Journal of Digital Convergence
Vol. 16. No. 7, pp. 9-17, 2018

ISSN 1738-1916
https://doi.org/10.14400/JDC.2018.16.7.009

전자금융사기의 사회공학적 진화: FGI를 통한 실제 피해자 분석

박종필[1*], 류재관[2]
[1]경남대학교 경영정보학과, [2]성균관대학교 일반대학원 경영학과

Social Engineering Evaluation of Electronic Financial Fraud: Analysis of Actual Victims through FGI

Jong-Pil Park[1*], Jae Kwan Ryu[2]
[1]Management Information Systems, School of Business, Kyungnam University
[2]Business Administration, SKK Business School, Sungkyunkwan University

요 약 최근 전자금융사기에 대한 관심이 증가되고 있다. 특히, 전자금융사기는 사회공학적 양상으로 진화하고 있다. 이러한 높은 관심에도 불구하고 전자금융사기를 방지하기 위한 적절한 가이드라인은 거의 없는 실정이다. 더군다나, 실제피해자들을 대상으로 관련 연구가 거의 이루어지지 않고 있다. 본 연구의 목적은 실제 피해자들을 대상으로 왜 전자금융사기가 발생하는지에 대한 근원적 접근을 시도하고자 한다. 보다 실제적인 현실세계를 반영하기 위해, 본 연구에서는 피해자들을 대상으로 초점면접기법(FGI)을 활용해 분석하였다. 분석결과, 전자금융사기를 당하는 데에는 일정한 피해패턴이 있음을 발견할 수 있었다. 또한 왜 전자금융사기가 발생하는지에 대한 근본적인 물음에 대한 해답은 행동경제학에 바탕으로 둔 인간의 낙관적 편향이라는 심리적 인지오류로 인해 피해가 발생함을 확인할 수 있었다. 이 연구의 수행을 통해 위기관리 관점으로 향후 전자금융사기를 방지하기 위한 의미 있는 가이드라인과 방향성을 제공하며, 궁극적으로는 정부 및 산업계의 효과적 정책을 개발하기 위한 중요한 기초자료로서 활용되기를 기대한다.

주제어 : 전자금융사기, 사회공학, 보이스피싱, 랜섬웨어, 포커스그룹인터뷰

Abstract Recently, much attention in electronic financial fraud has been dramatically increased. In particular, the electronic financial fraud has been transforming to social engineering. Despite the growing interest in electronic financial fraud, few guidelines exist how to effectively avoid the serious damage from electronic financial fraud. Moreover, it is rarely investigated cases of victims from financial fraud. Therefore, the purpose of this study is to investigate why financial fraud crime victims occurs. To enhance mundane realism, we conducted Focus Group Interview(FGI) with actual victims from financial fraud crime. Drawing analysis of FGI with actual victims, we found that there are certain damage patterns. Further, we found that the reason why financial fraud crime victims occurs is optimistic biases of humans rooted in behavioral economics. Therefore, this study provides the valuable guidelines and directions to prevent electronic financial fraud based on risk and crisis management perspective. Ultimately, this study is able to help the establishment and implementation of a comprehensive electronic financial fraud prevention policy.

Key Words : Electronic Financial Fraud, Social Engineering, Voice Phishing, Ransomeware, FGI(Focus Group Interview)

*Corresponding Author: Jongpil Park(jpark@uok.ac.kr)
Received February 6, 2018
Revised May 18, 2018
Accepted July 20, 2018
Published July 28, 2018

1. 서론

정보통신기술(ICT)의 발달은 인간의 경제활동에 직접적인 편리함을 제공했지만, 역설적으로 이러한 용이성과 편리함이 금융사기라는 부작용을 낳고 있다. 금융사기는 금융거래에서 속임수를 통해 사기범이 금전적인 이익을 취하는 불법적인 행동을 말한다. 이러한 금융사기는 무지하거나 노약자들에게만 일어나는 것이 아니라 일반 시민, 대학교수, 법원장까지 사회계층을 불문하고 발생한다[1].

더욱 심각한 것은 최근의 금융사기는 사회공학적(social engineering) 방식으로 진화하고 있다. 한국인터넷진흥원에 따르면, 개인정보 탈취의 가장 주된 원인으로 사람의 취약점을 공략하여 정보시스템을 기반으로 하는 정상적인 보안절차를 무력화 시키는 사회공학적 기법이 지목되고 있다[2]. 이러한 금융사기는 보이스피싱(Voice Phishing), 파밍(Parming), 메모리해킹(Memory Hacking), 스미싱(Smishing), 랜섬웨어(Ransom Ware) 등으로 점차적으로 진화되고 있다.

금융사기는 이미 많은 사람들이 인지하고 있고, 뻔한 수법이지만, 왜 많은 사람들이 여전히 피해를 당하고 있을까? 이것이 본 연구의 주된 연구 질문이다.

