The Journal of Digital Policy & Management 2013 Oct; 11(10): 217-224

통신과금서비스의 피해예방을 위한 개선방안

유순덕*, 김정일**
한세대학교*, 한세대학교 e-비즈니스학과**

How to improve carrier (telecommunications) billing services to prevent damage

Soonduck Yoo*, Jungil Kim**
Dept. of e business Hansei University*

요 약 통신과금서비스는 온라인 등 각종 구매대금을 휴대전화 요금 청구시 청구되는 방식으로 이용자에게 후불제로 이용되고 있으며 이용자의 선호도로 시장확대에 영향을 주었다. 또한 거래내역을 실시간 확인할 수 있고 SMS(Short Message Service) 인증을 통해 거래 승인하는 안전한 거래로 인식되어져 왔다. 그러나 현재는 통신과금서비스를 통한 각종 사기거래가 증가하고 있어서 사회적 문제로 등장하고 있다. 최근에는 휴대전화에 각종 어플리케이션을 설치할 수 있는 환경에서 악의적인 사용자들이 SMS(Short Message Service) 인증프로세스 등을 가로채어 이용자 몰래 결제를 수행하고 이용자의 경우는 월말에 청구되는 휴대전화사용료에서 확인함으로써 문제가 되고 있다. 본 연구는 이 문제에 대해 중요성을 인식하고 피해방지 할 수 있는 개선 방안을 제시하고자 한다. 갈수록 증가하는 사기거래에 대응하기 위해 관련기관의 체계적인 환경수립을 통한 적극적인 개선노력이 필요하다. 즉 전자결제시스템의 보완, 사기거래에 대한 적극적인 홍보, 모니터링 및 사기감지 기능 강화, SMS 인증 외에 새로운 인증서비스 도입 유도 등을 개선방안으로 제시하였다. 본 연구는 안전한 통신과금서비스 환경을 제공하기 위한 방안으로 관련시장의 확대에 영향을 줄 것이다.

주제어 : 통신과금, 보안, 사기, 제도개선

Abstract Due to the development of mobile technologies, the carrier (telecommunications) billing service market is rapidly growing. carrier (telecommunications) billing service allows users to make on-line purchases through mobile-billing. Users find this particularly convenient because the payment acts as a credit transaction. Furthermore, the system is commonly believed to be secure through its use of SMS (Short Message Service) authentication and a real-time transaction history to confirm the transaction. Unfortunately, there is a growing number of fraudulent transactions threaten the future of this system. The more well documented types of security breaches involves hackers intercepting the authentication process. By contaminating the device with security breaching applications, hackers can secretly make transactions without notifying users until the end of month phone bill. This study sheds light on the importance of this societal threat and suggests solutions. In particular, “secure” systems need to be more proactive in addressing the methods hackers use to make fraudulent transactions. Our research partially covers specific methods to prevent fraudulent transactions on carrier billing service providers’ systems. We discuss about the proposed improvements such as complement of electronic payment systems, active promotion for fraudulent transactions enhanced monitoring, fraud detection and introduce a new authentication service. This research supports a future of secure communications billing services, which is essential to expanding new markets.

Key Words : Carrier billing, Security, Fraud, System improvement

* 본 논문은 2013년 한세대학교 학술연구비에 의하여 지원되었음
Received 28 July 2013, Revised 29 August 2013
Accepted 20 October 2013
Corresponding Author: Soonduck Yoo(Hansei University)
Email: harry-66@hanmail.net

ISSN: 1738-1916

1. 서론

1.1 모바일과 통신과금서비스 시장

IDC에 따르면, 전 세계 모바일 사용현황을 보면 2016년 거래금액은 6,170억달러, 이용자 수는 4억4,800 만명이 될 것으로 전망하고 있다. 국내의 모바일 쇼핑시장 규모는 2013년도에는 4조원에 달할 것으로 예상되고 있으며 국내 모바일을 활용한 거래시장은 2014년도에는 약 7.6조원으로 폭발적인 증가가 예상되고 있다. 모바일을 활용한 결제시장은 통신과금서비스와 밀접한 관계를 가지고 있다. Table 1은 국내 년간 모바일거래금액을 나타낸 표이다.

〈Table 1〉 Annual domestic mobile transaction amount(Unit: Year/One hundred million Korean won)

Year	2009	2010	2011	2012	2013	2014(Estimated)
Transactions	100	3,000	6,000	17,000	39,700	76,000

※ Source : Korea online shopping 2012.

