Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.24, NO.6, Dec. 2014 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2014.24.6.1243

전자금융사기 예방서비스의 개선방안에 관한 연구: 2013년 전자금융사기 피해사례분석을 중심으로*

정 대 용,[1†] 이 경 복,[1] 박 태 형[2‡]
[1]고려대학교 정보보호대학원, [2]소프트웨어정책연구소

A Study on Improving the Electronic Financial Fraud Prevention Service: Focusing on an Analysis of Electronic Financial Fraud Cases in 2013*

Dae Yong Jeong,[1†] Kyung-bok Lee,[1] Tae Hyoung Park[2‡]
[1]Graduate School of Information Security, Korea University, [2]SPRi

요 약

전자금융사기의 방법이 나날이 진화하면서 금전적 피해도 함께 늘어나고 있다. 이에 따라 전자금융사기 예방서비스가 시행되고 있으나 여전히 피해가 발생되고 있는 상황이다. 본 연구는 실제 피해사례를 중심으로 전자금융사기 예방서비스의 한계를 분석하여, 그 개선방안을 제안하는 것을 목적으로 수행되었다. 예방서비스 시행 전후의 사고 사례를 분석한 결과, '스마트폰 앱 이용 사기'와 '전화 및 문자 이용 사기' 유형이 서비스 시행 이후에도 건수가 증가하였고, '스마트폰 앱 이용 사기' 유형은 피해금액도 증가한 것으로 확인되었다. 본 연구는 각 세부사례 분석을 통해 식별된 전자금융 예방서비스의 한계점을 보완하기 위해 전자금융사기 예방서비스와 유사하게 현재 시행중인 예방 관련 서비스/제도 및 기술적 인프라의 도입과 활용을 중심으로, 전자금융사기 예방서비스 자체를 개선하고, 현재 시행/논의 중인 다양한 정책을 종심방어적 관점에서 종합적으로 연계하는 방안에 대해 고찰하였다.

ABSTRACT

With the methods of electronic financial frauds becoming advanced, economic losses have greatly increased. The Electronic Financial Fraud Prevention Service(hereafter EFFPS) has taken effect to prevent electronic financial frauds, but economic losses still occurring. This paper aimed to suggest a direction for improvement of the EFFPS, through the analysis of electronic financial fraud cases. As a result of analysis on the fraud cases before and after implementation of the EFFPS, 'Fraud using Smartphone App' and 'Fraud using Calls and SMS' were increased after implementation of the EFFPS, and also the damage cost of 'Fraud using Smartphone App' had increased. Also we revealed some limitations of the EFFPS. For complementing this limitations, authors considered direction for improvement of the EFFPS focus on application of current services/systems related prevention of electronic financial fraud and considered the ways that are make connection with several measurements related prevention currently being discussed and implemented in perspective of defense in depth.

Keywords: Electronic Financial Fraud Prevention Service, Electronic Financial Fraud Case, Consumer Financial Information Security, Defence In Depth

접수일(2014년 6월 13일), 수정일(1차: 2014년 8월 29일, 2차: 2014년 10월 29일), 게재확정일(2014년 11월 6일)
* 본 논문은 미래창조과학부 및 정보통신산업진흥원의 '지식정보보안인력양성 최고정보보안전문가과정' 사업의 연구결과로 수행되었음 (과제번호 : NIPA-H2102-13-1002)
† 주저자, dyjeong75@naver.com
‡ 교신저자, mosto2004@korea.ac.kr(Corresponding author)

I. 서 론

정보통신기술의 발달로 인터넷을 통해 다양한 서비스들이 편리한 환경에서 제공되고 있다. 금융 분야에서는 전자금융거래라는 이름으로 개인용 컴퓨터와 스마트폰 등의 기기를 이용하여 언제 어디서든지 금융거래가 가능한 환경이 정착되었다. 하지만 새로운 금융환경의 위협으로 전자금융방식의 취약점을 이용하여 금전을 편취하는 새로운 범죄가 발생되고 있으며, 그 피해도 커져가고 있다. 이에 근본적인 예방을 위하여 관계당국이 대안을 논의하여[1], 전자금융사기 예방서비스(이하, 예방서비스)를 전 금융기관을 대상으로 시행하기로 결정하였고, 2013년 9월 26일부터 이를 의무화하여 시행하고 있다[2].

금융당국은 예방서비스를 통해 범죄의 예방이라는 목적을 달성할 것으로 기대하였고, 시행 이후 실제로 범죄의 발생이 어느 정도 감소한 효과를 거두었으나, 의무화 시행 이후에도 전자금융사기는 계속 발생하고 있으며 점차 새로운 범죄수법으로 진화해나가고 있다. 즉, 예방서비스가 효과를 거두었지만 이를 통해 전자금융사기의 위협이 완전히 제거된 것은 아니며, 예방서비스의 한계를 이용하여 지속적으로 공격하는 피해사례들이 계속하여 발생되고 있다.

이러한 상황에서 안전한 전자금융거래 환경을 실현하기 위해서는 그 동안 발생한 전자금융사기 사례를 면밀히 분석하여 범죄수법을 확인하고, 현재까지 연구되고 시행되어온 각종 대응방안에 대한 종합적 검토를 통해 문제점과 한계를 도출한 후, 이러한 문제점과 한계를 극복하기 위한 방안을 연구하여 이를 개선할 방향에 대하여 고민해 볼 필요성이 제기된다.

따라서 본 연구에서는 현재 시행중인 예방서비스를 고찰하고, 전자금융 사기의 유형과 피해사례를 분석하여 이를 바탕으로 예방서비스의 한계점을 파악한 뒤, 이에 대한 대응방안을 모색해보고자 한다.

II. 이론적 배경

2.1 전자금융사기 피해의 현황

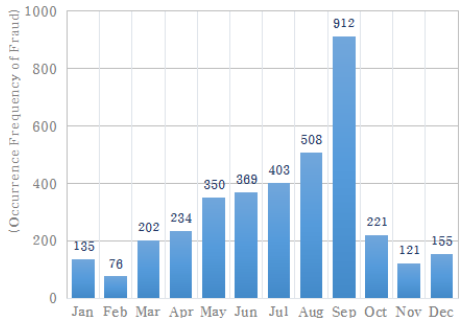
2.1.1 국내 전자금융의 현황 [3]

2013년 말 현재 국내 19개 금융기관에 등록된 인터넷뱅킹(모바일뱅킹 포함) 등록 고객 수는 9,549만 명으로 전년 말(8,643만 명) 대비 10.5%인 906만 명이 증가하여 증가세가 지속되고 있다. 또한 2013년 중 인터넷뱅킹(모바일뱅킹 포함) 일평균 기준 이용건수 및 금액은 5,429만 건, 33조 6,867억 원으로 전년대비 각각 18.7%, 1.3% 증가하였고, 특히 인터넷뱅킹의 업무처리 비중이 꾸준히 상승하면서 비대면 거래의 비중이 늘어나고 있는 추세로, 자금이체 거래 중 인터넷뱅킹의 업무처리 비중이 34.1%로 나타나고 있으며 자금의 이동이 없는 조회서비스의 경우 이용 편의성이 큰 인터넷 뱅킹이 비대면 거래의 대부분(73.8%)을 차지하고 있다. 이러한 인터넷뱅킹의 규모의 확산은 전자금융사기 등 범죄의 기반으로서 잠재적인 위협을 가져올 수 있다.

2.1.2 전자금융사기의 발생 현황[1)]

2013년 동안 대한민국에서 발생하여 경찰에 접수된 전자금융사기 피해사례는 모두 3,686건으로 피해액은 약 192억원으로 집계되었고, 건별 피해금액의 평균은 522만원으로 나타났다. 전자금융사기는 Fig.1.과 같이 2013년 1월부터 전체적으로 발생이 증가하여 2013년 9월 912건으로 최대를 기록한 후, 예방서비스가 시행된 9월 26일 이후인 10월 221건, 11월 121건 등 대폭 감소하였다.

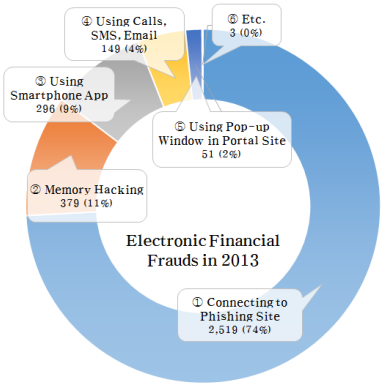
2013년 동안에 발생한 전자금융사기 사례들을 발생건수와 유형별로 분류하면, Fig.2.와 같이 ① 금융기관을 가장한 피싱사이트로 연결하는 수법, ② 메모리해킹 수법, ③ 스마트폰 앱을 이용한 수법, ④ 전



(Source: Korean National Police Agency, Rearranged by Author)

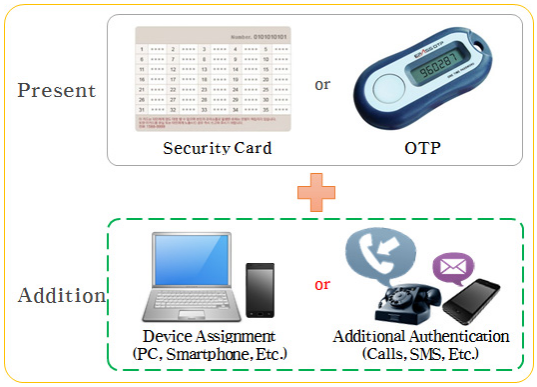
Fig. 1. Occurrence Frequency of Electronic Financial Frauds in 2013

1) 본 연구에서 분석한 전자금융사기 발생건수/피해사례는 경찰청에서 전국 경찰서에 전자금융사기로 신고 접수된 데이터를 기반으로 유형에 따라 재분류한 자료로서, 원인이 불명하거나 구체적이지 않은 사례는 유형구분 및 대응의 논의가 어려우므로 분석에서 제외하였다.



(Source: Korean National Police Agency, Reclassified by Author)

Fig. 2. Types and Occurrence Frequency of Electronic Financial Frauds in 2013



(Source: Financial Supervisory Service)

Fig. 3. Concept of the Electronic Financial Fraud Prevention Service

화·문자·메일을 이용한 수법, ⑤ 포털 등에서 팝업창을 이용하는 수법의 순서로 많이 발생하였다

2.2 전자금융사기 예방서비스[4],[5]

2.2.1 서비스 시행의 배경

2012년 금융위원회, 금융감독원, 경찰청 등 관계기관이 합동으로 수립한 『보이스피싱 피해방지 종합대책』의 일환으로 마련된 예방서비스는 사기범이 고객의 금융정보를 불법으로 획득 후 타인 명의의 공인인증서를 부정 발급받아 고객의 금융자산을 편취하는 사기 행위를 예방하기 위해 도입된 본인확인 절차를 강화하는 서비스이다.

2012년 9월 25일부터 은행권역 그리고 2013년 3월 12일부터 비은행권역에서 신청자를 대상으로 시험 시행되었으며, 2013년 9월 26일부터 모든 금융이용자를 대상으로 전면 시행하기로 결정되어, 2013년 5월 14일에 가이드라인이 전 금융기관에 배포되었고, 현재 대부분의 금융기관에서 시행되고 있다.

