싱사기범이 피싱사이트를 통해 탈취한 금융정보로 금융회사 홈페이지에서 피싱사기 피해자의 금융자산의 규모를 인지하고 피싱사기범의 수취 계좌로 송금/이체하기 위해 1회 300만원 미만 금액으로는 피싱사기 피해자의 금융자산 전체를 송금/이체할 수 없다. 따라서 피싱사기범은 직전에 송금/이체한 피싱사기범의 수취 계좌로 중복 이체를 한다. 금융회사 이용자들이 1회 이체한도 제한 때문에 동일 계좌로 중복 이체를 하는 경우는 있지만 중복 이체건 모두 300만원 미만 금액으로 이체하는 경우는 상식적으로 하는 행위는 아니다.

Ⅴ. 제안한 거래행위분석 기반 이상증후 탐지 방법의 검증

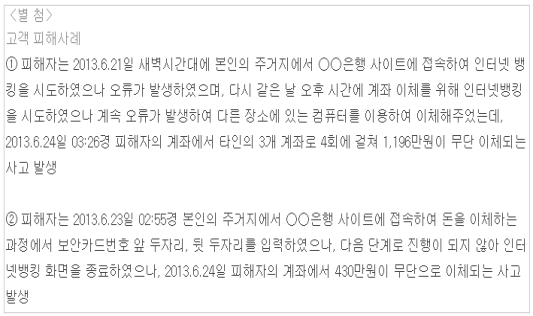
본 장에서는 언론상에서 피싱사기에 의해 피해를 입은 주요 사례를 통해 제안한 거래행위분석 기반 이상증후 탐지 방법에 대해 검증을 한다.

5.1. 정상 인터넷 뱅킹 화면에 가짜 팝업창을 띄우는 방법의 피싱사기

5.1.1 가짜 팝업창 신종 피싱사기 수법 설명

본 사건은 2013.07.02 경찰청 보도자료를 통해 알려진 신종 사기기법으로 은행의 정상적인 인터넷 뱅킹 화면에 가짜 팝업창을 띄워 고객의 계좌 비밀번호, 보안카드 난수 앞, 뒤 2자리 암호를 입력토록 하여 탈취한 다음, 이체 오류를 발생시키거나 브라우저를 종료시키는 방법으로 고객의 거래를 차단하고, 탈취한 정보를 이용하여 인터넷 뱅킹을 통해 고객의 금융자산을 편취하는 사기수법이다.

이 신종 사기수법은 전자금융감독규정 제34조 (전자금융거래 시 준수사항) 2항 6호의 '비정상적으로 거래


〈별 첨〉
고객 피해사례
① 피해자는 2013.6.21일 새벽시간대에 본인의 주거지에서 ○○은행 사이트에 접속하여 인터넷 뱅킹을 시도하였으나 오류가 발생하였으며, 다시 같은 날 오후 시간에 계좌 이체를 위해 인터넷뱅킹을 시도하였으나 계속 오류가 발생하여 다른 장소에 있는 컴퓨터를 이용하여 이체해주었는데, 2013.6.24일 03:26경 피해자의 계좌에서 타인의 3개 계좌로 4회에 걸쳐 1,196만원이 무단 이체되는 사고 발생

② 피해자는 2013.6.23일 02:55경 본인의 주거지에서 ○○은행 사이트에 접속하여 돈을 이체하는 과정에서 보안카드번호 앞 두자리, 뒷 두자리를 입력하였으나, 다음 단계로 진행이 되지 않아 인터넷뱅킹 화면을 종료하였으나, 2013.6.24일 피해자의 계좌에서 430만원이 무단으로 이체되는 사고 발생

〔그림 5〕 금융감독원 발표 : 신종 피싱사기 피해사례

를 종료하면, 다음 거래 시 동일한 비밀번호를 요구할 것'을 악용한 사기수법이다. 피싱 사기범은 악성코드에 의한 팝업창으로 탈취한 보안카드 난수 앞, 뒤 2자리 암호와 피싱사기 피해자의 금융정보로 금융회사 홈페이지에 재접속하여 탈취한 보안카드 난수의 앞, 뒤 2자리 암호를 입력하고 피싱사기범의 대포통장으로 피싱사기 피해자의 금융자산을 이체하는 사기수법이다.