전자거래 결제수단은 신용카드, 계좌이체, 가상계좌, 통신과금 등이 있다. Table 2는 결제 수단별 지급현황에 대해 2008년과 2011년을 비교한 것이다. 결제방식에 따른 전자결제현황으로 2011년도에는 신용카드가 60.8%, 가상계좌가 17.8%, 계좌이체가 12.3 % 이며 통신과금서비스는 약 7.0%를 차지하고 있다. 2008년 대비 2011년에 전체 거래 중에서 통신과금서비스(일부는 소액결제라고 일컫음) 점유율이 9%에서 7%로 하락했지만 전체 전자거래 시장은 증가했다. 통신과금서비스는 연간 이용자가 약 1,200만 명이 사용하고 있으며 2013년 말 기준으로 국내 통신과금서비스 시장규모가 약 3조에 이르고 있다. 통신과금서비스는 게임, 콘텐츠 등 상대적으로 소액인 상품대금을 휴대전화 이용요금과 연계하여 결제하는 것으로 스마트 기기 기술발달로 최근 관련시장이 빠르게 증가하고 있다.

〈Table 2〉 Domestic electronic trading trend according to payment method

Classification	Yr. 2008		Yr. 2011	
	Transaction rate	Amount per	Transaction rate	Amount per
Credit card	63.1%	39.561원	60.8%	46,297원
Virtual Account	16.9%	40,321원	17.8%	71,235원
Real-time bank transfer	9.0%	26,939원	12.3%	43,366원
Carrier Billing service	9.3%	8,428원	7.0%	9,672원

※ Source : The Bank of Korea 2012

통신과금서비스의 경우 개인정보와 휴대전화 인증번호만 알고 있으면 결제가 가능한 구조이다. 따라서 스마트폰에 불법어플리케이션 설치로 쉽게 인증번호를 탈취할 수 있는 환경으로 인해 관련 사기거래인 스미싱이 일어나고 있다. Table 3은 스미싱 관련 사기건수 및 해결현황이다. 2012년 11월에 630건인 사기거래가 2013년 3월에는 약 2,000건으로 증가하였다.

본 연구는 전자결제시장의 결제수단 중의 하나인 통신과금서비스가 성장함에 따라 최근에 등장하는 사기거래인 인증서를 가로채어 진행하는 스미싱에 대해 살펴본 후 이를 방지할 수 방안에 대해 논의 하고자 한다.

〈Table 3〉 Consumer complaints consultation and resolution trend according to smishing

Classification	2012.11	2012.12	2013.01	2013.02	2013.03	2013.04	Total (per)
Complaint counseling	630	607	1,110	1,494	1,909	1,046	6,796
Resolutions	4	9	25	34	57	35	164

※ Source : Cyber Terror Response Center in Korea

2. 선행연구

전 세계적으로 휴대전화요금에 함께 청구되고 있는 통신과금서비스(일부는 소액결제라고 일컫음) 시장이 증가하고 있다. 관련분야의 선행연구는 2008년 이전에는 통신과금서비스 시장현황 및 규모에 대한 조사가 이루어졌으며 2010년 이후부터는 증가되는 시장으로 인해 등장하는 문제점에 대한 지적과 이를 해결하기 위한 방안으

로 제도 및 관련 이슈사항에 대한 연구가 이루어졌다.

김서영(2011)은 “주요국가 소액결제 시스템 운영구조”에서 각 나라별 소액결제 시스템의 운영형태를 살펴보고 국내의 소액결제 시스템과 비교를 진행하였다. 소액결제의 경우 대량 거래수행에 따른 안전한 서비스를 제공하기 위해서 소액결제 시스템의 보안 강화 및 백업을 통한 기반을 지원을 해야 한다고 주장했다[3].

한국산업경제정책연구원(2011)이 발간한 “통신과금서비스 제도개선 방안 연구”에서 통신과금서비스로 인한 피해유형과 이용자 보호방안을 제시하고 통신과금에 대한 현행 법체계와 정보통신망법 개정안에 대한 의견을 제시하였다. 또한 통신과금서비스 분쟁을 해결하기 위한 별도의 분쟁해결기관의 설치에 대하여 주장하였다[5].

이재학, 박철(2010)은 “온라인 소액결제의 속성중요도에 대한 연구-안정성차원을 중심으로-”에서 온라인 환경에서 소비자들이 소액결제를 이용할 때 선호하는 결제수단과 중요시하는 속성에 대하여 399명을 통해 조사하였다. 결과는 개인정보보호와 같은 안정성에 많은 관심으로 보이는 것으로 나타났다. 따라서 온라인 소액결제 활성화를 위해서는 전자거래 시스템의 안전성을 확보하는 게 매우 중요하다고 주장했다[4].