2.2.2 예방서비스의 개념 및 목적

예방서비스는 공인인증서 재발급이나 인터넷뱅킹 등을 통한 자금 이체 시(1일 누적 300만원이상) 본인확인 절차를 강화함으로써 전자금융사기를 예방하는 제도로, 시행 이전에는 공인인증서 재발급 및 자금 이체 시 보안카드 또는 OTP(일회용 비밀번호)등으로 본인여부를 확인하였으나, 시행 이후에는 보안카드 또는 OTP 등을 통한 본인확인 이외에 지정된 단말기를 이용하거나, 미지정 단말기에서는 추가 확인하는 절차(SMS인증, 2채널인증 등)를 의무화하여 운영되고 있다.

Fig.3.과 같이 예방서비스는 기존의 보안카드·OTP 인증방식을 보안하기 위해 추가적인 인증수단의 도입을 통해 본인확인 절차를 강화함으로써 전자금융범죄에 따른 피해를 예방하는 데 목적을 두고 있다.

2.2.3 서비스의 구성

공인인증서를 발급하거나 전자자금이체 서비스를 제공하는 은행, 증권회사, 상호저축은행, 신용협동조합 등의 금융기관들은 이용자에게 단말기 지정의 허용여부에 따라 다음과 같은 방식으로 예방서비스를 선택적으로 제공한다.

먼저, 이용자에게 단말기 지정을 허용하는 경우[2]에는 ① SMS인증, ② 2채널인증[3], ③ 영업점 방문[4] 중 한 가지 방법을 통해 이용자 본인의 단말기를 거래이용 단말기로 지정하도록 예방서비스를 제공하며, 이용자는 지정된 단말기에서 '추가 인증절차 없이' 기존 방법대로 거래를 이용할 수 있다.

이용자에게 단말기 지정을 허용하지 않는 경우에는 거래 유형에 따라, 공인인증서 재발급 또는 타행 발급 공인인증서 등록 시, 위의 세 가지 인증방법(①~③) 중 하나의 방법으로 추가적인 본인인증을

2) 예방서비스는 단말기를 PC나 스마트폰, 스마트패드 등으로 정의하며, 총 5대 이내로 제한할 것을 권고한다.
3) 인터넷뱅킹을 이용 중인 PC 외에 유선전화 등 다른 통신수단 또는 장비를 통해 인증하는 방식이다.
4) 오프라인에서 1회용 인증번호를 발급받아 인증한다.

거친 후 공인인증서를 재발급 또는 등록하게 하고, 1일 누적 300만원이상 이체 시, ①~②의 인증방법 중 하나로[5] 추가적인 본인인증을 거친 후 이체를 허용하도록 예방서비스를 제공한다.

2.3 전자금융사기 예방에 관한 선행연구

예방서비스는 2013년 9월 26일부터 시행된 제도로서 아직까지 서비스 자체에 대한 문제점을 분석하거나, 대안을 제시하는 연구는 수행되지 않았다. 본 연구는 실제 전자금융사기 피해 사례를 분석하여 현재 시행되고 있는 예방서비스의 한계를 확인하고, 개선방안을 도출하는 것에 목적을 두고 있으므로, 다소 일반적인 내용이라 하더라도 전자금융사기의 예방과 보안 강화에 관한 다양한 선행 연구를 검토해 볼 필요가 있다.

전자금융사기와 관련된 선행연구는 크게 두 가지 유형으로 분석된다. 하나는 전자금융사기를 예방하기 위해 개인·금융정보의 유출수단으로 활용되는 피싱·파밍 사이트를 차단하고 대응하는 사전 예방적 방안에 대한 연구[6][7]이며, 다른 하나는 거래과정에서 CAPTCHA[8], OTP[9], 모바일 디바이스 이용 2채널인증 등의 인증 기술에 대한 연구이다. 최근의 연구들은 휴대전화 등을 이용한 2채널인증에 대한 연구가 다수 발표되었는데, 구체적으로 SMS[10], 모바일 기기를 통해 생성된 인증정보[11], QR코드[12] 등의 연구가 주를 이루고 있다.

기존의 연구들은 대부분 몇 건의 피해사례와 인증과정에 대한 이론적인 취약점을 분석하여 강화된 인증방식을 제안하는 데 그치고 있으며, 예방서비스 시행을 통해 SMS인증 및 전화(ARS)인증 등 2채널인증 방식의 적용에도 불구하고 스미싱 등 공격수법으로 스마트폰 해킹의 위협이 증대된 현재의 상황을 충분히 반영하지 못하고 있다. 또한 강화된 인증방식을 통한 실질적 범죄발생의 감소효과와 추가된 인증방식에도 불구하고 발생되는 피해사례 및 그 보완에 대한 논의는 매우 미흡하다 할 수 있다.

이러한 측면에서 본 연구는 2013년 1년간 대한민국에서 발생한 전체 전자금융사기 피해사례를 분석하고 특히 예방서비스 시행 전후의 발생상황을 비교하는 실증적인 방법을 통하여 문제점과 한계를 도출한다는 점에서 기존 연구와 차별된다. 따라서 예방서비스라는 제도를 통하여 선행연구에서 제안한 보안강화방안이 실제 국내 모든 금융기관에서 시행되는 경우 어느 정도의 피해예방 효과가 있는지 실질적으로 확인 가능할 것으로 기대되며, 더 나아가 현재의 전자금융 보안의 문제점을 확인하고 이를 개선하기 위한 방안을 제공할 수 있을 것으로 기대한다.

III. 연구 분석의 절차

본 연구는 2013년 9월 26일 전면 시행된 예방서비스의 실효성을 확인하기 위해 먼저 예방서비스를 구성하는 구체적인 서비스 내용을 분석한다. 그리고 예방서비스 시행 전후의 전자금융 사고건수와 피해 금액 등의 분석을 통해 예방서비스 시행 이후 전자금융사기 피해유형이 어떻게 변화하였는지를 분석한다. 또한 예방서비스 시행 이후 발생된 실제 피해사례를 분석하고, 그 피해 유형을 분류하여 예방서비스가 특정 유형의 전자금융사기를 방지하지 못하는 구체적인 원인을 식별하여 예방서비스의 한계점을 파악한다. 마지막으로 앞서 도출된 예방서비스의 한계점을 보완하기 위해 예방서비스 자체의 보완과 다른 예방정책과의 연계를 통한 예방서비스의 통합 및 개선방안을 제시한다.

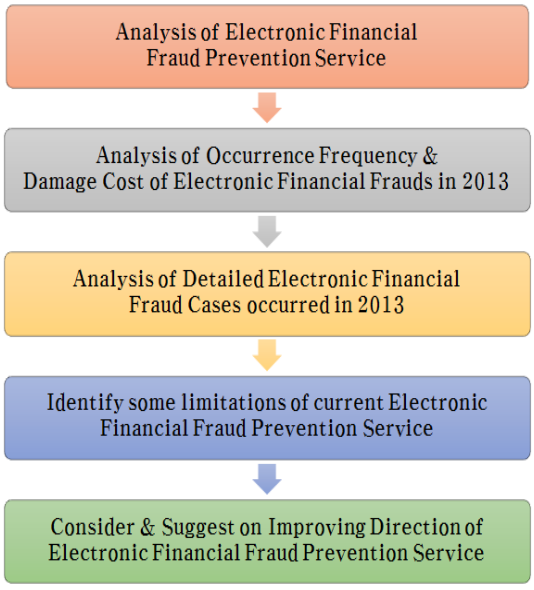


Fig. 4. Flow of Research Procedure

5) 이용자가 추가인증을 '기본'으로 설정하고, 추후 추가인증을 원하지 않는 경우, 추가인증 절차를 생략 가능하되, 이체결과를 문자메시지로 통보한다.

IV. 전자금융사기 예방 관련 서비스/제도 분석

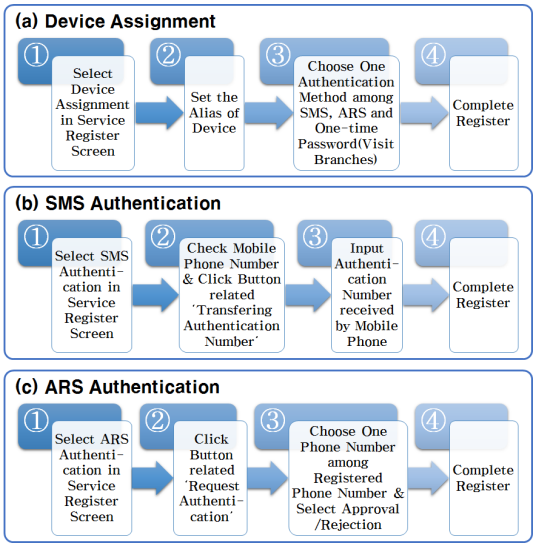
4.1 전자금융사기 예방서비스 분석

4.1.1 전자금융사기 예방서비스의 이용과정

예방서비스는 피싱·파밍 사이트 혹은 해킹을 통한 개인·금융정보의 유출을 사전에 차단하는 방법이 아닌 개인·금융정보가 유출된 상황일지라도 추가인증수단을 통해 본인여부를 확인하여 ① 본인 이외의 공인인증서 재발급 차단을 통한 피해 발생의 방지, ② 본인 이외의 300만원 이상(1일 누적)의 계좌 이체를 차단하여 피해액의 최소화하는 방법으로 피해를 예방하는 제도이다. 예방서비스는 단말기를 지정하거나, 미지정 단말기에서는 추가 인증(SMS인증, 2채널인증 등)을 의무화하여 운영하고 있으며, 각각의 인증 방법은 다음의 절차로 신청된다[2].

첫째, 단말기 지정의 인증 방법은 인터넷을 통해 단말기를 지정할 수 있으며, SMS인증이나, 2채널인증을 통하거나 영업점을 방문하여 1회용 인증번호를 발급받아 인증하는 방법 중 한 가지 방법을 통하여 신청해야 한다.

둘째, 추가인증 방법 중 SMS인증은 계좌정보에 등록되어 있는 휴대전화 번호로 SMS 인증번호를 발송하여 인증번호를 수신한 고객이 인증번호를 입력하는 방법으로 본인 인증을 하는 방법이다.



(Source: Financial Supervisory Service)

Fig. 5. Registration Procedure of Electronic Financial Fraud Prevention Service

셋째, 다른 추가인증 방법인 2채널 인증방식으로 주로 사용되는 전화(ARS)인증은 거래 시 금융회사에 등록한 전화번호로 고객에게 ARS 자동응답전화가 걸려오게 되며, 전화 통화를 통해 고객이 요청한 거래의 내역을 설명하고 거래내용이 맞는지 확인을 요청한다. 고객은 이러한 설명을 듣고 승인(1번), 거절(2번)을 누르는 등의 방식으로 인증이 이루어진다.

4.1.2 전자금융사기 예방서비스 시행에 따른 변화

4.1.2.1 서비스 시행 전후 피해건수의 비교 분석

예방서비스가 시행된 2013년 10월 이후 전자금융사기 범죄는 72.7%가 감소하였다. 구체적으로 Table. 1과 같이 피싱사이트로 연결을 유도하는 수법과 메모리해킹 수법 등 범행기법의 다수를 차지하는 유형의 발생이 대폭 감소한 반면에 스마트폰 앱을 이용한 기법과 전화·문자·메일을 이용한 기법의 경우, 각각 6.4%, 31.6% 증가한 것으로 나타났다.