특히 본 연구에서는 금융사기가 사회공학적 방식으로 진화되고 있음에 주목하여 다음과 같은 두 가지 분명한 연구목적을 갖는다. 첫째, 금융사기를 당하는 주된 이유가 무엇인지를 규명하고자 한다. 둘째, 금융사기 피해 단계를 분석하여 패턴화 하여 제시하고자 한다.

본 연구의 차별성은 다음과 같다. 기존의 금융사기와 관련한 연구는 다소 진행 되었지만 실제 피해자들을 대상으로 한 연구는 거의 없는 실정이다. 이러한 이유는 현실적으로 금융사기를 경험한 피해자들을 구하기 어렵기 때문이다. 그러나 본 연구에서는 실제로 금융사기를 당한 피해자들을 대상으로 금융사기를 당하는 근본적인 이유와 구체적으로 피해 단계를 분석한 연구의 차별점을 가지고 있다.

말하자면, 본 연구에서는 위기관리 관점으로 금융사기의 예방 및 대책을 수립하기 위해, 기술적 접근이 아닌 인식적 접근으로 실제 피해자를 대상으로 피해 원인을 파악하고 인식 제고에 대한 제언을 제시하고자 한다. 즉, 금융사기가 발생 할 수 밖에 없는 피해 단계를 분석하고, 피해자들의 인간 측면의 심리 및 인식 문제에 주안점을 둔다. 이를 위해 개인적 차원에서 발생하는 심리적 인지오류 도출하여 설명하고 토의하고자 한다.

2. 이론적 배경

2.1 금융사기

금융사기란 '금융거래에 필요한 신용과 신뢰를 위배하여 악의적으로 금전적 이익을 추구하는 행위로 금융거래 주체 사이에서 안전을 침해하고 궁극적으로는 국민 질서를 위배하는 것'으로 정의된다[3].

일반적으로는 전자금융거래의 취약점을 이용하여 피해금액을 이체시키는 신종 금융범죄수법인 피싱·파밍·메모리해킹 등을 통칭하는 용어로 사용된다[4]. 금융사기에 대한 대표적인 수법은 다음과 같이 크게 세 가지로 분류될 수 있다. 첫째, 공격자가 피해자를 속여 스스로 정상적인 이체를 하게 하는 행위, 둘째 공격자가 피해자의 개인금융정보를 알아내어 인증과정을 통과하고 자금을 직접 이체하는 행위, 셋째 공격자가 악성코드를 이용하여 피해자의 정상적인 이체거래 요청 정보를 수정하여 공격자가 확보한 계좌로 이체되도록 하는 행위로 분류할 수 있다[4].

2.2 금융사기 관련 선행연구 고찰

금융사기와 관련한 소비자의 직접적인 피해와 금융사기 피해 관련 요인 등을 분석한 논문은 그리 많지 않은 실정이다. 기존의 연구들은 주로 범죄학 및 법학분야에서 연구되었으며 금융사기와 관련된 제도, 개선방안, 처벌 방안 등을 살펴본 연구가 있고 범죄에 취약하다고 여겨지는 특정 계층으로 고령층에 대한 금융사기 및 전반적인 사기 취약성에 대하여 살펴본 연구들이 진행되었다. 그러나 일반적인 소비자를 대상으로 금융사기를 살펴본 연구는 그리 많지 않은 실정이다[5].

먼저, 범죄학 및 법학에서 금융사기와 관련하여 수행된 연구들은 일반적인 금융사기의 현황 및 동향, 관련 제도의 개선 및 처벌, 손해 배상 등에 대하여 논의하여 왔다. 한편 일반적인 금융사기의 동향 및 투자사기에 관하여 살펴본 박정선 외 2(2011)의 연구는 투자사기의 개념을 정의하고 유형을 분류하여 제시하였으며 1999년부터 2010년 사이 국내외 언론에 보도된 총 112건의 투자사기를 분석하여 그 유형별 특징 및 피해 규모 등을 제시하였다[6].

또한 금융사기와 직접적인 연관성이 있는 연구들로서는 국내에서 보이스피싱 관련 피해가 최초로 보고된 2006년 이후에 보이스피싱의 동향, 대응방안, 국제적인

비교, 피해자 손해보전 방안 등을 살펴본 연구들이 존재한다. 보이스 피싱의 원인과 피해자 특정 등을 함께 설명한 연구들이 있으며[7-9], 이훈재[8]의 연구에서는 국제공조 및 국내 유관기관의 공조 시스템 강화, 금융 및 통신 시스템의 개선, 전담 수기기관의 확충, 대국민 홍보 및 교육 강화 등을 제시하였다[8].

한편, 이봉한[10]의 연구에서는 전자금융사기피해 구제법, 휴대전화 단말기의 부정 이용 방지법 등의 법 제정이 필요하다고 역설하였으며, 이봉한[8]과 이훈재[10]의 경우에는 보이스피싱의 피해자 특성이 특정 연령이나 성별, 계층에 한정되지 않고 무차별적이라는 점을 제시하였다. 아울러, 차영민과 송영시[11]는 보이스피싱 사기 피해가 「전기통신금융사기 피해 방지 및 피해금 환급에 관한 특별법」에 의해 일부 보전이 되기는 하지만 실질적인 피해의 보전이 이루어지지 못하고 있는 점을 지적하고 있다.