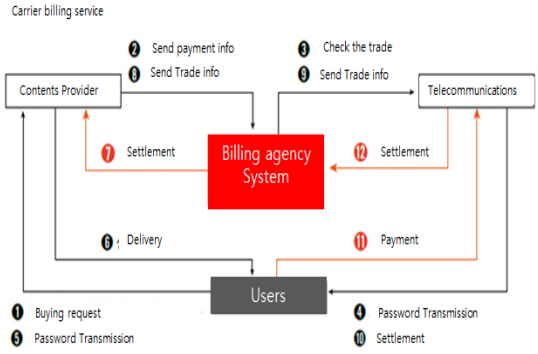
공명제(2008)는 “소액결제제도에 대한 소고”에서 소액결제제도의 현황을 살펴보고 이와 관련된 문제점으로 소액결제업무의 금융기관 확대문제, 모바일 확대에 따른 문제, 금융의 국제화에 따른 결제문제 및 운영주체의 관리문제 등에 대하여 논의 하였다[9]. 선행 연구는 통신과금서비스의 운영형태 및 서비스 개선사항에 대해 연구하였다.

앞에서 살펴 본바와 같이 선행 연구는 소액결제 시스템운영의 보안강화, 현행법의 개정의견, 전자결제서비스의 안전성확보 등에 대하여 연구하였다. 본 연구는 최근에 등장하는 각종 사기거래를 방지하기 위한 개선사항에 대해 연구 하고자 한다. 연구방법은 관련분야 전문가와 4차례 인터뷰를 통해 사기거래 문제점과 해결방안에 대해 논의를 했다. 전문가는 이동통신사, 통신과금서비스 제공기업, 한국전화결제산업협회, 한국무선인터넷산업협회의 실무자 및 관련분야 변호사로 총 15인으로 구성하였다. 본 연구방법을 선택하게 된 배경은 사기거래 측면은 통신과금서비스의 업무이해도와 운영하고 있는 시스템을 정확히 인지해야 개선방안을 도출할 수 있기 때문이다.

3. 통신과금서비스

3.1 통신과금서비스

통신과금서비스는 이용자들이 온라인에서 제공되는 각종제품이나 서비스를 구매하고 그 대금을 통신요금과 함께 납입하는 것이다. 또한 온라인에서 물건을 구입하면 결제대행사의 시스템을 통해 거래내역이 확인되고 결제내역을 근거로 휴대전화 요금에 통합되어 통신사가 고객으로부터 결제대금을 청구하는 형태로 구성되어 있다[1][2][7]. 통신과금서비스가 온라인 콘텐츠 구매, 전자상거래 등 다양한 분야에서 보편적 결제수단으로 활용되고 있다. Figure 1은 통신과금서비스의 결제 프로세스의 구성도이다.



[Fig. 1] Carrier(Telecommunications) billing service configuration

통신과금서비스의 경우는 미래창조과학부 관리하에 운영되고 있으며 사업을 영위하기 위해서는 통신과금 결제서비스 뿐만 아니라 정보보안 등 각종 요건을 갖추고 관리기관으로 부터 심사를 통해서 서비스 제공업을 등록할 수 있다. 통신과금서비스 제공자 등록현황을 보면 총 31개 업체가 등록되어 있다(2013.03 기준). 이동통신 3사(KT, SKT, LGU+)와 주요 통신과금서비스 업체인 주요 4사 (KG모빌리언스, 다날, 갤럭시아컴즈, 인포허브 등)가 전체 시장점유율은 약 98 %를 차지하고 있으며 기타 업체들로 22개 업체 (전자결제고지대행업 등)들이 서비스를 제공하고 있다.

통신과금서비스의 경우 다른 지급결제수단 대비 결제수수료율이 약 5-13% 형성되어 높은 수준을 유지하고 있다. 수령한 수수료의 5-7% 정도는 이통통신사 인프라

를 사용료 형태로 이통통신사에게 지급되고 있다.

통신과금서비스와 관련된 법제도는 “정보통신망 이용촉진 및 정보보호 등에 관한 법률”과 (방통위고시 제2012-25호) 통신과금서비스 운영에 관한 고시와 더불어 “전자상거래 등에서의 소비자보호에 관한 법률”이다[8].