4.1.2.2 서비스 시행 전후 피해규모의 비교 분석

예방서비스 시행 전후로 전자금융사기 범죄로 인한 피해금액을 분석한 결과, Table. 2와 같이 전체적인 피해 금액은 감소한 것으로 나타났다. 특히 앞에서 제시되었던 피싱사이트로 연결을 유도하는 수법과 메모리해킹, 포털 등에서 팝업창 이용 등으로 인해 발생되는 피해 규모는 감소한 반면에 동일기간 동안 스마트

Table 1. Number of Electronic Financial Fraud Before & After Regulation Enforcement

Type of Fraud	Before (Jul~Sep)	After (Oct~Dec)	Rate of Increase(%)
	(A)	(B)	(B-A)/A×100
Total	1,823	497	- 72.7
Connecting to Phishing Site	1,241	231	- 81.4
Memory Hacking	285	31	- 89.1
Using Smart-phone App	141	150	6.4
Using Calls, SMS, Email	38	50	31.6
Using Pop-up Window	34	12	- 64.7

Source: Korean National Police Agency, Reclassified by Author

Table 2. Number of Electronic Financial Fraud by Damage Cost Before & After Regulation Enforcement

Type of Fraud	Damage Cost	Before	After	Total Period
Total	≥3M	1,026	166	1,192
	<3M	1,803	399	2,202
Connecting to Phishing Site	≥3M	806	66	872
	<3M	1,434	213	1,647
Memory Hacking	≥3M	112	6	118
	<3M	216	45	261
Using Smart-phone App	≥3M	33	53	86
	<3M	92	118	210
Using Calls, SMS, Email	≥3M	63	39	102
	<3M	34	13	47
Using Pop-up Window	≥3M	12	2	14
	<3M	27	10	37

Source: Korean National Police Agency, Reclassified by Author

폰 앱을 이용한 기법의 경우 증가한 것으로 나타났다.

4.1.3 예방서비스 시행 이후의 피해사례 유형 분석

앞서 조사한 바와 같이, 예방서비스 시행 이후에도 계속해서 전자금융사기로 인한 실제 피해 사건들이 발생하고 있다. 따라서 서비스 시행 이후에 발생한 전자금융사기 피해사건의 주요 유형을 살펴보고, 각 유형별 주요 피해사례에 대한 분석을 수행하였다.

4.1.3.1 유형 1 - 스마트폰앱을 이용한 전자금융사기

사례 1-1 경기 구리시에 거주하는 피해자 A는 2013년 10월 25일 국민은행 스마트뱅킹 앱을 설치하라는 문자메시지를 받고 첨부된 URL을 클릭하여 가짜 국민은행 스마트뱅킹 앱을 설치하였다. 이후 A는 해당 앱을 실행하여 앱에서 요구하는 대로 계좌번호, 보안카드 번호 등을 입력하였고, 이후 A명의의 계좌에서 타인명의의 계좌로 6,685.893원이 이체되어 동액상당의 피해를 입었다.

사례 1-2 서울 수서구에 거주하는 피해자 B는 2013년 9월 29일 법원등기 미수령에 대한 문자메시지를 전송받아 첨부된 URL을 클릭하여, 가짜 하나은행 스마트뱅킹 앱을 설치하였다. 이후 보안강화를 위해 새로운 버전으로 업데이트하라는 메시지가 스마트폰에 현출되었고, 계좌번호와 보안카드 번호의 입력을 요구하였다. B가 이를 입력하자 이후 타인명의의 계좌로 2,470,000원이 이체되어 동액상당의 피해를 입었다.

상기 발생한 두 사례는 가짜 스마트뱅킹 앱의 설치를 이용한 전자금융사기 사례이다. 이들 피해사례의 유형은 주로 휴대폰 소액 결제 사기(스미싱)와 같은 수법으로 스마트폰에 클릭을 유도하는 문자메시지[6]를 전송하여 피해자가 링크를 클릭하면 악성코드를 다운로드하게 한 후, 이러한 악성코드를 이용하여 스마트폰에 위조된 각 금융기관의 스마트뱅킹 앱을 설치하거나, 업그레이드하게 유도한다.

설치된 가짜 스마트뱅킹 앱은 피해자에게 보안승급 등의 이유를 들어, 보안카드 번호 등 금융정보를 요구하고, 피해자가 입력한 정보를 지정된 서버나, 메일로 전송하며, 범죄자들은 이를 이용하여 피해자 계좌에서 금액을 이체하여 피해를 발생시킨다.

4.1.3.2 유형 2 - 전화, 문자를 이용한 전자금융사기

사례 2-1 서울 마포구에 거주하는 피해자 C는 2013년 10월 8일 자신의 휴대전화로 걸려온 전화에서, 불상의 피의자가 자신은 서울강남검찰청 이동철 검사이며 사건에 연루되었으니 지시에 따라야 한다는 내용의 통화를 하고, 위조된 사이트인 e-금융민원센터(122.135.119.106)에 접속하여 계좌번호와 보안카드번호 등을 입력하였다. 이후 C명의의 하나은행 계좌에서 2,800,500원이 타인명의의 계좌로 이체되어 동액상당의 피해를 입었다.

사례 2-2 서울 동대문구에 거주하는 피해자 D는 2013년 11월 8일 자신의 휴대전화로 걸려온 전화에서, 불상의 피의자가 검사를 사칭하며 불상의 인터넷 사이트(211.255.15.147)에 접속하여 금융정보 등을 입력할 것을 요청하여, 해당 사이트에 접속하고 OTP번호 등을 입력하였다. 이후 D명의의 하나은행 계좌에서 63회에 걸쳐 60,499,900원이 타인명의의 계좌로 이체되어 동액상당의 피해를 입었다.

상기 발생한 두 사례는 보이스피싱을 이용한 전자

6) 휴대폰 소액결제 사기와 마찬가지로 무료 쿠폰증정, 돌잔치·결혼식·동창회 초대 등 각종 유인 메시지로 피해자의 관심을 유도하여 첨부된 링크를 클릭하게 한다.

금융사기 사례이다. 이들 유형의 전자금융사기는 전화를 이용하여 검찰·경찰 혹은 금융기관 직원을 사칭하여 피해자에게 전화를 한 후, 금융정보가 유출되었으니 보안을 강화하여야 한다는 등의 수법으로 피해자를 속여 검찰청, 금융감독원 등 사이트를 가장한 피싱사이트에 접속하게 하거나, 문자메시지 혹은 이메일을 통해 피해자를 기망하여 피싱사이트에 접속하게 한 후, 금융정보를 가로채고, 이를 이용하여 금전을 이체하여 편취한다.

4.1.3.3 유형 3 - 메모리해킹을 이용한 전자금융사기

사례 3-1 서울 양천구에 거주하는 피해자 E는 2013년 9월 30일 계좌 이체를 위해 농협 인터넷 뱅킹 사이트에 접속하여 공인인증서 비밀번호와 OTP 번호를 입력하였다. 그러자 순간 오류가 발생하여 접속이 차단되고 잠시 후 타인명의의 신한은행 계좌로 1,990,000원이 이체되어 동액상당의 피해를 입게 되었다.

사례 3-2 경남 양산시에 거주하는 피해자 F는 2013년 9월 30일 17시 40경 자신의 사무실 컴퓨터를 이용하여 공사 식대를 이체하기 위해 농협 G명의의 계좌로 200,000원을 송금하기 위해 계좌이체를 실행하였으나, 전혀 다른 계좌인 농협 H명의의 계좌로 1,499,000이 이체 되어 동액상당의 피해를 입게 되었다.

위의 두 사례는 메모리해킹을 이용한 전자금융사기 사례이다. 메모리해킹은 특정 어플리케이션이 사용하는 컴퓨터 메모리에 대한 모니터링을 통해 특정 문자열 및 수치 변화를 추적하여 해당 데이터가 저장되는 주소를 알아내 필요할 때 그 값을 바꿔치기 하는 방법으로, 이를 이용한 전자금융사기에서는 피해자 PC에 악성코드를 사전에 설치하고 PC의 메모리를 모니터링하며, 피해자가 정상적인 전자금융 거래를 하는 동안 입력한 계좌번호, 공인인증서 비밀번호, 보안카드 번호 등의 정보를 가로채고, 오류를 발생시켜 피해자 PC 상의 거래를 중단시킨 후, 일정시간 경과 후 범죄자가 동일한 보안카드 번호 입력하여 범행계좌로 이체하거나, 메모리 상 데이터를 변경하여 범죄자가 원하는 계좌에 지정된 금액을 이체시킨다.

4.1.4 예방서비스가 작동하지 않는 원인 분석

4.1.4.1 스마트폰에 악성코드를 설치하는 공격

스마트폰 앱을 이용한 전자금융사기의 경우, 금융거래 정보를 유출하려는 목적으로 스마트폰에 가짜 스마트뱅킹 앱 등을 설치하기 때문에, 이 과정에서 스마트폰 내 정보를 유출하는 악성코드가 함께 설치될 가능성이 매우 높다. 만약 이러한 유형의 피해사례에서 정보유출 악성코드가 함께 설치된다면, 피해자가 예방서비스를 신청하였더라도 2채널인증을 위한 SMS를 탈취하여 해커에게 전송할 수 있으므로 예방서비스를 통한 전자금융사기의 예방이 불가능한 것으로 분석된다. 이는 Table. 1과 같이 예방서비스 시행 후에도 스마트폰 앱을 이용한 피해건수가 감소하지 않고 오히려 증가한 점에서 확인된다고 유추할 수 있다. 악성코드가 설치되는 경우를 보다 구체적으로 살펴보면, 다음과 같은 세 가지를 고려할 수 있다.

첫째, 스미싱 기법이나 앱마켓을 통해 스마트폰에 악성코드가 사전 설치되는 경우이다, 이 유형은 악성코드가 설치된 이후 가짜 금융 앱, 피싱사이트 등을 통해 개인정보/금융정보가 탈취되어 전자금융사기가 발생한다. 둘째, 피싱사이트를 통해 악성코드가 설치되는 경우이다. 이 유형은 피싱사이트에서 개인/금융정보를 요구하고, 보안 강화 등을 이유로 피싱 앱을 다운로드하거나 설치하게 한다. 셋째, 피싱·파밍 기법으로 피해자의 개인·금융정보를 먼저 취득한 후 이를 이용하여 보다 정교한 맞춤형 스미싱 공격 등을 통해 피해자의 스마트폰에 악성코드를 설치하는 경우이다.

이와 같은 방법으로 악성코드가 설치된 스마트폰은 피해자가 금융기관 앱을 통해 개인정보와 금융정보를 입력 시 해당 금융정보를 유출하며, 사기범은 이렇게 확보한 정보를 이용하여 금융기관에 접속한 후 SMS 인증을 신청하고, 스마트폰으로 전송되는 인증번호를 탈취하여 공인인증서 재발급과 단말기 지정과 다액이체를 함으로써, 예방서비스를 무력화할 수 있다.