그러나, 이러한 일련의 연구들은 최근의 금융사기의 트렌드와 새로운 유형의 피해현황 그리고 사회공학적 진화양상들을 담아내지 못하고 있는 한계점을 비판할 수 있다.

2.3 금융사기의 최근 피해현황

금융사기와 관련한 가장 최근의 공식통계자료인 경찰청의 발표에 따르면, Table 1과 같이 2014년부터 2015년까지 2년간 피싱, 파밍, 메모리해킹을 통한 전자금융사기는 모두 20,301건이 발생했다. 연도별로는 2014년 총 9,218건, 2015년 총 11,083건으로 월 평균 약 845건에 달한다. 특히 주목할 것은 금융사기에 대한 홍보 등으로 인해 경각심이 사회전반적으로 확산되었음에도 불구하고 Fig. 1과 같이 피해건수는 더 증가하고 있는 실정이다.

특히, 최근에 랜섬웨어에 대한 공포는 사회전반적으로 확산되고 있다. 랜섬웨어의 피해현황은 Table 2와 같다. 자세히 살펴보면, 피해자, 피해액, 비트코인 지급액(해커에게 지급) 추정치가 2015년 대비 2016년에 3배 이상 증가하였고, 추가적으로 2016년 발견된 랜섬웨어의 공격방식은 16가지로 2015년 8가지에서 2배 증가하였다.

더 구체적으로 살펴보면 기존 개인정보를 거래하던 시장의 붕괴로 해커는 비트코인(bit coin)을 얻기 위해 사회공학적 기법을 접목하여 더욱 지능적인 범죄로 발전할 것으로 보인다. 이에 맞서 피해자는 랜섬웨어 위험에 대한 인식 수준이 확대되어 정기적인 데이터 백업과 발전된 보안기술을 기반으로 랜섬웨어의 타겟은 기존 개인정보에서 병원 DB, 클라우드 저장소, 기업의 문서중앙화 시스템, 인사자금 기밀파일, 공기업 기밀파일 등으로 진화 되고 있다[12].

Table 1. Type and Occurrence Frequency of Electronic Financial Frauds in 2014-2015(Source: Korean National Police Agency, Jung et al. 2017)

	2014	2015	Sum	Ratio
Phishing	1,962	1,726	3,68	18.2%
Pharming	7,101	9,233	16,334	80.5%
Memory Hacking	155	124	125	1.4%
Sum	9,218	11,083	20,301	100%

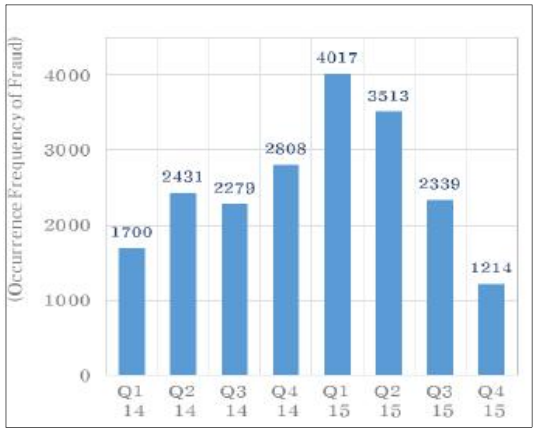

Fig. 1. Occurrence Frequency of Electronic Financial Frauds in 2014-2015(Source: Korean National Police Agency, Jung et al. 2017)

Table 2. Occurrence Frequency of Ransomeware Crime(Source: Korean National Police Agency, Jung et al. 2017)

	2015	2016	Sum
Crime Report	2,678	3,855	6,533
Victims	53,000	130,000	183,000
Demage Amount	$11 Million	$30 Million	$41 Million
Bitcoin Amount Paid	$3 Million	$10 Million	$13 Million

2.4 금융사기의 사회공학적 진화

최근 금융사기는 사회공학적으로 진화하는 양상을 띄고 있다. 사회공학적 기법이란 사람의 취약점을 공략하여 인간 상호작용의 신뢰를 통한 정상적인 보안절차를 무력화시키는 행위를 말한다[2].

일반적으로 정보시스템의 운용은 하드웨어(H/W), 소프트웨어(S/W), 그리고 인적요소(Humanware)로 구성되어있다. 이 중, 가장 취약한 요소는 바로 '인적요소'이다. 왜냐하면, 사람이란 예측 불가능한데다가 조작이나 설득에 의외로 쉽게 걸려들기 때문이다. 각종 연구에서 인간은 행동 일정한 패턴 경향이 있는데 이는 치밀한 수법에 이용당할 가능성이 있음을 보여주고 있다. 즉, 보안침해피해를 당했으며 앞으로도 지속적으로 당할 가능성이 큰 경우는 기술적인 해킹이나 크래킹 때문이 아니라 바로 사회공학적 요인에 주로 기인한다고 볼 수 있다[13].