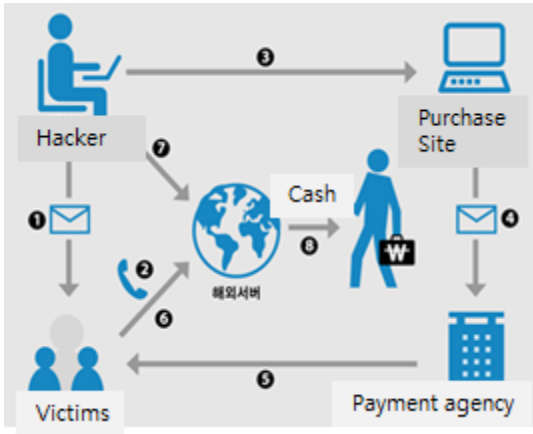
국내의 통신과금서비스 관련기관들은 미래창조과학부, 사이버경찰청, 한국소비자원, 이동통신사, 결제대행사, 콘텐츠 제공업체, 보안업체, 한국전화결제산업협회 및 통신과금안전결제협의체 (2013.04.에 발족) 이다. 미래창조과학부는 통신과금서비스 업체를 관리 감독한다. 사이버경찰청은 피해구제 및 피해예방전파, 사기조직 색출 및 검거, 스미싱 범죄형태 자료를 제공하는 역할을 수행한다. 한국소비자원은 소비자 피해신고 접수 및 업체와의 피해구제 조율, 소비자 불만 정형화 및 해결책을 제시하고 있다. 통신과금안전결제협의체는 2013. 4. 23일 발족한 민/관 협의체로서 스미싱 피해현황, 피해에 대한 이용자 구제 진행현황 및 사업자의 이용자 보호 추진 사항 등을 논의했으며 향후 보다 안전한 통신과금서비스 제공을 위한 업계의 공동노력을 결의했다. 구성위원으로는 미래창조과학부, 이동통신사, 결제대행사, 주요 컨텐츠 제공사(게임사), 한국소비자원의 업무담당자가 참여하고 있다. 컨텐츠 제공사는 사용자들에게 통신과금서비스로 컨텐츠를 판매하는 업체로서 역할을 수행한다. 다음은 통신과금서비스 사기이슈에 대하여 논의한다.

4. 통신과금서비스를 통한 사기이슈

통신과금서비스에서 최근 등장하는 사기유형은 결제창 조작을 통한 사기, 보이스 피싱 사기, 번호변작을 통한 거래사기, 스미싱 결제사기, 성인 앱을 이용한 결제사기 등이 있다. 본 연구는 통신과금서비스 결제수단과 연관된 사기거래 중에서 스미싱사기 중심으로 연구하고자 한다.

4.1 스미싱(Smishing)

통신과금서비스를 이용하기 위하여, 이름, 주민등록번호, 휴대전화번호개인정보와 결제당시 피해자에게 보내는 결제인증번호를 필요로 한다. 스미싱은 피싱 문자메시지(SMS)를 통해 결제정보를 획득하는 새로운 통신과금서비스 사기수법으로, 일명 문자메시지 (SMS)와 피싱(Phishing)의 합성어이다. Figure 2는 스미싱 사기방식에 대한 설명이며 스미싱을 통해 결제한 후 해커는 해당금액을 현금화하여 수령 한다



[Fig. 2] Smishing Fraud Flow

(1) 사전 수집한 개인정보를 기반으로 특정사용자들에게 악성앱 설치용 SMS발송
(2) 피해자가 SMS속 URL 클릭시 악성앱 감염 피해자 단말기의 정보 해외서버로 전송
(3) 해커가 게임사이트 등에서 소액결제 요청
(4) PG사에서 본인인증번호를 피해자에 발송
(5) 악성앱이 인증번호를 보이지 않게 하고 PG사의 인증번호를 해외서버로 몰래 전송
(6) 해커가 해외서버에서 정상적으로 구매절차 수행
(7) 해커가 적립된 사이버머니를 현금화 한다.