4.1.4.2 전화/문자를 통해 피해자를 속이는 공격

전화/문자를 이용한 전자금융사기의 경우, 기본적으로 전화나 문자메시지를 통해 피해자를 기망하여 금융 거래에 필요한 정보를 입력하게 하거나 직접 물어보는 방식으로 탈취하는 수법을 사용한다. 따라서 피해자가 OTP 값과 보안카드 번호 등의 금융 정보 뿐

아니라, 예방서비스 이용에 요구되는 SMS 인증번호 등의 인증정보를 스스로 범죄자에게 제공할 가능성이 높다. 이 경우 본인인증 과정을 거치는 것은 기망에 빠진 피해자 자신이므로 현재의 예방서비스와 같이 사용자의 본인인증을 강화하는 방식의 예방기법만으로는 예방이 불가능한 것으로 분석된다.

이러한 사항은 Table. 1에서 나타난 바와 같이 예방서비스 시행 후에도 전화/문자메시지를 이용한 피해건수가 감소하지 않고 오히려 증가한 점에서 확인된다고 유추할 수 있다.

4.1.4.3 이체계좌번호를 변조하는 메모리해킹 공격

메모리해킹 기법은 Table. 1에서 나타난 바와 같이 예방서비스 시행 이후 피해사례가 대폭 감소한 것으로 확인되나, 사용자가 예방서비스의 단말기지정 서비스를 이용하는 경우 메모리상의 이체계좌번호를 변조하는 방식의 메모리해킹에 대하여 예방서비스의 작동구조상 대응이 어려운 것으로 분석된다.

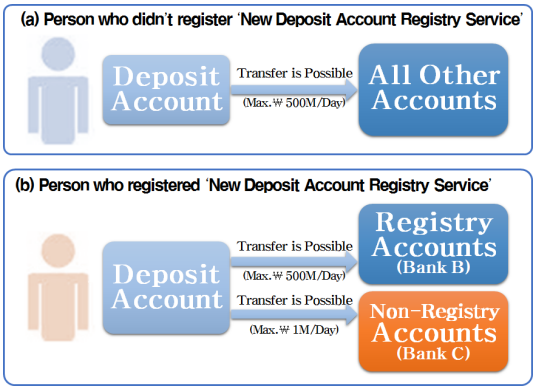
단말기지정 서비스는 최초 단말기 지정시에는 2채널 인증을 거쳐야 하나 이후 지정된 단말기에서의 거래시에는 추가인증을 거치지 않는 방식이므로 단말기지정서비스를 이용하지 않거나 미지정 PC에서의 거래시에는 ARS 등 추가인증과정에서 이체계좌번호의 변조여부를 확인할 수 있으나, 지정된 PC에서의 거래의 경우 추가인증을 거치지 않으므로 이체계좌번호의 변조여부에 대한 확인이 불가능하다.

메모리해킹의 경우 예방서비스의 시행이후 피해가 감소하였음에도 불구하고 구조적인 취약점은 계속 존재하고 있으므로 이에 대한 대응방안이 필요하다.

4.2 전자금융사기 예방을 위한 기타 서비스 분석

4.2.1 입금계좌지정 서비스

입금계좌지정 서비스는 전자금융사기 피해금이 피해자가 이체한 이력이 없는 사기이용계좌(대포계좌)로 불법 입금된다는 점에 착안하여, 고객이 사전에 등록한 입금계좌('지정계좌')로는 기존 방식대로 이체거래를 하고, 등록하지 않은 입금계좌('미지정계좌')로는 소액이체만 허용하는 제도이다. 이와 관련하여 2013년 12월 3일에 금융위원회와 금융감독원은 『신·변종 전기통신금융사기 피해방지 종합대책』의 일환으로 현재 시행되는 입금계좌지정 서비스를 보완한 新입금계



(Source: Financial Supervisory Service)

Fig. 6. New Certificate of Deposit Account Registry Service

좌지정 서비스를 2014년 9월부터 신청자를 대상으로 시행할 계획임을 발표하였다[13][14].

기존 입금계좌지정 서비스는 지정계좌로만 이체가 가능하고 미지정계좌로는 이체가 불가능하였으나, 개선된 新입금계좌지정 서비스는 지정계좌는 기존 방식대로 이체 거래를 하고, 미지정계좌는 소액 이체만(100만원 한도 내 선택적 설정) 허용하게 된다.

그러나 이 서비스는 예방서비스와는 별도로 시행되어 서비스 신청자에게도 예방서비스는 동일하게 적용된다. 新입금계좌지정 서비스에서 지정된 계좌라도 300만원이상(1일 누적) 이체 시 예방서비스 상의 추가인증을 거쳐야 하고, 계좌등록도 일일이 지정해야 하므로 이용자의 편의성을 높이기는 어렵다.

또한 서비스 신청·해지 및 계좌등록도 영업점 방문(대면신청)을 기본으로 하나 비대면 신청도 금융회사가 자체적으로 정하여 시행하도록 규제하는데, 이러한 비대면 신청에서 안전성 확보를 위한 사항으로 전화(ARS)·SMS인증과 같은 추가본인확인과 지정된 계좌 내용의 SMS문자 통보를 예시로 제시하고 있다. 하지만 이러한 비대면 채널에서의 안전성 확보 방안은 예방서비스와 마찬가지로 스마트폰에 악성코드를 설치하는 방법 등으로 인증절차를 통과할 수 있으므로 피해예방을 위해서 추가적인 보완책이 필요하다.

4.2.2 지연인출제도 & 지연이체제도

금융위원회 등 관계기관 합동 TF에서 2012년 1월 31일에 발표한 『금융소비자 보호를 위한 보이스피싱 피해방지 종합대책』의 일환으로 제시되어, 2012년 6월 26일부터 시행중인 지연인출제도는 300만원이상

현금입금(송금, 이체 등)된 통장에서 자동화기기(CD/ATM기 등)를 통해 현금카드 등으로 출금 시, 10분간 출금을 지연하는 제도이다[15].

지연인출제도는 입금계좌 기준으로 1회 300만원 이상 현금 입금된 건에 대해 카드 등으로 자동화기기에서 인출할 경우에 적용되며, 1회 300만원이상 입금된 후 이체 등으로 잔액이 변동되어도 입금된 금액을 한도로 10분간 인출을 지연하며, 이를 통해 사기범이 피해금을 인출하기 전에 지급정지를 용이하게 하여, 피해를 예방할 수 있도록 하는 예방적 조치의 일환으로 시행되고 있다.

전자금융사기에 의한 불법 자금이체의 경우에도 실시간으로 거래가 이루어져 피해자금 회수에 발생하는 한계를 해결하기 위해 제시된 지연이체제도는 금융위원회 등으로 구성된 전기통신금융사기 방지대책협의회에서 2014년 8월 13일에 발표한 『「신·변종 전기통신금융사기 피해방지 종합대책」 이행상황 점검 및 보완대책 추진』의 일환으로 제시되었으며, 현재 전자금융거래법의 개정을 통해 2015년 시행을 목표로 추진되고 있다[16].

지연이체제도는 이용자의 신청에 의해 서비스가 제공되며, 자금 이체시 일정시간 경과 후 지급효력이 발생하도록 하고, 효력발생 전까지 거래 철회를 보장함으로써, 전자금융사기로 인한 피해를 예방한다.

4.2.3 해킹사고 이용계좌 지급정지 제도

인터넷을 통한 금융거래 시 발생한 해킹사고 피해 신고가 크게 증가하는 가운데, 현재의 해킹사고 이용계좌(대포통장)의 지급정지 제도가 피싱, 대출사기 등 여타 금융사기에 비해 제한적(해킹사고에 직접 이용된 은행권 계좌의 피해금액에 한정)으로 운영되고 있어, 피해금의 타계좌 이전(이전계좌) 및 피해금 인출의 억제를 통한 피해자 보호가 곤란함에 따라, 금융감독원에서는 이에 대한 대책으로 해킹사고 이용계좌에 대한 지급정지의 강화 계획을 발표하였다[17].

강화된 해킹사고 이용계좌 지급정지 제도는 해킹피해 확산을 방지하기 위해 제도의 적용을 여타 금융사기 수준으로 확대한다. 구체적으로 강화된 해킹사고 이용계좌 지급정지 제도는 제도 적용 대상을 확대하여, 현재 조치중인 은행권역 이외에 인터넷뱅킹 서비스를 제공하는 증권사, 저축은행, 상호금융조합 및 우체국, 새마을금고 등 타 금융권도 적용대상으로 규정한다. 그리고 지급정지 대상 계좌와 금액을 확대하여, 사고에 직접이용(1차계좌)된 계좌잔액 중 피해금액 범위 내에서만 지급정지하는 현재의 규제를, 1차계좌 잔액전부의 지급정지와 이전계좌의 이전금액 내 지급정지로 확대하며, 추가 피해발생 방지 등을 위해 1차 피해계좌에 대한 입금정지를 실시하도록 한다. 또한 해킹 사고 관련 대포통장 명의의 타 계좌에 대해서도 '비대면채널 인출거래'를 제한한다.

4.2.4 추가 피해방지를 위한 제도 - 비대면인출제한 제도 및 개인정보노출자 사고 예방시스템

앞서 살펴본 전자금융사기의 예방과 관련하여 추가적으로 금융감독원은 보이스피싱의 대응과 관련된 주요제도로 '비대면인출제한제도'와 '개인정보노출자 사고 예방시스템'을 보이스피싱 예방 웹페이지(phishing-keeper.fss.or.kr)에서 제시하고 있다.

비대면인출제한제도는 피싱사기 이용계좌 명의인의 추가피해를 방지하기 위해 피해자의 지급정지요청이 있는 사기이용계좌 명의인의 정보를 교환하여 사기에 이용되지 않은 다른 계좌에 대한 자동화기기, 인터넷뱅킹, 텔레뱅킹, 모바일뱅킹 등 비대면 거래를 제한하는 제도로서, 추가피해를 막기 위한 제도로 시행되고 있다.

개인정보노출자 사고예방시스템은 주민등록증, 운전면허 분실 등 개인정보를 노출한 금융소비자가 대출사기 등의 금융 사고를 우려하여 금융회사로부터 보호를 받고자 할 때, 금융회사 한 곳에 개인정보 노출사실을 신고 시 타 금융회사도 동시에 공유하도록 하는 시스템이다. 이와 같은 제도는 개인정보가 유출되거나 사기 피해가 발생된 경우 추가 피해를 방지하기 위한 예방효과를 얻을 수 있다.

4.3 소결 : 전자금융사기 예방 관련 서비스/제도의 한계

4.3.1 전자금융사기 예방서비스의 한계

4.3.1.1 예방서비스의 내용 분석을 통해 식별된 한계

예방서비스는 지정 단말기를 등록하는 경우, 공인인증서를 재발급·등록하는 경우, 그리고 300만원이상을 계좌이체 하는 경우 모두 인증절차에서 SMS인증과 전화(ARS)를 이용한 2채널 인증방식을 선택적으로 허용하고 있으므로 이러한 인증방식 중 하나를 공

격하여 통과하거나, 우회할 수 있다면 모든 금융거래가 가능하게 된다.

구체적으로 공격자가 공인인증서를 사전에 탈취한 경우에는 ① 즉시 300만원 미만 이체 ② 추가인증을 통과하여 전액 이체 ③ 추가인증을 통과하여 단말기 지정 후 전액 이체가 가능하며, 공인인증서를 탈취하지 못한 경우라도 추가인증을 통과하여 공인인증서 재발급을 받은 후 같은 방식으로 이체가 가능하므로 공격자가 원하는 계좌에 이체가능금액 전액을 이체할 수 있게 되어 피해를 예방할 수 없게 된다.