3. 연구 방법

3.1 FGI: 질적접근으로서의 초점집단 인터뷰와 타당성

본 연구는 금융사기의 원인을 보다 근원적으로 파악하여 예방 및 대책을 제시하는 목적으로 질적 연구방법으로 시도하였다. 특히 질적연구에서는 현상이나 사실을 연구하기 위한 기법과 도구의 적용과 선택이 중요하다[14]. 다양한 질적 연구방법 중 본 연구에서는 '포커스그룹 인터뷰'(FGI: focus group interview)를 채택하였다. 이러한 주된 이유로는, 포커스그룹 인터뷰(FGI)는 인터뷰 참여자와 심층적인 대화를 통해 수량화가 불가능한 가치, 태도, 인식을 도출하여 구체적인 사례와 제언을 심층적으로 이해할 수 있으며 주제에 대한 타당한 질적 논거를 구축 할 수 있기 때문이다[15]. 또한 인간이 느끼는 생생한 체험의 의미를 서술하고 조사함으로써 체험을 통하여 형성되는 지식 현상을 분석하는 도구로 유용하게 사용될 수 있기 때문이다[16,17].

따라서, 본 연구에서는 초점집단면접을 통해 연구참여자와의 심층적인 대화과정을 통해 녹취한 자료들을 해독하고 주요 진술들을 체계적으로 분석하여 기초자료들을 도출한다는 점에서 초점집단면접기법을 주요 연구방법으로 채택되었다.

특히, 본 연구에서 강조하고 싶은 점은 실제 피해자들(actual victims)을 대상으로 초점인터뷰면접을 진행하였다는 점이다. 사실, 기존의 금융사기와 관련해 진행된 대부분의 연구들은 애초의 연구취지와는 다르게 금융사기 피해자가 아닌 일반 불특정 다수를 바탕으로 연구를 진행하고 있으며 그러한 결과를 일반화 시키는 심각한 연구방법적 오류를 범하고 있다(research methodological error). 그러나 본 연구에서는 실제로 금융사기를 당해 막대한 경제적 피해를 경험한 '실제 피해자'들을 대상으로 포커스집단면접을 진행하였다.

3.2 자료수집 및 절차

기본적으로 본 연구에서는 금융사기를 경험한 실제피해자들을 대상으로 인터뷰를 통한 자료수집을 하고자 하였다. 그러나, 현실적으로 금융사기를 당한 실제피해자들을 구한다는 것은 매우 어려운 일이다. 이에 다음과 같은 창의적 접근(creative research approach)을 통해 실제피해자들을 통한 귀중한 데이터들을 수집할 수 있었다.

구체적인 자료수집 절차는 다음과 같다.

첫째, 본 연구자들은 금융사기와 관련한 실제피해자들을 모집하기 위해 다양한 창의적인 방법들을 동원하였다. 예를 들어, 금융사기를 당한 피해자의 경우 자신과 동일한 피해 경험이 있는지를 알아보기 위해 인터넷 커뮤니티를 찾는다는 행위적 패턴이 있다는 것을 착안하게 되었다. 이에, 이미 2011년 9월 19일에 개설되어 현재 우리나라에서 가장 많은 회원 수(7,753명)를 보유하고 있는 '네이버까페 - 금융피해자 소송모임(http://cafe.naver.com/pax1004)이라는 온라인 커뮤니티 카페를 발견할 수 있었다.

둘째, 네이버까페 - 금융피해자 소송모임의 게시판에 본 연구의 목적과 취지에 대해 진정성 있게 기술하여 인터뷰 참가자를 모집한다는 공지와 함께 인터뷰 참가자들에게는 스타벅스커피 기프트콘과 같은 소정의 선물을 제공한다는 공지사항을 올렸다.

셋째, 공지사항을 보고 인터뷰에 응한 대상자 중, 과거의 실제 사건을 당했을 당시, 네이버까페 - 금융피해자 소송모임에 피해사례에 대해 글을 게시했거나 경찰과 해당 거래은행에 피해사실을 접수한 실제피해자 12명을 선정하여 최종 인터뷰 대상자로 선정하였다. 이러한 시도를 통해 자료수집의 정교성과 신뢰성을 높이고자 하였다.

최종 선정된 인터뷰 대상자들에게 2017년 3월 2일부

터 3월 16일까지 2주일 동안 전화인터뷰를 실시하였다. 전화인터뷰로 진행한 이유로는 첫째, 피해자들의 경우 직접적인 노출을 꺼리는 경향이 있고 둘째, 피해자들의 거주지역이 수도권과 지방 등과 같이 광범위하게 거주하는 시·공간적 제한으로 인해 전화인터뷰 방식으로 진행하였다.