스미싱의 경우는 원초적인 보이스피싱 형태와 신종 스미싱 방식으로 나누어질 수 있다. 원초적 스미싱인 보이스피싱 형태는 1) 문자 메시지 전송, 2) 연결 / 전화, 3) 정보 확인을 위한 개인정보 요청, 4) 취소를 위한 인증번호 요청, 5) 해당 정보로 자동결제/결제 진행 방식으로 이루어진다. 신규 스미싱의 경우는 1) 문자 메시지에 URL 전송, 2) URL 클릭시 악성 앱 설치, 3) 악성 앱을 통해 개인정보 탈취 및 스마트폰 조정, 4) 인지하기 전에 각종 결제로 30만원 통신과금서비스를 한다. 이 경우는 한도 탈취 및 인증문자와 결제 확인 문자 등 차단 기능까지 악성 앱이 컨트롤 기능 내장되어 있다. 스미싱 사기유형을 살펴보면, 첫째 이벤트, 무료 쿠폰 위장 문자하는 방식이

다. 이벤트 당첨, 무료 쿠폰 등 혜택을 받을 수 있는 것으로 위장한 문자메시지 발송하여 휴대폰에서 문자메시지에 포함된 링크를 제공하여 이용자가 클릭하면 특정 어플리케이션 설치를 유도한다. 그리고 어플리케이션 설치 후 실행 시 소액결제가 진행되어 피해 발생하는 방식이다.

둘째, 결제인증번호 요구하는 형태로서 핸드폰으로 인증번호가 발송되도록 본인(수신자) 모르게 통신과금결제 신청한 후 수신자가 내용확인을 위해 해당번호로 연락할 경우 결제취소를 사유로 인증번호 요구하는 방식이다. 거래 후 인증번호 전달 시 해당번호로 통신과금결제가 진행되어 피해가 발생한다.

스미싱 문자 예시를 살펴보면 1) [업체명] 행사 내용, 무료 쿠폰/할인 쿠폰 제공 내용 - 앱 설치 URL, 2) [지인사칭] 추천 유머나 동영상 URL 전송, 3) [이통사] 요금 및 미환급금 조회 URL, 4) [공공기관] 법적 이슈 및 행정 이슈로 관심을 끌고 URL로 접속 유도, 5) [결제대행사] 결제 확인 문자인 것 같이 이목을 끌고 URL로 접속 유도, 6) [금융사]개인정보 유출 및 이체 거래 내역으로 URL 접속 유도, 7) [최신앱]최신 고성능 앱에 내용과 출시를 알리며 해당 앱 설치(URL), 8) [행사] 청첩장, 모임 안내 문자와 함께 URL 접속 유도, 9) [보안업체] 보안을 강화하기 위한 백신 다운로드 URL 으로 분류할 수 있다.

4.2 통신과금서비스의 문제점

모바일을 통한 전화결제금융사기가 등장하고 있고 통신과금서비스를 통한 결제사기도 사회적 문제로 등장했다. 통신과금서비스의 경우 지난 10년 전에 만들어진 시스템을 지속적인 업그레이드를 통하여 서비스를 제공하고 있지만 새로운 기술인 스마트폰 발달을 따라가지 못하고 있는 실정이다. 다음은 통신과금서비스 문제에 대하여 논의하고자 한다.

첫째, 스마트폰 기술발달에 따라 해킹기술도 발달했다. IOS는 애플에서 어플리케이션관리를 진행하는 거와는 달리 안드로이드는 개방형 플랫폼으로 다양한 형태의 어플리케이션이 자유롭게 유통되고 있다. 따라서 해킹기술도 발달하여 악성앱을 통해 인증번호를 가로채는 사기가 발생하고 있다. 특히 안드로이드의 경우 불법 어플리케이션을 통제관리 하는 제도가 없을 뿐만 아니라 국내는 안드로이드 보급률이 높은 상황이다.

둘째, 각종기관에서 유출된 개인정보가 시중에서 유통되고 있다. 현재 운용되고 있는 시스템에서 SMS 인증번호 등 일부정보를 해커가 확보한 경우 손쉽게 결제처리를 할 수 있는 환경을 보유하고 있다. KT, 네이트 등 국내 대형 온라인사이트에서 이미 해킹을 통해 국내 대다수의 개인정보가 유출된 관계로 스미싱 사기는 피해자의 휴대폰으로 보내는 결제인증번호를 가로채기만 하면 피해자도 모르게 금융사기가 가능한 현실이다[6].

셋째, 이용자가 사기거래에 대해 알지 못해서 사기거래발생 및 적절한 대응이 이루어지지 못한다. 기술 발달에 따라 여러 가지형태로 등장하는 사기거래에 대해 이용자가 인지 못해 일어나는 경우가 대부분이다.

넷째, 사기거래를 줄일 수 있는 제도가 상대적으로 미흡하다. 예를 들면 사기거래를 처벌할 수 있는 징벌적 조항이 있지만 사기거래를 통해 얻은 수익이 징벌적 조항보다 우수하다고 여기는 경우 사기거래 발생 가능성이 등장하기 때문이다.