또한 단말기 지정 서비스를 이용하는 경우에도 한 번의 인증으로 지정된 단말기에서는 추가인증 없이 편리하고 신속한 거래가 가능하나, 지정되지 않은 단말기나 해당 서비스를 이용하지 않는 경우에도 추가인증을 거치면 모든 거래가 가능하므로 추가적인 예방효과는 기대하기 어렵다.

앞서 분석한 바와 같이, 실제 전자금융사기 피해는 예방서비스 시행 이후 대폭 감소한 것으로 확인되나, 완전히 근절되지 않고 지속적으로 발생하고 있으며, 이는 피해를 예방하기 위한 방법으로 추가인증에만 초점을 두고 있어 추가인증을 우회하거나 통과하는 방식의 공격에 취약하다는 예방서비스의 근본적인 한계로 인한 것으로 분석된다.

4.3.1.2 금융사기 피해사례 분석을 통해 확인된 예방서비스의 한계

예방서비스 시행 전후의 피해건수와 피해금액을 비교 분석한 결과, 예방서비스의 시행 이후 전체적인 사건 발생 건수가 감소하였고, 특히 범죄의 대부분을 차지하는 금융기관을 가장한 피싱사이트로 연결하여 금융정보를 탈취하는 수법과 메모리해킹 수법 및 포털 등의 팝업창을 이용한 수법의 경우 피해 감소가 뚜렷하게 나타나고 있다는 것을 알 수 있다.

그러나 예방서비스의 시행 이후 발생이 증가한 사례를 기준으로 예방서비스의 한계점을 고찰하면,

첫째, 사례 1-1, 1-2와 같은 가짜 스마트폰 앱을 통한 전자금융사기의 경우, 피해자의 스마트폰은 범죄에 활용 가능한 악성코드가 이미 설치되었을 가능성이 높기 때문에, 예방서비스의 SMS인증이나 전화(ARS)를 통한 추가인증 방식만으로는 전자금융사기의 예방이 불가능하다. 특히 악성 앱을 통해 휴대폰의 인증번호를 탈취하여 소액결제를 처리한 사례[18]나, 유출된 개인정보를 이용하여 다른 휴대전화로 착신전환을 신청하여 인증번호를 탈취한 사례[19]와 같이, 인증정보를 그대로 유출하거나, 착신전환을 통해 피해자의 전화/문자를 대신 받게 된다면, 인증절차를 우회적으로 통과할 수 있어 피해 발생이 가능하다는 것을 확인할 수 있다.

둘째, 사례 2-1, 2-2와 같이 전화나 문자, 메일을 이용하여 피해자를 금융기관을 가장한 피싱사이트로 유도하는 전자금융사기 유형의 경우, 피해자로부터 공인인증서 비밀번호와 ARS 인증번호 혹은 OTP 번호를 입력하게 하거나[7], 직접 전화로 알아내어 범행에 이용하므로 예방서비스를 통한 피해 예방이 불가능하다.

셋째, 사례 3-1, 3-2의 메모리해킹에 의한 금융사기의 경우, 추가적 방법으로 SMS문자·전화(ARS)인증을 통과할 수 없다면 300만원이상의 다액을 이체하기는 어려우나, 300만원 이하의 이체는 충분히 가능하다. 또한 악성코드가 설치된 PC가 지정된 단말기가 아닌 경우 추가 인증과정에서 거래정보의 변경을 확인하여 300만원이상의 거래를 차단할 수 있으나, 다만 지정된 단말기인 경우 300만원이상의 피해를 막을 수 없어, 단말기 지정 서비스를 이용하는 경우 더욱 위험하다 할 수 있다.

즉, 예방서비스의 시행에도 불구하고, 피해 감소 효과가 전혀 없거나 부분적인 효과만이 나타나는 유형을 중심으로 피해사례를 분석한 결과, 스마트폰에 가짜 금융 앱과 스미싱 악성코드를 설치/이용한 경우와 착신전환을 통해 전화나 SMS를 대신 받는 경우, 전화통화를 통해 피해자를 완전히 속이는 경우 그리고 단말기 지정된 PC를 통한 이체로 추가인증이 생략되는 경우에 메모리해킹 공격을 받는 경우 등은 현재의 예방서비스로 차단이 불가능한 한계점이 존재한다.

4.3.2 예방 관련 서비스/제도의 분산으로 인한 한계

앞서 분석한 바와 같이, 예방서비스 외에도 전자금융사기 예방/방지/대응을 위해, 입금계좌지정 서비스, 지연인출제도, 해킹사고 이용계좌 지급정지 제도 등과 같은 다양한 서비스와 제도가 이미 존재한다.

이들 서비스의 목적을 개별적으로 살펴보면, 전자금융사기 프로세스 별로 전자금융사기 예방서비스는 본인인증절차를 강화하여 타인의 이체 승인을 방지하는 목적이며, 입금계좌 지정서비스는 이체 대상 계좌

7) 예방서비스 가이드라인에서는 OTP를 이용하는 경우 2채널인증을 선택사항으로 규정하고 있다.

를 지정하여 원치 않는 계좌로의 이체를 방지위한 목적이라 할 수 있고, 지연인출제도는 범행계좌로의 이체 후 지급정지를 위한 시간을 확보하기 위한 제도이며, 지급정지제도는 이체된 계좌에서의 출금을 방지하여 피해금액을 회복하는데 목적을 두고 있다고 볼 수 있다. 즉, 이들 서비스는 세부적으로는 조금씩 다르지만, 거시적 관점에서는 모두 전자금융사기 예방을 위한 목적을 가지고 도입되어, 전자금융사기 대응에 있어 각각 중요한 역할을 담당하고 있다.

하지만 따라서 이러한 전자금융사기의 예방을 위한 서비스 및 제도들은 서비스의 제공과 이용에 있어 연계나 통합이 이뤄지고 있지 않다. 예방서비스와 입금계좌 지정서비스는 각각 별도로 신청을 통해 제공되고 있으며, 이체 후 피해금 확보와 피해회복을 위한 지연인출제도나 지급정지제도와의 연계성도 명확하게 발표되지 않은 채로 시행되고 있다.

지난 2013년 12월 3일 금융위원회 등 관계기관에서 합동 발표한『신·변종 전기통신금융사기 피해방지 종합대책』에서는 입금계좌지정 및 계좌지급정지등에 대한 예방법은 포함하고 있으나, 전자금융사기 예방서비스와 지연인출제도 및 비대면인출제한제도 등에 대해서는 다뤄지고 있지 않았으며[13], 지난 8월 12일 발표된『「신·변종 전기통신금융사기 피해방지 종합대책」이행상황 점검 및 보완대책 추진』에서도 예방서비스와의 연계 등에 대한 내용을 다루고 있지 않은[16] 점을 볼 때, 전자금융사기의 예방을 위한 서비스/제도에 대하여 통합적 관점의 논의가 부족하다는 것을 확인할 수 있다.

전자금융사기가 다양한 유형으로 발생하고 있고, 사기가 발생하는 금융 제도의 취약점이나 기타 원인이 매우 다양함을 고려할 때, 예방의 측면에서 보다 체계적인 대응이 이뤄질 필요가 있으며, 이를 위해서는 현재 분산되어 있는 전자금융사기 예방 관련 서비스/제도가 하나의 서비스/제도 하에 통합적으로 구성되어야, 예방의 관점에서 서로 다른 서비스가 상호 보완되어 보다 안전한 금융 환경이 마련될 수 있을 것이다.

또한 전자금융사기 예방이 소비자 관점에서 매우 중요함을 감안한다면, 현재와 같이 개별적으로 분산되어 시행되고 있는 예방 서비스/제도는 서비스를 이용하거나 제공받는 소비자의 입장에서 인식하기 어려울 뿐 아니라, 편의성도 저해될 가능성이 높다. 특히 소비자들이 전자금융사기 피해 예방을 위한 제도들이 어떠한 것이 있는지 확인하기 어렵다는 사실은 단순히 인식의 문제를 넘어, 소비자들이 인지한 서비스만을 신청하게 하여 전자금융사기 대응의 사각지대에 위치할 위험성을 내포한다.

V. 전자금융사기 예방서비스 개선의 고려사항

5.1 금융 보안 강화를 위한 예방서비스의 개선 방향

앞서 수행된 분석을 통해, 현재 규정된 전자금융 예방서비스로는 날이 갈수록 진화하는 금융사기 수법들에 대응하는 데 한계가 있는 것을 확인할 수 있다.

이러한 상황에 적절히 대응하기 위해서는 현재 제공되고 있는 예방서비스를 강화하고, 예방서비스의 한계를 보완하기 위한 다양한 제도적(서비스)·기술적(인프라) 관점이 통합되어 전자금융사기의 예방을 체계적으로 접근해야한다. 또한 이를 지원하기 위한 법제도를 정비할 필요가 있다.

5.2 현행 예방서비스의 강화

현재 시행되고 있는 예방서비스의 취약점은 4.3.1에서 식별한 바와 같이, 착신전환이나 피싱 등으로 인증 수단 자체를 우회하거나, 단말기 지정서비스를 이용하더라도 미지정 기기에서 추가인증을 하면 거래가 가능하여, 예방서비스가 무력화된다는 점이다. 따라서 기본적으로 현재의 전자금융사기 예방서비스의 강화를 위해 상기 언급된 취약점을 개선해야 한다.

이를 위해 기본적으로 전화(ARS)인증 및 SMS인증을 제한적으로 허용하거나 차단하는 방안을 고려할 수 있고, 단말기 지정 서비스를 보완하거나 폐지하는 방안을 고려할 수 있다. 또한 피싱 등에 의해 피해자가 완벽히 속임을 당한 경우 피해발생에 대한 사후적 조치사항으로 지연인출제도 및 지급정지제도를 통한 피해회복의 관점과 홍보와 교육 등을 별도의 추가적인 대응방안으로 고려할 필요가 있다.

본 절에서는 현재 제공되고 있는 예방서비스의 내용, 즉 인증 방식과 단말기 지정 서비스에 초점을 두고 예방서비스 강화를 위해 각 요소가 어떠한 방향으로 개선되어야 하는지를 검토하도록 한다.

5.2.1 예방서비스 내 인증방식의 개선

먼저, 앞서 분석된 예방서비스의 문제점을 보완하기 위해서는 예방서비스의 인증방식을 강화해야 할 필요가 있다. 현재 예방서비스의 인증방식인 SMS인증

과 전화(ARS)인증에 대한 개선방안을 고찰하면 다음과 같다.

5.2.1.1 전화(ARS)인증의 제한적 허용 검토

현 예방서비스 내 전화(ARS)인증은 착신전환을 통하여 사기범이 전화를 대신 받는 경우와 스마트폰 등이 해킹 또는 악성코드에 감염되어 전화가 도청되는 경우 위험이 발생할 수 있다.

먼저 착신전환을 이용한 경우는 예방서비스에서 기본적으로 착신전환이 신청된 전화번호에 대하여 전화인증을 허용하지 않도록 규정함으로써 예방이 가능하다. 단, 착신전환이 반드시 필요한 경우를 감안하여, 착신전환 대상 전화번호가 같은 명의자인 경우 등에 한하여 전화(ARS)인증을 제한적으로 허용하거나, 착신전환 전화 허용에 대해 사용자가 신청하는 등의 방안을 함께 고려해야한다.