4. 결과 분석 및 논의

실제 인터뷰는 다음과 같은 방식으로 진행되었다. 우선, 실제 피해자들에게 미리 사전에 구조화된 설문지(structured questionnaire)를 제공하고 개별적으로 인터뷰 시간을 통보한 다음, 해당 시간에 전화 인터뷰를 진행하였다. 실제 인터뷰 시에는 자료분석을 하기 위해 모든 내용은 제보자들의 허락을 받아 녹음했으며, 인터뷰를 하는 동안 Patton[14]와 같은 질적 연구자들의 권고에 따라 이론노트(TN), 방법노트(MN)와 같은 현장 노트를 활용하여 즉석에서 메모했으며 나중에 이를 결과분석에 활용하였다[13].

4.1 피해자 특성

인터뷰를 실시한 응답 피해자들의 특성은 Table 3과 같다. 응답 피해자들의 특성을 살펴보면 성별로서는 주로 여성이 많으며, 연령으로는 20대에서 50대에 이르기까지 다양하다. 한편, 흥미로운 것은 금융사기는 학력수준이 낮거나 소위 무지(無知)에서 발생하는 것이 아니라, 응답 피해자의 대부분은 대학 이상의 학력을 가졌다는 것이다. 실제 피해자들과의 인터뷰 결과 명문대 출신이나 대학원 이상의 학력을 소지한 사람들도 다수 있었으며, 이는 소위 누구나 금융사기를 당할 수 있다는 것을 암시해 주었다.

피해 금액적으로는 최소 5백만원에서 주로 3천만원~6천만원대가 가장 많았으며 심지어는 1억 2천만원에 이르기까지 막대한 금액의 금융사기 피해를 당한 것으로 조사되었다.

4.2 피해단계 패턴 분석

초점집단인터뷰를 통한 실제 피해자들의 피해 과정을 분석한 결과, Fig. 2와 같이 일정한 피해 패턴으로 요목화하여 제시될 수 있었다.

Table 3. The Profiles of FGI Victims

	Gender	Age	Education	Damage Amount
Victim A	Female	20s	Undergraduate	$50,000
Victim B	Female	30s	Undergraduate	$15,000
Victim C	Male	50s	High School	$120,000
Victim D	Female	20s	Undergraduate	$60,000
Victim E	Female	30s	Graduate	$45,000
Victim F	Female	40s	Undergraduate	$60,000
Victim G	Female	40s	Undergraduate	$35,000
Victim H	Male	20s	Undergraduate	$50,000
Victim I	Female	30s	Undergraduate	$45,000
Victim J	Female	30s	High School	$25,000
Victim K	Male	40s	Undergraduate	$40,000
Victim L	Female	20s	Graduate	$45,000

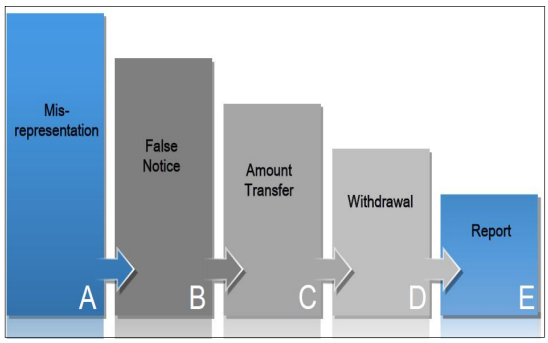

Fig. 2. Demage Patterns of Electronic Financial Frauds

[1단계] 공공기관 사칭

금융사기범들은 주로 경찰이나 검찰 혹은 금융감독원을 사칭하여 피해자들에게 접근한다.

[2단계] 계좌해킹통보

금융사기범들은 피해자 자신의 계좌가 해킹 당했다는 사실을 거짓으로 통보한다. 놀라운 것은 이때, 금융사기범들은 피해자들의 정확한 인적사항 뿐만 아니라 주거래 은행의 이름과 심지어는 잔고금액까지 말한다. 즉, 이러한 것은 금융사기기법이 사회공학화와 더불어 점점 정교하게 진화되어, 과거와 같이 무작정 접근하는 것이 아니라, 파밍 혹은 메모리 해킹과 같이 사전에 피해자가 사용하고 있는 컴퓨터 자체를 해킹하여 피해자가 의심의 여지가 없도록 정교한 개인정보를 획득한 후 접근하고 있다. 이러한 정확한 정보를 통해 상대방에게 “지금 본인이

사용하는 계좌가 해킹 당했는데, 금융감독원의 안전한 공적계좌에 입금"할 것을 권유한다.

[3단계] 실제 계좌 이체

피해자들은 본인의 목돈이 입금된 계좌가 해킹당했다는 소식에 당황한 나머지 사기범들이 알려준 '거짓 금융감독원 계좌'에 실제로 입금한다

[4단계] 관련 금액 인출

미리 은행 ATM기에 대기하고 있던 또 다른 조직원이 피해자가 일명 대포통장으로 입금한 관련 금액을 실시간으로 인출해 간다.

[5단계] 신고

피해자는 어느 정도 시간이 지난 후, 별다른 연락이 오지 않아 혹시나 하고 최초 걸려온 전화번호로 다시 전화하지만 전화를 받지 않자 속았음을 깨닫고 거래은행과 경찰에 신고한다.