다섯째, 전자결제대행업의 경우 CP(Contents Provider)에 대한 확인절차 기준의 완화로 인해 발생하고 있다. 통신과금 전자결제대행 기업의 경우는 대형 CP사로부터 거래 수수료를 저가로 받지만 사기 거래 등 위험 리스크가 높은 CP의 경우 고액의 수수료를 수령하여 기업의 이익을 보전하고 있기 때문에 거래를 허용하고 있다.

여섯째, 사기거래 발생 후 이용자 피해 대책마련이 미흡하다. 이용자의 경우 사기거래 발생 후 등장하는 피해가 이용자의 과실로 고려하여 적절한 피해 보상을 받지 못하고 있다.

일곱째, 기존 수년간 사용해 온 SMS 인증서비스가 한계에 도달해 있다. 통신과금서비스 거래승인을 위해 휴대전화에 수령된 인증번호를 소비자가 입력하는 것이 인증수단으로 책정된 SMS 서비스가 현재 기술에서는 인증서비스로 받아들이기에는 한계를 보유하고 있다.

여덟째, 전자결제대행기업과 이동통신사의 사기거래 감지 시스템의 미흡으로 발생하고 있다.

다음은 통신과금서비스의 피해에 대한 개선방안에 대해 논의 하고자 한다.

5. 통신과금서비스 피해예방을 위한 개선방안 연구

스마트폰 기술이 발달하고 있어 현행 SMS를 통한 통

신과금서비스는 한계에 도달하고 있으며 이를 악용한 사기거래가 최근 등장하고 있다. 따라서 본 논문은 사기거래 피해예방을 위한 구체적인 방안에 논의했다.

첫째, 스마트폰 기술발달에 따라 지속적인 전자결제 시스템에 대한 보완이 필요하다. 이를 위해서는 전자결제시스템에 대한 이통사와 운영업체들은 기존 시스템을 통한 수익창출에 안주하기 보다는 운영시스템에 대한 적극적인 투자를 통해 발달하는 기술에 대응할 수 있는 환경을 조성해야 한다. 금융거래 시스템의 경우 안전성이 최우선으로 고려되며 서비스 운영기업의 적극적인 의지가 반영되어야 시스템개선에 대해 투자가 이루어질 수 있다. 따라서 정부는 관련 시스템을 업그레이드를 할 수 있는 환경을 자율규제 등을 통해 지원해야 한다.

둘째, 개인정보 등 유출에 강력한 처벌뿐만 아니라 대해 이에 따른 피해에 대한 책임을 처벌할 수 있는 제도적 환경조성을 해야 한다. 2012년에 발표된 주민번호 수집 제한에 대한 제도개선을 대표적인 사례로 들 수 있다. 그리고 개인정보 유출은 여러 분야에 파급효과가 커서 지속적인 보완 및 연구가 필요하다.

셋째, 최근 등장하는 사기거래 위협에 대해 이용자에게 적극적으로 홍보가 필요하다. 이용자에게 피해방지 방안, 피해발생시 대처방안 및 피해 재발방지 방안으로 분류하여 다양한 매체로 홍보가 진행되어야 한다. 이용자의 경우 피해를 방지하기 위해서는 모바일 및 정보관리에 적극적으로 관리를 해야 한다. 이용자는 스마트폰용 백신프로그램을 설치하고 주기적으로 업데이트 하여 악성코드 설치의 차단이 필요하다. 필요시 네이버 앱스토어, T스토어, 올레마켓, U+앱마켓 등 공인된 오픈마켓을 통해 앱(App)을 설치해야 한다. 또한 출처가 확인되지 않은 링크를 클릭하지 않도록 하고, 인터넷상에서 다운받은 APK 파일은 스마트폰에 저장/설치를 자제해야 한다. 이와 더불어 각 통신사 고객센터 및 홈페이지를 통해 소액 결제를 원천적으로 차단하거나 사용하고자 하는 결제금액을 확인하고 필요시 사용금액을 제한해야 한다. 이용자가 스미싱 사기를 인지했을 때는 스미싱 피해 구제의 경우 1단계는 경찰서에 피해내용을 신고해 사건사고 사실 확인원을 수령하고, 2단계는 이동통신사, 결제대행사, 게임사 등 관련사업자에게 관련 구비서류를 제출해야 한다. 3단계는 관련사업자를 확인 연락하고, 마지막인 4단계는 피해금액 청구보류나 환급하는 절차를 거쳐야 한다.