그리고 스마트폰이 해킹 또는 악성코드에 감염되는 경우, 통화내용이 실시간으로 도청된 사례와 스마트폰을 원격으로 조작하거나, ARS에 자동으로 응답하도록 악성코드가 동작할 수 있기 때문에, 스마트폰에 전화(ARS)인증을 차단하는 방안을 기본적으로 검토할 필요가 있다. 최근의 070번대 번호를 사용하는 인터넷전화도 스마트폰 운영체제를 그대로 사용하는 경우가 존재하므로 인터넷전화도 전화(ARS)인증 차단을 검토할 필요가 있다. 이에 비해 유선전화(02, 031 등 지역번호 사용)나 피쳐폰의 경우는 악성코드를 포함하여 추가적인 프로그램이 설치되지 않아 해킹으로부터 안전하므로 이에 한하여 전화(ARS)인증을 허용하는 방안을 고려할 수 있다.

현재 대부분의 휴대전화 사용자가 스마트폰을 사용하며, 등록된 전화번호만으로는 피쳐폰과 스마트폰을 구분할 수 없어 휴대전화 중 스마트폰을 선별적으로 차단하기 어렵고, 피쳐폰의 비율이 점점 낮아지는 추세를 감안한다면, 휴대전화와 인터넷전화에 대해 전화(ARS)인증을 차단하고, 유선전화의 경우만 허용하는 식으로 제한적인 전화(ARS)인증 방식을 고려할 필요가 있다.

즉, 착신전환과 휴대전화에 대해서 전화(ARS)인증의 제한적 허용을 검토하는 방향으로 전화(ARS)인증의 개선을 고찰할 필요가 있다.

5.2.1.2 SMS인증에 대한 재검토

SMS인증의 경우에도 스마트폰에 악성코드가 설치되는 경우 안전하지 않은 것으로 보고되고 있으며, 전화(ARS)인증과 같은 문제점이 발생할 수 있는 가능성이 높기 때문에 SMS인증은 예방서비스에서 인증을 위한 수단으로 사용할 것인가 자체를 검토해야할 필요가 있다.

먼저, SMS인증을 예방서비스에서 제외하는 방안을 고려하면, 앞의 전화(ARS)인증의 제한적 사용으로 유선전화만이 인증의 방안으로 사용될 수 있다. 하지만 정보통신정책연구원에서 발표한 유무선전화서비스 이용현황에 따르면 유선전화가 없는 가정의 비율이 2013년 32.63%로 2012년 20.74%에서 12% 가량 증가하는 추세[20]로 유선전화를 사용하지 않는 인터넷뱅킹 고객은 가정에서 금융서비스를 이용할 수 없다는 한계가 있어 금융소비자의 편리성에서 문제가 제기되므로, SMS인증을 제외하는 경우 다른 인증수단을 추가하는 대안이 필요할 상황에 놓이게 된다.

반면 그대로 SMS인증을 예방서비스에서 본인인증의 추가 수단으로 사용하게 하는 방안을 고려하면, 앞서 식별된 인증 우회를 예방하기 위해서는 결국 부가적인 인증수단이 추가적으로 요구된다. 즉, 현재의 예방서비스에서는 SMS인증을 제외하던 그대로 사용하던 간에 인증우회를 방지하기 위해서는 추가적인 인증이 요구되므로, SMS인증을 제외하고 대신 사용할 인증방식을 검토하는 것이 보다 바람직한 개선의 방향이라 할 수 있다.

5.2.1.3 전화(ARS)·SMS의 인증방식에 대한 개선방안

따라서 현 예방서비스의 전화(ARS)인증 방식은 착신전환의 제한적 허용 및 전화(ARS) 승인방식의 고도화를 전제로 유선전화와 휴대전화 모두 유지하는 방안을 채택하고 이와 함께, SMS인증 대신 선택적으로 활용하거나 보완할 수 있는 추가적인 인증방식을 검토하여, 도입함으로써 예방서비스를 강화해야 해야 한다.

예를 들면 휴대전화에 대한 전화(ARS)인증 시, 착신전환 차단을 의무화하고, 인증방식을 단순히 승인(1번), 거절(2번)을 입력하는 방식이 아닌 사용자가 알고 있는 정보 중 매번 다른 번호(4자리)를 요구하는 방식 등으로 고도화를 한다면 ARS에 자동으로 대응하거나, 실시간으로 전화내용을 도청하면서 스마트폰

을 원격 조작하는 방식의 수법 등을 차단할 수 있을 것이다.

SMS인증을 대체할 수 있는 추가적인 인증 수단으로 거래연동 OTP 등의 사용을 고려할 필요가 있다. 이와 관련된 내용은 5.4.1에서 다루도록 한다.

5.2.2 단말기 지정 서비스의 개선

예방서비스에서 단말기 지정 서비스는 서비스 대상 거래에 대해 매번 인증과정을 거쳐야하는 불편함을 해소하기 위한 서비스라 볼 수 있으며, 지정 서비스를 이용한다고 하더라도 예방효과가 강화되는 것은 아니기 때문에 이에 대한 폐지·보완·대체의 상황을 분석하고, 이에 대한 분석결과 및 개선방향을 제시하고자 한다.

첫째, 단말기 지정 서비스의 폐지와 관련하여 단말기 지정 서비스를 폐지하고 적용대상 거래에 대하여 매번 추가인증을 받는 방안을 제시할 수 있다. 예방효과는 동일하거나 앞서 제시되었던 사례 3-1과 3-2의 경우 300만원이상 다액 이체 차단의 효과로 예방효과는 더 높아진다 할 수 있으나, 이용자의 선택을 제한하고 300만원이상 다액 이체를 자주하는 이용자의 경우 상당한 불편함이 예상되는 점이 문제점으로 제기된다.

둘째, 단말기 지정 서비스의 보완과 관련하여 단말기 지정 서비스의 내용을 일부 변경하여 예방효과를 높이고 불편함을 최소화하는 방안을 제시할 수 있다. 인터넷뱅킹 이용 시 문제가 되는 경우는 다액 이체시므로 지정된 단말기에서 공인인증서 재발급을 받는 경우 추가인증절차 없이 이용하고 ① 300만원이상 이체 시 추가 인증을 받는 방안, ② 일정금액(예: 1000만원이상) 이체 시에만 추가인증을 받는 방안 등을 고려할 수 있다. ①의 경우 다액이체를 자주하는 이용자의 불편이 거의 감소되지 않으며, ②의 경우 일정금액 이하의 피해는 계속 발생할 우려는 있으나, 그이상의 금액에 대하여는 예방효과가 있으며, 매번 인증과정을 거치는 불편은 상당히 감소될 것으로 예상된다. 하지만 ②와 같이 특정 금액을 기준으로 제한하는 방식은, 해당 금액 이하의 피해는 예방이 불가능하기 때문에 근본적인 대책이라 할 수 없으므로 추가적인 제도와의 연계 등을 통해 단말기지정서비스 자체에 대한 보완 혹은 대체가 필요하다.

5.3 상호보완적 관점에서의 유사 서비스/제도와의 연계성 구축 - 종심방어 전략

4.2와 4.3.2.에서 고찰한 바와 같이 현재 전자금융사기를 예방하기 위해 예방서비스 외 여러 가지 제도가 분산되어 개별적으로 시행되고 있다. 따라서 이들 제도 및 서비스를 전자금융의 프로세스에 따라 본인인증, 계좌인증 등 단계별로 분류하여 각각의 중첩적인 예방 절차로 분류하여 체계화할 필요가 있다.

본 논문에서는 이를 구체화하기 위하여 전자금융사기 예방을 위한 종심방어전략의 개념을 적용하고자 한다. 종심방어란 얇은 방어선을 여러 겹으로 깔아서 적의 공격을 둔화시키고 소모시키는 과정을 통해 전선을 유지하는 고전적인 군사전략으로서 네트워크 보안 등 다양한 분야에서 활용되고 있다.

현재 전자금융사기의 예방을 목적으로 개별적으로 시행되는 제도와 서비스를 하나의 종심방어전략으로 구성하여 전자금융사기 공격에 대응하여 각 단계별로 보안을 강화하고 이를 연계하여 종합적인 보안수준을 향상하고자 하며, 이를 도식으로 표시하면 Fig.7.과 같다. 각 단계 별 세부적인 구성은 다음과 같다.

5.3.1 본인 인증 단계

본인인증단계에서는 현재의 예방서비스가 적용되어, 예방서비스의 핵심인 본인인증 강화를 중심으로 전자금융사기를 예방한다. 5.2에서 제안한 바와 같이 현재 예방서비스에서 이용하는 인증방식을 고도화하여 이를 통해 사기 피해를 우선적으로 예방한다.

5.3.2 계좌 인증 단계

전자금융사기에 있어 공격자의 목적은 자신들이 확보한 계좌(대포통장)로 피해금을 이체시키는 것이다. 따라서 본 단계에서는 新입금계좌 지정서비스를 통해 이체실행 전 계좌를 인증하는 단계를 추가하여 만일 공격자가 본인인증과정을 통과/우회한다 하더라도 계좌인증 단계에서 원치 않는 계좌의 이체를 차단하여 피해를 예방한다. 또한 본 단계에서는 기술적 수단으로 거래연동 OTP를 적용할 수 있다.

5.3.3 계좌 이체 실행 단계

이체 실행 단계에서는 자금 이체시 일정시간 경과

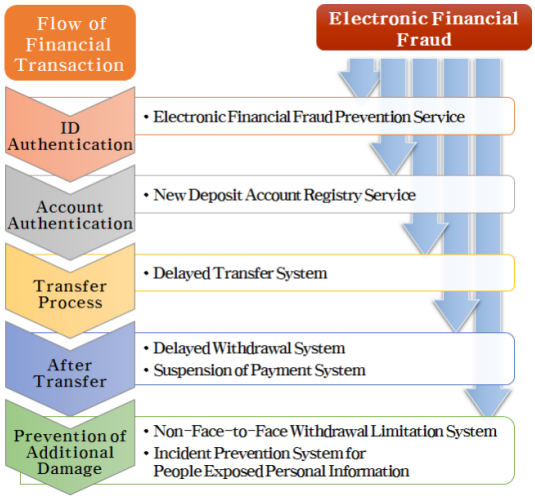


Fig. 7. Defence In Depth Prevention to Electronic Financial Fraud in terms of Service/System Integration & Flow of Electronic Financial Transaction

후 지급효력이 발생하도록 하고, 효력발생 전까지 거래 철회를 보장하는 제도인 지연이체제도를 적용한다. 이를 통해 공격자가 본인인증과 계좌인증 절차를 통과/우회하여 이체를 실행한다 하더라도 일정시간이 지날 때까지는 피해자금의 지급효력이 발생하지 않으므로 이를 철회할 수 있다.

지연이체제도의 안전성을 확보하기 위해서는 이체 실행과정 및 완료 즉시 사용자에게 단말기 및 전화 등으로 이체내역을 다시 확인할 수 있도록 하는 조치가 병행되어야 한다.