5.1.2 제안한 거래행위분석 기반 이상증후 탐지 방법에 의한 분석

본 피싱사기에 대한 제안한 방법의 분석은 [그림 5] ①의 고객 피해사례와 [그림 4] 의 제안한 탐지방법의 순서도를 가지고 설명한다.

step 1 : N

피싱사기 피해자 계좌에서의 무단 이체는 피해자 컴퓨터가 아닌 피싱사기범의 컴퓨터에서 발생했으므로 피해자가 과거에 접속하지 않은 컴퓨터 IP, MAC 주소로 피해자 계정으로 금융회사 홈페이지에 접속을 한다.

step 2 : N

[그림 5] ① 피해사례를 보면 피싱사기 피해자와 관계가 없는 타인으로 이체가 되었다. 일반적으로 피싱사기에 사용되는 대포통장은 수사기관의 수사를 피하기 위해 불특정 계좌 소유주의 대포통장을 사용한다. 따라서, 피싱사기 피해자와 대포통장 소유주와의 관계는 없다.

step 3 : Y

[그림 5] ① 피해사례를 보면 4회에 걸쳐 1,196만원

이 이체가 되었다. 1회당 평균 299만원 이체가 된 것이고 이는 2012년 6월 26일부터 시행하는 300만원 이상 입금 시 자동화기기에서 10분 지연 인출해야 하는 제도를 피하기 위한 이체금액이다.

step 4 : Y

[그림 5] ① 피해사례에 공인인증서 재발급은 나오지 않으나 금융회사에서 전자금융이체할 때 공인인증서를 배제하고 이체를 할 수 없다. 악성코드에 의해 가짜 팝업창이 나타날 때 이미 피싱사기 피해자의 계좌번호, 계좌비밀번호, 공인인증서 비밀번호는 모두 탈취가 된 상태이다. 피상사기범이 공인인증서를 재발급하지 않고 악성코드에 의한 백도어를 통해 공인인증서 폴더 자체를 피싱사기범 컴퓨터에 복사하는 것을 가정가면 피싱사기범은 해킹 기술까지 보유하여야 하고 사기에 소요되는 노력은 더 많이 들것이다. 따라서 이미 금융정보를 알고 있으므로 금융회사 홈페이지에서 재발급을 통해 공인인증서를 발급받는다.

대응방법

step 4 까지의 의심행위로 금융회사는 피싱사기를 대비하기 위한 사고등록 또는 SMS 인증/투 채널 인증으로 본인확인을 할 수 있다.

5.2. 마이너스 통장 부정 인출 사건

5.2.1 마이너스 통장 부정 인출 사건 설명

본 사건은 2013.6.20 전자신문에 보도된 사건으로 마이너스 통장에서 200만원씩 수차례에 걸쳐 3500만원이 부정 인출된 사고이다. 구리시에 사는 A씨는 6월 16일 휴대폰으로 공인인증서 재발급 문자를 수신하였고 계좌조회를 했더니 수차례에 걸쳐 200만원씩 3500만원의 돈이 여러 은행의 전혀 모르는 계좌주로 분산이체가 된 사건이며 공인인증서 탈취에 의한 해킹으로 의심이 되는 사건이다.

5.2.2 제안한 거래행위분석 기반 이상증후 탐지 방법에 의한 분석

본 사고에 대한 제안한 방법의 분석은 [그림 4] 의 제안한 탐지방법의 순서도를 가지고 설명한다.

step 1 : N

피해자는 외부 이동중에 공인인증서 재발급 문자를 수신하였다. 이는 고객이 주로사용하는 컴퓨터가 아닌 컴퓨터에서 피해자 계정으로 금융회사 홈페이지에 접속해서 공인인증서를 재발급 받은 것을 의미한다. 따라서, 사기범은 피해자가 과거에 한번도 접속하지 않은 컴퓨터 IP, MAC 주소를 금융회사에 접속한 것이다.