넷째, 기술발달에 따른 사기거래를 줄일 수 있는 제도적 개선 강화에 대한 연구가 필요하다. 특히, 사기거래를 통해 얻은 수익보다 처벌됨으로써 얻는 손실이 크다는 것을 인식할 수 있는 방향으로 제도개선이 이루어져야 한다. 이 뿐만 아니라 새롭게 등장하는 사기거래에 대한 지속적인 연구를 통해 개선방향을 제시해야 한다. 예를 들면, 통신과금서비스의 경우 이용자의 인식 없이 휴대전화 구매시 자동으로 통신과금결제 한도가 설정되었다. 그러나 최근에 사기거래 방지 차원에서 이동통신사의 참여로 휴대전화 개통시 통신과금서비스 사용 및 사용한도 금액에 대해 이용자의 동의여부를 수령하는 절차를 도입했다. 이와 같이 지속적으로 관련제도에 대한 개선이 필요하다.

다섯째, 전자결제대행업의 경우 CP(Contents Provider)에 대한 거래 허용절차 기준강화가 필요하다. 통신과금서비스 시장이 증가하여 전자결제 수수료 매출은 증가했다. 그러나 전자결제대행기업간 경쟁 강화로 전자결제대행 수수료는 하락하고 있다. 특히 대형 CP의 경우 대량 거래규모로 인해 낮은 수수료를 지불하고 있어 전자결제대행기업의 경우 수익성 창출에 많은 고민을 하고 있다. 그러나 사기거래 위험이 높은 기업의 경우 거래제한을 강화하여 시기거래를 줄임으로써 안전한 통신과금서비스라는 이미지를 제시해야 한다. 장기적으로는 통신과금서비스 시장증가에 기여하여 동반성장하는 효과를 가져 올수 있다.

여섯째, 사기거래에 대한 이용자의 피해구제에 보다 더 적극적인 방안을 제공해야 한다. 사기거래에 대해 이용자의 과실에 책임을 전가하기 보다는 관련 시스템 및 거래 환경에 대한 보완이 철저히 이루어짐으로써 사전에 방지가 가능할 수 있었다는 측면에서 접근해야 한다.

일곱째, 현재 SMS의 인증서비스를 보완하거나 다른 형태의 통신과금서비스 인증시스템을 도입할 수 있도록 관련기관은 지원을 적극적으로 해야 한다. 이동통신사에서 SMS 인증절차를 보완하기 위해 개인이 직접 입력한 비밀번호와 발송된 인증번호를 결합한 모델을 시장에 도입하고 있는 것은 매우 환영할 일이다. 그리고 이동통신사들은 통신과금서비스를 SMS 인증이 아닌 신규 인증서비스 도입에 적극적인 지원을 해야 한다. 따라서 다양한 인증서비스를 이용자가 선택할 수 있는 환경을 조성

해야 한다.

여덟째, 전자결제시스템에서 모니터링 및 사기감지 기능을 통한 사기거래가 차단되어야 한다. 예를 들면 신용카드의 경우 지속적인 사기거래(Fraud detection)에 대한 연구를 통해 관련내용을 시스템에 적용하여 운영하고 있다.

다음은 통신과금서비스에 적용할 수 있는 사기거래 방지기능 이다. 1) 시스템에서 사용자의 결제 형태를 분석하여, 스미싱 형태로 의심되는 결제요청에 대해서는 결제 차단 혹은 결제 확인 ARS 인증 진행, 2) 의심 결제 분류: 최초 소액결제 진행자, 고령자, 해당 컨텐츠 업체에 최초 결제, 연속 고액 거래자(한도까지 채워서 결제), 3) 해외 IP 차단 : 해외 IP 결제 차단, 4) 불량 IP 차단 : 불량(스미싱/보이스피싱/불법거래 등) IP 결제 차단, 5) 사용이력별 한도제한 : N개월 동안 사용 이력 없을 시 한도제한 (건당 한도, 월 한도), 6) 스미싱 사용자 제한 : 스미싱과 관련된 IP 또는 ID 사용 시 결제 차단, 7) 민원을 기준으로 차단 (민원 접수된 거래의 IP를 차단), 8) 고액 집중결제의 차단 (1시간 안에 n개 회선 이상 m원 이상 집중 결제하는 경우 차단), 9) 과거 불법 결제와 연루되었던 개인정보를 기반으로 Blacklist IP 작성, 10) 신규사용자의 고액사용 IP 수집. 상기와 같은 내용을 적용하여 사기거래에 대한 피해 예방을 할 수 있다. 그러나 개선방안이 통신과금서비스 시장축소를 유도해서는 안 된다. 기술발달에 따라 통신과금서비스 시장이 소비자에게 많은 편리성을 제공하므로 시장수요는 계속 증가할 것으로 보고 있으며 이를 활성화하면서 시장에 등장하는 부작용요소를 제도적, 환경적으로 개선하는 데에 초점을 맞추어 진행해야 할 것이다.