5.3.4 계좌 이체 이후 - 추가피해 방지 예방조치 단계

사기범이 상기 예방수단을 모두 통과/우회하여 계좌이체까지 성공한 경우에는 지연인출제도를 통해 피해금의 즉시 인출을 차단하여 지급정지를 위한 시간을 확보하고, 강화된 해킹사고 이용계좌 지급정지 제도를 통해 범행에 이용된 계좌의 지급을 정지하여 피해금을 확보하고 피해회복을 보장한다.

전자금융사기 공격에 대한 시도가 있거나, 이체가 성공한 경우 해당 사용자에 대한 개인정보와 금융정보는 대부분 노출된 것으로 볼 수 있으므로 1차적인 피해를 차단한다 하더라도 추가 피해 발생의 우려가 높다고 할 수 있다.

이에 대하여 개인정보노출자 사고 예방시스템을 통해 본인확인절차를 강화하여 추가피해를 방지하고, 사기이용계좌 명의인의 정보를 통한 추가 공격을 예방하기 위해 비대면인출제한제도를 통해 계좌 명의인의 정보를 교환하여 사기에 이용되지 않은 다른 계좌에 대한 거래를 제한하여 추가 피해를 예방할 수 있다.

5.3.5 소결 : 예방 수단의 연계와 통합 관리 구현방안

이와 같이 현재 개별 시행되고 있는 예방 관련 제도를 인증부터 추가 피해방지 단계까지 하나의 절차로 통합하여 각 단계별로 예방수준을 강화한다면, 전자금융사기 공격이 각 단계를 통과/우회한다 하더라도 다음 단계에서 공격을 차단하여 전체적인 예방 수준을 향상시킬 수 있다. 이러한 통합적 예방 전략을 구현하기 위해서는 구체적으로 다음을 고찰할 필요가 있다.

첫째, 무엇보다도 전자금융사기 예방에 대한 통합된 금융정책이 필요하다. 즉, 금융감독기관에서 현재와 같이 개별적인 정책으로 시행되는 예방을 위한 서비스를 통합적 관점으로 논의하여 연계되고 통합된 하나의 서비스로 구축하여 시행할 필요가 있다.

둘째, 서비스에 대한 접근성을 강화하여야 한다. 현재 적용되는 다양한 예방 서비스의 경우 개별적 홍보와 각각 별도의 신청절차를 거쳐야 하나, 사용자의 편의성을 고려하여 본인인증 방식과 계좌인증 방식 및 지연이체제도의 알림방법 등록 등의 절차를 하나의 신청으로 통합 관리할 필요가 있다.

셋째, 사용자별 맞춤형 예방서비스로의 전환이 필요하다. 개별 사용자의 본인인증 단계 및 계좌인증 단계의 보안수준을 평가하여 등급화하고 이를 통해 각자의 보안수준에 따라 추가인증방법을 적용하거나, 1일 혹은 1회 이체한도를 제한하거나, 지연이체 및 지연인출 금액과 시간을 조정하여, 강화된 보안서비스의 사용을 유도할 수 있다. 그리고 특정 단계에 편중되거나, 보안강화의 효과 없이 중복된 절차를 생략하여 보안성과 편의성을 종합적으로 고려된 예방이 가능할 것이다.

5.4 예방서비스 지원을 위한 금융보안 인프라의 연계

전자금융사기 예방을 위해서는 앞서 기술한 예방정책적 제도 및 관리적 서비스의 고려 뿐 아니라 금융보안을 실제로 구현하는 기술적 측면의 인프라와 긴밀하게 연계되어야 예방의 강화가 이뤄질 수 있다.

이에 본 논문에서는 예방서비스를 지원하기 위한 금융보안 기술 인프라를 고려함에 있어 소비자 단

(front-end)과 금융기관(back-end)으로 구분하여, 각각 거래연동 OTP의 도입과 이상금융거래탐지시스템(FDS)의 연계를 고찰하도록 한다. 이러한 전반적인 금융보안 인프라의 지원은 종단에서의 예방서비스를 지원할 뿐 아니라, 균형적인 보안시스템을 구축하는데 기여할 수 있을 것이다.

5.4.1 소비자 단에서의 금융보안 인프라 - 거래연동 OTP의 도입

본 논문은 5.2.1에서 고찰한 현행 인증방식의 개선에서 SMS인증의 대체 또는 보완을 위해 예방서비스에 추가 도입을 고려할 수 있는 인증방식으로 거래연동 OTP를 제시한다. 거래연동 OTP는 사용자가 PC에 입력한 계좌번호와 결제금액 등의 거래정보와 연동된 OTP를 생성하여, 전자금융 서버에서 이를 확인하고 거래정보가 변경된 경우 이를 거부한다.

거래연동 OTP는 표준 SSL/TLS의 이용과 웹 표준을 준수하여 서비스를 제공하기 때문에 표준 브라우저 및 대부분의 플랫폼에서 별도의 프로그램 없이 동작하고 별도의 리더기 없이 OTP 발생기만으로 거래서명 값을 발생할 수 있다는 특징을 가지며[21], 이를 통해 비록 OTP 값이 유출되거나 메모리 해킹을 통해 이체계좌번호가 변경된다 하더라도 OTP 값을 생성할 때 입력한 계좌가 아닌 다른 계좌로의 이체를 차단할 수 있다는 장점을 가지고 있다.

다만 사용자 편의성 측면에서 매번 계좌번호를 입력하여야 하므로 많은 조작이 필요하다는 단점이 있다. 하지만 ① OTP 사용으로 추가 인증절차를 생략하는 경우[8], 시간동기화 OTP는 탈취한 OTP값을 1분 이내 입력하여 계좌 이체가 가능하고, 단말기 지정된 PC에서 메모리해킹이 발생한 경우 예방이 불가능하다. 이에 반해 거래연동 OTP는 이러한 피해를 모두 예방할 수 있어, 편의성은 약간 저하되지만 보안성이 향상된다. ② 보안카드 사용으로 추가인증절차를 거치는 경우에도 추가적인 인증과정(전화(ARS)·SMS)을 거쳐야하지만, 거래연동 OTP 사용 시 추가 인증절차 생략할 수 있어 한 번의 거래연동 OTP 입력으로 보안성이 향상되고 편의성도 저하되지 않으므로, 예방서비스에 도입하여 적용하기에 적합하다.

8) 인터넷뱅킹을 통한 이체 시 추가적인 본인인증절차는 금융회사별 선택사항이다.

5.4.2 금융기관의 예방서비스 지원 - 이상금융거래 탐지시스템과의 연계

2013년 7월 10일 금융위원회와 금융감독원에서 발표한 『금융전산 보안 강화 종합대책』에서는 카드사 위주로 운영 중인 이상금융거래 탐지시스템(Fraud Detection System)을 은행·증권 등으로 확대 구축하고, 이상금융거래 정보를 전 금융권과 공유체계를 구축할 것을 권고하였다[22]. 하지만 2014년에 들어 금융위원회에서 은행 17곳을 조사한 결과 3곳의 은행만이 이상금융거래 탐지시스템을 구축하였고, 10개 은행이 2014년도 내 시스템을 구축하겠다고 보고하는 등, 권고에 따른 시스템의 구축이 제대로 이행되고 있지 않아, 2014년 상반기 중 은행과 증권사를 대상으로 시스템 구축 행정지도를 나설 것을 밝혔다[23]. 금융감독원도 은행장 회의에서 고객정보 유출사고에 대한 대책으로 이상금융거래 탐지시스템의 조속한 도입을 요구하였고[24], 이러한 움직임에 따라 금융감독원과 금융위원회는 2014년 6월 제정·발표한 『금융회사 정보기술(IT)부문 보호업무 이행지침』에서 금융회사에게 이상금융거래 탐지시스템을 구축, 운영할 것을 명시함으로써[25] 은행을 비롯한 금융기관 전체에 이상금융거래 탐지시스템의 구축이 급격히 추진되고 있다.

이러한 이상금융거래 탐지시스템은 사고가 발생한 이후에 대응하는 사후적 조치이지만, 부정한 거래를 차단한다는 점에서 전자금융사기 예방의 관점에서 함께 다뤄질 필요가 있다. 또한 이상금융거래 탐지시스템은 전자금융 전체에 걸쳐 정보 등이 유기적으로 연결·공유되고, 이를 통해 부정거래의 의심/탐지/차단 등이 신속하게 이뤄져야 그 효과성이 높아질 수 있는 특성을 가진다. 이러한 점을 고려할 때 현재 각 금융기관에서 구축·운영되고 있는 이상금융거래 탐지시스템은 예방서비스를 지원하는 금융 보안의 기술적 기반으로써 예방서비스와 상호 연계될 필요가 있다.

즉, 금융기관 단에서 각 금융기관의 이상금융거래 탐지시스템 상 이상금융거래의 의심/탐지/차단의 기능과 이에 대한 통고 등이 예방서비스에서 제공하는 본인인증이나, 거래내역의 통보 등과 상호 보완적으로 연계되어, 예방서비스를 지원할 수 있어야 한다.

5.5 관련 법제도 보완을 통한 예방서비스의 간접 개선

앞에서 분석한 전자금융사기 사례 현황과 예방서비

스의 한계에서 스마트폰을 이용하는 경우에 특히 취약하고, 여러 가지 문제점을 내포한 것으로 나타났다. 이는 현재 제공되는 예방서비스의 경우에는 제공범위가 한정적이라는 근본적인 문제점을 가지고 있다. 그렇기 때문에 기본적으로 현재 운영되고 있는 금융보안 규제의 보완을 통해 예방서비스를 간접적으로 보완하는 것이 필요하다. 특히 전자금융사기의 발생 원인을 파악하여 이러한 원인들을 제도/서비스나 기술적 측면이 아닌 법제도적/정책적 차원에서 접근하여 금융보안 관련 법규를 종합적으로 개선하여 전자금융사기들을 사전에 예방하는 것이 선결되어야 할 것이다.

특히 5.3에서 제시하는 전자금융사기 대응을 위한 사전 예방적 관점의 유사 서비스를 통합하고, 5.4에서 제시하는 금융보안 인프라를 예방서비스와 연계하기 위해서는 이들과 관련된 현재의 다양한 정책을 검토하고, 법제도적 근거에 따라야 할 것이기에 더욱 관련 법제도의 보완이 요구된다고 할 수 있다.

VI. 결 론

본 연구에서는 2013년 한 해 동안 경찰에 신고 접수된 모든 전자금융사기 피해사례를 조사하여 시기별·유형별 등으로 분류하고 발생 원인을 분석하여 2013년 9월 26일부터 모든 금융기관에서 의무시행 중인 예방서비스의 한계와 문제점을 시행 이전과 이후로 나누어 분석하였다. 그 결과, 예방서비스의 시행 이후 전체 발생건수는 감소하였으나, 완전히 근절되지는 못하였고 오히려 발생건수가 증가한 유형도 나타났다.

원인을 분석한 결과, ① 스마트폰에 악성코드가 설치되는 경우, ② 착신전환 서비스를 이용하는 경우, ③ 전화를 통하여 피해자를 완벽하게 속이는 경우, ④ 단말기 지정서비스 이용 시 메모리해킹의 경우에는 예방효과를 보장하기 어렵다는 것을 발견하였다. 또한 현재 전자금융사기 예방을 위한 제도들은 예방서비스 외에도 전자금융사기 예방/방지/대응을 위해, 입금계좌지정 서비스, 지연인출제도, 해킹사고 이용계좌 지급정지 제도 등과 같은 다양한 서비스와 제도가 이미 존재하고 있으나, 통합적 관점의 논의가 부족하여 보안강화 및 사용자 편의성을 보장하기 어렵다는 점을 확인하였다.