4.3 금융사기 왜 당하는가: 기존 범죄학적 분석과 한계점

기존의 금융사기를 설명하는 이론은 대부분 범죄학 분야에서 논의되어 왔다. 대표적으로 금융사기가 발생하는 일반적인 원인을 설명하는 이론으로는 일상활동이론(Routine Activity Theory)이 있다. 생활양식이론은 인구통계학적 특성이나 사회경제학적 특성에 인해 금융사기의 피해자가 발생한다는 이론이다. 대표적인 인구통계학적 특성 및 사회경제학적 특성으로는 개인의 직업이나, 가정, 여가 등의 일상생활에서의 특정한 양식을 들 수 있다[18].

예를 들면 Pratt [19]은 일상생활에서 온라인 활동을 많이 하는 사람일수록 온라인 사기를 당할 피해가 더 크다는 것을 주장하였다. 한편, 김성언과 양영진[9,20]은 컴퓨터의 발달과 ICT의 폭넓은 사용으로 인해 인터넷뱅킹 등의 비대면 거래가 활발해 지기 때문에 보이스 피싱과 같은 금융사기가 발생할 수 있는 기회가 더 많아 진다고 주장하였다.

즉, 일상활동이론의 핵심은 환경과 기술의 발달로 인해 일상생활의 변화가 일어나고 이러한 변화는 개인이 범죄를 당할 수 있는 여건이 조성되고 되어 특정 개인들이 범죄를 당하게 된다는 것을 말한다.

한편, 범죄학 분야의 피해자화(Victimization)이론도 제시할 수 있다. 피해자화 이론은 금융사기 피해자가 되는 과정 및 원인 등에 대해 설명하는 이론인데, 구체적으로는 구조적 선택모형(structural choice model)과 신지명성이론 등이 있다[10].

구조적선택모형은 범죄의 피해자가 되기 쉬운 환경에 처해 있기 때문에 피해자가 되기 쉽다는 모형을 말한다. 구체적으로 범죄자의 접근이 쉬운 환경이나, 위험에 노출되어 있는 경우 범죄자의 표적이 되기 쉽다는 것이다. 아울러, 신지명성이론은 피해자가 범죄자로부터 지명을 받기 쉽도록 행동하기 때문에 피해가 발생한다는 것이다.

그러나, 이러한 일련의 기존의 범죄학적 이론들은 비록 일반 점죄를 경험하는 이유에 대해서는 설명해 줄 수 있으나, 실제 현실세계에서 금융사기를 당하는 근원적인 이유에 대해서 설명력이 부족한 한계점을 지적할 수 있다.

4.3 금융사기 왜 당하는가: 행동경제학적 분석

본 연구에서 FGI를 통한 심층분석을 통해 금융사기의 발생 원인을 보다 근원적인 시각으로 분석해 본 결과, 가장 주된 이유로는 "설마 이런 일이 나에게 일어나겠어?'라는 소위 낙관적 편향(optimistic bias)라는 심리적 오류를 범하는 것으로 분석되었다.

낙관적 편향이란 행동경제학적(behaviroal economics)인 대표적인 심리적 오류로서 최근 정보보안(information security) 분야에서 매우 중요한 이론적 개념을 제공해 주고 있다. 그러나, 이론적 파급성에 비해 실제 활발한 연구는 진행되지 않고 있다.

특히, 2017년 노벨 경제학상으로는 행동경제학 분야의 대표적인 연구자인 시카고 대학(Chicago University)의 Richard Thaler 교수가 수상했다. 핵심내용으로는, 기존의 고전적 경제학(traditional economics)에서는 '인간은 합리적 존재'라고 가정하지만 행동경제학은 그렇지 않다. 즉, 행동경제학 측면으로 보는 인간이라는 존재는 '제한된 합리성'(bounded rationality)만을 가지고 있고[21], 사실 인간은 일반적으로 '주먹구구식'의 휴리스틱(heuristic) 방식으로 의사결정을 하고 있다는 것이 행동경제학의 핵심 이론이다[22].

즉, 인간에게는 낙관적 편향과 같은 아주 근거없는 주관적 믿음을 가지고 있으며 금융사기와 같은 일은 결코 자신에게는 일어나지 않고 무지하거나 나이가 많은 할아버지, 할머니와 같은 분들에게만 일어난다는 빈약한 정

보보안 의식을 공통적으로 가지고 있음이 분석되었다.

"제가 금융사기에 당하게 될 줄은 꿈에도 몰랐어요" (피해자 A)

"금융사기는 할아버지 할머니나 무식한 사람들만 당하는 줄 알았거든요. 제가 당할 줄은 진짜 몰랐어요" (피해자 B)

"TV나 뉴스에서 금융사기 당한 사람들 보면 아주 바보 같다는 생각을 했는데 제가 그렇게 되었다고 생각하니 정말 제 자신이 한심스러워요." (피해자 C)

이러한 낙관적 편향의식에 대해 이론적으로 좀 더 자세히 살펴보면, 낙관적 편향(optimistic bias)이란 본인에게 불리한 결과가 일어날 확률을 낮게 책정하는 반면 자신들에게 유리한 결과가 일어날 사건에 대해 그 확률을 높게 보는 경향을 뜻한다.