step 2 : N

피해자는 무단 이체된 계좌번호의 소유주를 전혀 모르는 것으로 보도되었다. 따라서, 피해자와 대포 통장 소유주와 과거에 전자금융거래가 일어나지 않았음을 알 수 있다.

step 3 : Y

[그림 2] 피싱사기 피해자와 거래가 없는 수취 계좌로 불법 이체된 내역이 본 사건에서 무단 이체된 피해자의 거래내역이다. 이체된 금액을 보면 196만원, 199만원, 200만원, 205만원, 206만원 등이다. 이는 자동화기기(ATM, CD 기기 등)에서 즉시 인출할 수 있도록 2012년 6월 26일 시행한 지연인출제도 300만원 이체금액 제한을 역이용한 것이다.

step 4 : Y

앞서 사건 설명한 바와 같이 피해자는 외부 이동중에 공인인증서 재발급 문자를 수신하였다.

대응방법

step 4 까지의 의심행위로 금융회사는 피싱사기를 대비하기 위한 사고등록 또는 SMS 인증/투 채널 인증으로 본인확인을 할 수 있다.

Ⅵ. 결론

지금까지의 금융회사 이용자를 위한 피싱, 파밍, 해킹의 보호대책은 단말기 지정, 투채널 인증, OTP(One Time Password) 등을 금융회사 전체 이용자에게 강요하고 있었다. 또한 Active X 방식의 공인인증서 체계 폐지 등을 공론화하였다. 피싱사기 방지 홍보 홈페이지,

피해신고 및 피해금 환급 절차에 대해서 홍보를 하고 있지만 여전히 많은 고객들이 피싱사기로 피해를 입고 있다. 그리고 피해자 정보가 유출된 뒤 피싱사기범이 금융회사 내부에서 고객을 가장한 행위에 대해서는 대책이 없었다.

2013년 9월 26일 시행한 전자금융사기 예방서비스에서는 공인인증서 재발급 시 본인인증을 강화하여 피싱사기에 대해 효과가 있지만 보이스피싱 피해자들은 피싱사기범의 유도에 따라 본인확인용 인증번호를 불러줄 수 있기 때문에 본 논문이 제안한 방법으로 이상증후 거래 계좌에 대해서 사전 사고등록해서 불법 이체 차단을 한 후 고객과의 추가적인 확인을 통한 더욱 적극적인 고객 피해 방지에 노력해야한다.

아울러 획일적인 300만원 이상 금액의 지연 인출제도로는 피싱사기에 의한 피해 방지에 제한이 있으므로 은행, 증권, 보험, 카드회사와 금융결제원간의 거래 전문에 제안한 방법의 이상증후여부 Flag를 통해 불법 이체가 의심되는 금융회사간 이체에 대해서는 별도의 지연인출제도를 부가적으로 시행하는 것을 제안한다.

이러한 거래행위분석 기반 이상증후 탐지방법으로 금융회사 신뢰가 향상되고 금융감독당국과 금융회사의 피싱, 파밍, 해킹 방지 대책 관련된 연구에 도움이 되리라 예상된다.

참고문헌

[1] 금융감독원 보도자료. “피싱사기에 의한 피해유형 분석 및 금융거래 시 유의사항”(2013년 7월 3일 검색)

[2] 금융감독원 보도자료. “카드업계, 5.17~21일부터 카드론 지연입금 시행”(2012년 5월 15일 검색)

[3] 금융감독원 보도자료. “‘12.6.26일(화)부터 지연인출제도 시행”(2012년 6월 11일 검색)

[4] 금융감독원 보도자료. “전자금융사기 예방 서비스 시범시행”(2012년 9월 14일 검색)

[5] 전자신문 보도자료. “우리은행 마이너스 통장서 3500만원 부정 인출”(2013년 6월 20일 검색)

〈저자소개〉

김 정 선 (Kim Jung Sun)
동양증권 IT보안팀
1999년 2월 : 서울과학기술대학교 전기공학과 졸업
2013년 9월~현재 : 고려대학교 정보보호대학원 석사과정
<관심분야> 개발보안,보안경제학