이에 대한 대응방안으로 전화(ARS)방식은 보안성을 강화하여 유지하고 문제가 되는 SMS인증방식은 폐지하는 방식을 선택하고 발전된 인증방식인 거래연동 OTP와 입금계좌 지정서비스를 일부 수정하여 적용하는 방식으로 전자금융사기 예방서비스를 개선하고, 종심방어 개념을 도입하여 전자금융사기 예방을 위한 다양한 제도들을 통합/연계하고 이를 지원하기 위한 기술적 인프라로서, 거래연동 OTP 기술과 이상금융거래탐지시스템과의 연계를 제안하였다.

전자금융사기는 결국 사기범이 확보한 범행계좌로 피해금액을 이체한 후 이를 현금화시키는 것을 목적으로 하는 범죄로서, 대부분의 경우 본인인증절차를 통과/우회한 후 피해금을 이체하고 이를 인출하는 방식을 사용하고 있다. 따라서 본인인증 방식을 강화하고 입금계좌를 인증하여 범행계좌로의 이체를 차단하고, 이미 이체가 실행된 경우 지급효력과 인출을 지연시키고 지급정지를 통해 피해금을 동결시키는 등 단계별 보안강화방안을 연계하여 실행한다면 범죄피해를 상당부분 차단할 수 있을 것이다.

이는 본 연구에서 제시한 거래연동 OTP의 도입을 통해 본인인증과 계좌인증을 동시에 진행하거나, 입금계좌를 직접 확인하고 인증한 후 거래를 진행하는 입금계좌지정방식을 통한 예방서비스의 강화와 종심방어적 예방서비스의 연계가 대안이 될 수 있을 것이다.

이러한 개선안은 현재의 금융시스템을 크게 변경하지 않고 이용이 가능하며, 추가적인 비용 부담도 많이 발생시키지 않으면서 현재의 전자금융사기 예방서비스에 비해 예방효과는 더욱 높으며, 이용자의 편의성도 크게 저하시키지 않는 방식이라고 판단된다. 또한 사용자단의 거래연동 OTP 기술과 이상금융거래탐지시스템을 통한 기술적 지원과 금융보안 규제의 보안과 같은 정책적 차원의 접근을 통해 더욱 효과를 높일 수 있을 것이다.

본 연구에서는 실제 피해사례를 중심으로 문제점을 분석하는 사례연구 기법으로 서술하였다. 그러나 대부분의 피해사례들은 실제 피해자의 입장에서 확보된 진술을 재구성한 것으로 실제 사기범들이 각각의 범죄수법에 대하여 어떤 방법으로 인증과정을 통과하거나 우회하였는지에 대하여 구체적으로 기술하기 어렵다는 한계를 가진다.

또한 다양한 피해사례들의 전체적인 발생경향과 유형별 공격기법 등을 분석하여 그에 대한 대응방안과 개선된 예방서비스를 분석하는데 중점을 두었기에 각각의 공격기법에 대한 기술적 분석은 이루어지지 못하였다는 한계점을 가지고 있다. 이러한 한계점을 보완하기 위하여 절차적인 분석을 통하여 효과를 검토하는 방법을 활용하였다.

본 연구에서는 2013년 발생한 모든 전자금융사기

피해사례에 대한 전체적인 경향과 유형별 피해사례 분석은 향후 금융보안 강화를 위한 추가연구의 기초자료로서 의미 있는 역할을 할 것이라 기대되며, 제시된 개선방안 역시 직접적인 적용이 어려운 경우라 할지라도 또 다른 개선방안을 찾는 데 도움이 될 것이라고 기대한다.

2013년 말을 기준으로 19개 금융기관에 등록된 인터넷뱅킹 등록 고객 수는 이미 9,500만 명을 넘어선 것으로 보고되었다. 이는 중복 고객을 감안하더라도 경제활동 인구의 대다수가 인터넷뱅킹을 이용한다고 볼 수 있다. 이렇게 거대한 규모의 전자금융 시스템에 있어서 거래의 안전과 원활한 거래의 이용은 시스템 전체의 운명을 좌우하는 매우 중대한 문제이다. 따라서 새롭게 도입되는 금융보안 정책은 이론적 검토뿐만 아니라 충분한 기간의 시범서비스와 다양한 상황을 가정하고 안전성과 가용성 등을 반복적으로 검증한 후 시행되어야 하며, 이와 함께 이용자의 시각에서 접근해야 할 것이다.

References

[1] FSC(Financial Services Commission) and FSS(Financial Supervisory Service), "「Electronic Financial Fraud Prevention Service」 Test Operation - Enforcement of Identification Procedure on Replacement of Certificate and Electronic Transaction," Press Release, Sep. 14, 2012.

[2] FSC and FSS, "「Electronic Financial Fraud Prevention Service」 Fully Enforcement," Press Release, Sep. 25, 2013.

[3] The Bank of Korea, "Internet Banking Services 2013," Press Release, Feb. 10, 2014.

[4] FSC and FSS, "「Electronic Financial Fraud Prevention Service」 Announcement of Fully Enforcement," Press Release, Sep. 16, 2013.

[5] FSC and FSS, "Distribution of 「Guideline to Fully Enforcement of Electronic Financial Fraud Prevention Service」," Press Release, May 14, 2013.

[6] Joon ho Sa and Sangjin Lee, "Real-time Phishing Site Detection Method," Journal of The Korea Institute of Information Security & Cryptology, 22(4), pp. 819-825, Aug. 2012.

[7] Ki-Hong Park, Jun-Hwan Lee and Han-Jin Cho, "Countermeasure against Social Technologic Attack using Privacy Input-Detection," The Journal of the Korea Contents Association, 12(5), pp. 32-39, May 2012.

[8] Sang-ho Lee, Sung-ho Kim, Jeon-il Kang, Je-sung Byun, Dea-hun Nyang and Kyung-hee Lee, "A Method of Enhancing Security of Internet Banking Service using Contents- Based CAPTCHA," Journal of The Korea Institute of Information Security & Cryptology, 23(4), pp. 571-583, Aug. 2013.

[9] Jonghoon Lee, Minho Park and Souhwan Jung, "OTP-Based Transaction Verification Protocol Using PUFs," The Journal of the Korean Institute of Communication Science B, 38(6), pp. 492-500, June 2013.

[10] T. Venkat Narayana Rao and Vedavathi. K, "Authentication Using Mobile Phone as a Security Token," International Journal of Computer Science Engineering and Technology, vol. 1, no. 9, pp. 569-574, Oct. 2011.

[11] Han-na You, Jae-Sik Lee, Jung-Jae Kim, Jae-Pio Park and Moon-Seog Jun, "A Study on the Two-channel Authentication Method which Provides Two-way Authentication using Mobile Certificate in the Internet Banking Environment," The Journal of the Korean Institute of Communication Science B, 36(8), pp. 939-946, Aug. 2011.

[12] Ben Dodson, Debangsu Sengupta, Dan Boneh and Monica S. Lam, "Secure, Consumer-Friendly Web Authentication and Payments with a Phone," Mobile

Computing, Applications, and Services, LNICST(Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering) 76, pp. 17-38, 2012.

〔13〕 FSC and FSS, "Comprehensive Measures to Prevent the New and Variety Form Telecommunications Financial Fraud," Press Release, Dec. 3, 2013.

〔14〕 FSC and FSS, "Distribution of Guideline for New Certificate of Deposit Account Registry Service," Press Release, Mar. 6, 2014.

〔15〕 FSC, Korea Communication Commission, KNPA(Korean National Police Agency), FSS, Korea Federation of Banks and The Credit Finance Association, "Comprehensive Measures to Prevent Voice Phishing Damage for Financial Consumer Protection," Press Release, Jan. 31, 2012.

〔16〕 FSC, MSIP(Ministry of Science, ICT and Future Planning), Ministry of Justice, KNPA, Korea Coast Guard and FSS, "Inspection on Implementing the 「Comprehensive Measures to Prevent the New and Variety Form Telecommunications Financial Fraud」," Press Release, Aug. 13, 2014.

〔17〕 FSS, "Enforcement on Suspension of Payment to Hacking Incident Account," Press Release, July 24, 2014.

〔18〕 KNPA Cyber Bureau, "Arrest A Suspect in Smartphone Billing Fraud(Smishing)," Important Incident, June 21, 2014.

〔19〕 Daegu Metropolitan Police Agency, "Arrest of A Smishing Criminal Organization under the mask of First Birthday Invitations," Press Release, Jan. 21, 2014.

〔20〕 Jihyung Shin, "Status of wired and wireless phone service," KISDI STAT Report 14-05, KISDI(Korea Information Society Development Institute), pp. 1-2, May 2014.

〔21〕 Financial Security Agency, "Research Report on the New Authentication Technologies for Electronic Financial Transaction", Research Report 2011-01, Financial Security Agency, pp. 38-48, Mar. 2011.

〔22〕 FSC and FSS, "Comprehensive Countermeasures to Enforce Online Security of Banks," Press Release, July 11, 2013.

〔23〕 Hansol Kim, "Only Three Banks built Fraud Detection System," The Kyunghyang Shinmun, Apr. 15, 2014. http://bizn.khan.co.kr/khan_art_view.html?artid=201404152124315

〔24〕 FSS, "A Meeting with Heads of Local Banks for Demanding a Reinforcement of Internal Supervision," Press Release, Apr. 15, 2014.

〔25〕 FSC and FSS, "Implementation Guideline for Finance companies' Protection Service in Information technology Sector," Press Release, June 2014.

〈저자소개〉

정 대 용 (Dae Yong Jeong) 정회원
1998년 2월: 경찰대학 법학과 학사 졸업
2010년 2월~현재: 충북지방경찰청 사이버범죄수사대장
2013년 9월~현재: 고려대학교 정보보호대학원 석사과정
〈관심분야〉 정보보호 정책 및 제도, 사이버범죄 예방, 컴퓨터 포렌식

이 경 복 (Kyungbok Lee) 학생회원
2008년 2월: 고려대학교 공과대학 산업시스템정보공학과 학사 졸업
2009년 3월~2010년 2월: 고려대학교 정보경영공학전문대학원 정보경영공학과(정보보호전공) 석사 졸업
2010년 3월~현재: 고려대학교 정보보호대학원 정보보호학과 박사 수료
〈관심분야〉 정보보호정책, 개인정보보호, 융합보안, 소셜네트워크분석

박 태 형 (Tae Hyoung Park) 정회원
2002년 2월: 고려대학교 서양사학과 학사 졸업
2004년 2월: 고려대학교 일반대학원 행정학과 석사 졸업
2004년 4월~2008년 4월: 한국행정연구원 연구원
2011년 2월: 고려대학교 정보보호대학원 박사 졸업
2011년 3월~2014년 11월: 고려대학교 정보보호연구원 연구교수
현재: 소프트웨어정책연구소 선임연구원
〈관심분야〉 정보보호정책, 성과평가, 사이버국방, 방위사업