즉, 낙관적 편향은 개인과 타인에 대한 위험 인식차이를 설명하는데 대표적인 이론적 배경으로 활용될 수 있는데 특히 다양한 정보보안 위험 상황에서 효과적으로 설명할 수 있다[23]. 이러한 낙관적 편향은 심리적인 관점에서 Egocentrism (자기중심적 사고), Positivity bias (긍정적 편향), Self-esteem (자존감), Illusion of control (통제의 환상), Social distance (사회적 거리) 현상 등과 관련해 깊은 연관이 있는 것으로 보고 있다[24].

관련 연구로서는, Rhee et al.[25]의 연구에서 컴퓨터 사용자들에게 정보보안에 필요한 방화벽과 백신 프로그램을 제대로 사용하고 있는지 설문조사를 실시한 결과, 본인이 바이러스에 감염될 가능성은 타인과 비교해 매우 낮게 평가했다. 또한 Rhee et al.[26]는 조직적 측면에서 낙관적 편향을 연구했다. 이 연구에서도 동일하게 각 조직의 CIO(chief information officer)들은 본인 회사의 정보시스템 보안은 다른 회사 보다 더 안전하다는 근거 없는 믿음을 갖고 있는 것으로 조사되었다.

따라서 본 연구에서도 분석된 동일한 현상은 정보보안 불감증의 주원인으로 금융사기 피해자 FGI를 통해 도출한 "설마 제가 사기를 당할 줄은 정말 몰랐어요", "의심조차 못했어요"라는 소비자의 근거없는 믿음이라는 행동경제학적인 측면으로의 근원적인 해석 가능하다.

5. 결론 및 시사점

본 연구는 최근 금융사기가 사회공학적 방식으로 진화하고 있는 것에 주목하여 금융사기 피해 단계를 분석하여 제시하고 보다 근원적으로 금융사기를 당하는 주된 이유가 무엇인지에 대해 행동경제학적인 해석을 시도하였다. 특히 기존의 관련 연구에서는 금융사기에 대한 연구를 수행한다고 하였지만 '실제 피해자'를 대상으로 수행한 연구는 거의 없는 실정에서 본 연구는 실제 피해자를 대상으로 분석한 중요한 의의를 갖는다.

본 연구의 결론을 정리하면 다음과 같다.

첫째, 본 연구의 결과는 오늘날 발생하는 금융사기는 사회공학적기법과 생활밀착형 키워드와 함께 지능형 범죄로 진화하여, 피해자가 보다 위험 인지가 보다 낮은 허점을 노려 의심의 여지없이 피해가 발생하는 것으로 실제로 파악되었다.

둘째, 본 연구의 결과는 피해자의 위험인지와 금융사기의 영향 요인 파악을 위해 FGI 기법을 통해 분석한 결과, 일정한 피해 패턴이 있음을 제시할 수 있었다.

셋째, 본 연구의 결과는 피해자의 위험인지 오류 및 심리적 오류인 낙관적편향(optimistic bias)가 금융사기를 당하는 주된 이유임을 알 수 있었다.

결론적으로 본 연구에서 분석한 결과를 통해 위기관리관점으로 금융사기의 예방 및 대책을 수립하기 위해 기술적 접근이 아닌 인식적 접근으로 실제 피해자를 대상으로 피해 원인을 파악하고 인식제고에 대한 제언을 제시할 수 있다. 앞으로 금융사기가 더욱 고도화된 사회공학적 방식으로의 진화가 예상되는 가운데, 정부, 기업 그리고 소비자 개인은 위기관리방식으로 보다 높은 경각심과 세심한 주의를 기울어야 할 것이다.

REFERENCES

[1] S. E. Kim & Y. J. Yang. (2008). The Evolution of Tele-financial Fraud: An Analysis of Offender-Victim Interaction Structures and Respondence to 'Voice Phising'. *Korean Academy of Public Safety and Criminal Justice, 17(3),* 101-149.

[2] KISA. (2008). *Changes in Social Engineering Hacking.* Seoul: Korea Internet & Security Agency.

[3] E. J. Kim & E. M. Kim. (2014). The Types of the Financial Fraud and Characteristics of Victims Focused

on the Middle-aged and Elderly Consumers. *Journal of Consumer Policy Studies, 45(2),* 23-46.

[4] D. Y. Jeong, G. Kim & S. Lee. (2017). A Study on Risk Analysis and Countermeasures of Electronic Financial Fraud. *Journal of the Korea Institute of Information Security & Cryptology, 27(1),* 115-128.

[5] H. G. Koo & J. Y. Rha. (2015). Which Factors Cloud Affect Financial Consumer Problems Experience? - Convergence Approach of both Technical Information and Subjective Competency. *Journal of Digital Convergence, 13(5),* 31-39.

[6] C. S. Park, J. T. Hwang & S. D. Yang. (2011). An Empirical Study on the Types of the Investment Fraud. *Korean Criminpological Review, 88,* 287-314.

[7] J. Lee. (2011). An Empirical Study on the Types of the Investment Fraud. *Korean Criminpological Review, 90,* 280-304.

[8] H. J. Lee. (2009). A Study on Voice Phishing Victims and Counterm easures of the police. *Korean Association of Victimology, 17(2),* 217-244.

[9] S. E. Kim & Y. J. Yang. (2008). The Evolution of Tele-financial Fraud: An Analysis of Offender-Victim Interaction Structures and Respondence to 'Voice Phishing'. *Korean Association Of Public Safety And Criminal Justice, 17(3),* 102-149.

[10] B. H. Lee. (2008). A Study on Victimization Factors of Internet Fraud. *Korean Association of Public Safety and Criminal Justice Review, 17(1),* 112-137.

[11] Y. M. Cha. (2014). A Study on Recovery of Voice Phishing Crime. T*he Legal Studies Institute of Chosun University, 21(2),* 535-559.

[12] Ransomware Computer Emergency Response Team Coordination Center. (2007). *Ransomware Infringement Analysis Report*. Seoul: RanCERT.

[13] Y. J. Choi. (2005). *Research About the Individual Information Infringement Which Uses the Society Engineering.* Master's Thesis, Konkuk University, Seoul.

[14] M. Q. Patton. (2002). *Qualitative Research and Evaluation Methods* (3rd ed.). Newbury Park, CA: Sage Publications.

[15] J. W. Creswell. (2017). *Qualitative Inquiry and Research Design: Choosing among Five Traditions* (3rd ed.). Newbury Park, CA: Sage Publications.

[16] H. J. Lee, Y. H. Lee, S. R. Park & I. J. Park. (2017). Improvement of ICT SMEs Technology Support Programs using Exploratory FGI and Delphi techniques. *Journal of Digital Convergence, 15(9),* 35-46.

[17] K. J. Song & G. T. Yeo. (2017). A Study on Extraction of International Freight Forwarders' Service Quality Factors : the Case of South Korea. *Journal of Digital Convergence, 15(8),* 45-58.

[18] M. J, Hindelang, M. R. Gottfredson & J. Garofalo. (1978). *Victims of personal crime: An empirical foundation for a theory of personal victimization.* Cambridge, MA: Ballinger.

[19] T. C. Pratt, K. Holtfreter & M. D. Reisig. (2010). Routine online activity and internet fraud targeting: Extending the generality of routine activity theory. *Journal of Research in Crime and Delinquency, 47(3),* 267-296.

[20] D. H. Ko & Y. A. Won. (2016). A Study of Effect on Media Exposure and Cybercrime Perception. *Journal of Digital Convergence, 14(5),* 67-75.

[21] H. A. Simon. (1957). *Models of Man*, New York: John Wiley & Sons.

[22] J. P. Park. (2015). *Users' Security Protection through Fear Appeals: A Behavioral Economics Approach,* Doctoral dissertation. Yonsei University, Korea.

[23] C. T. Kein & M. Helweg-Larsen. (2002). Perceived Control and the Optimistic Bias: A Meta-analytic Review. *Psychology and Health, 17(4),* 437-446.

[24] J. R. Chapin. (2000). Third-person Perception and Optimistic Bias among Urban Minority at- Risk Youth. *Communication Research, 27(1),* 51-81.

[25] H. S. Rhee, Y. U. Ryu & C. T. Kim. (2005). *I Am Fine But You Are Not: Optimistic Bias and Illusion of Control on Information Security.* International Conference on Information Systems, Las Vegas, NV.

[26] H. S. Rhee, Y. U. Ryu & C. T. Kim. (2012). Unrealistic Optimism on Information Security Management, *Computers & Security, 31(2),* 221-232.

박 종 필(Park, Jong Pil) [정회원]

- 2008년 5월 : 뉴욕대학교(New York University) Tourism Management
- 2015년 2월 : 연세대학교 경영학과 (경영학박사)
- 2012년 3월 ~ 2016년 2월 : 연세대학교 경영연구소 연구원 / 전문연구원 역임
- 2016년 3월 ~ 현재 : 경남대학교 경영정보학과 조교수
- 관심분야 : 정보보안 및 프라이버시, 4차 산업혁명, 미래트렌드 예측 및 미래경영전략기획
- E-Mail : jpark@kyungnam.ac.kr

류 재 관(Ryu, Jae Kwan) [정회원]

- 2017년 2월 : 경남대학교 경영정보학과 (경영학사)
- 2017년 3월 ~ 현재 : 성균관대학교 일반대학원 경영학과 재학
- 관심분야 : 뉴로이미징, 빅 데이터 분석, 데이터 마이닝
- E-Mail : ryujae92@skku.edu