6. 결론

눈부신 모바일 기술발달과 이동 중에서 손쉽게 접속할 수 있는 네트워크 정보의 증가로 인해 통신과금서비스 시장의 확대를 가져왔다. 따라서 통신과금서비스 운영 및 관련 기관들의 규모가 증가 했을 뿐만 아니라. 시장증가에 따라 모바일을 활용한 각종 사기거래도 급격하게 증가했다. 이로 인해 이용자의 불만과 통신과금서비스에 대한 안전성이 위협을 받고 있는 상황에 도달했다.

본 연구는 현재 통신과금서비스 시장의 현주소를 살펴보고 최근에 등장한 스미싱 등에 대한 사기방법에 대하여 논의했다. 또한 통신과금서비스 피해예방을 위해서는 다음과 같은 것을 제안한다. 첫째, 전자결제시스템에 지속적인 보완이 필요하다. 둘째, 개인정보 등 유출에 강력한 처벌뿐만 아니라 이에 대해 여러 각도로 책임을 제공하는 제도적 환경조성을 해야 한다. 셋째, 사기거래 위협에 대해 이용자에게 적극적으로 홍보가 필요하다. 넷째, 사기거래를 줄일 수 있는 제도적 개선 강화에 대한 연구가 필요하다. 다섯째, 전자결제대행업의 경우 CP (Contents Provider)에 대한 거래 허용절차 기준강화가 필요하다. 여섯째, 사기거래에 대한 이용자의 피해구제에 보다 더 적극적인 방안을 제공해야 한다. 일곱째, SMS의 인증서비스를 보완하거나 다른 형태의 통신과금서비스 인증시스템이 도입될 수 있도록 관련기관은 지원을 적극적으로 해야 한다. 여덟째, 전자결제시스템에서 모니터링 및 사기감지 기능을 통한 사기거래가 차단되어야 한다.

통신과금서비스를 포함한 금융거래에 대해서는 지속적인 관련기관의 연구를 통해 각종 사기거래에 대해 대응을 해야 한다. 또한 기술발달로 발생하는 사기거래에 대해 이용자 피해보상 및 재발방지에 대한 많은 노력을 기울여야 한다. 장기적으로 제도개선 및 연구 등 여러 활동을 통해 안정적인 통신과금서비스라는 이미지 확보를 통해 통신과금서비스의 활성화에 기여를 해야 한다.

ACKNOWLEDGMENTS

This work was supported by Hansei University.

Reference

[1] Cby beongrae, Pak Bonggu, Kim Daegyu, Traditional market model for the activation of a small settlement to support conceptual design for authentication and privacy, (The)Journal of Korea navigation institute. XIV No. 16, Issue 4 55th (August 2012), pp.665-672

[2] Park Dusu, Online retail payment systems for the protection of financial information on the smart

card-based protocol design, Soongsil University Graduate Thesis (MS), 2012.08

[3] Kim Seoyoung, Comparison of the operating structure of major retail payment systems, Payment and Information Technology. KFTC, Issue # 45 (July 2011), pp.31-59, 2011.07.31.

[4] Lee, Jae - Hak, Park Chul, Importance of online research on the properties of a small settlement-Dimensional stability around-, Internet and Information Security Chapter 1, Issue 1 (May 2010), pp146-164, 2011.

[5] Korea Development Economic Policy Institute, Research on telecommunications billing service system improvement, 2011

[6] National Council of Green Consumers Network, Damage micro payments 2010 01.04 Aggregate quarter alone close to the number reported in 2009 : Effective measures that blind spot without solution about consumer demage, Korea National Council of Consumer Organizations, XIV No. 318 (May 2010), pp.40-42, 2010.05.10.

[7] Kim, Tae - Hyun, Kang Yuri, Discuss the implications for service activation mobile payment trendsand , 2010

[8] Jang Gangbong, Choi Ganguk, Settlement of retail payment system risk analysis in Korea, Society of Payment. 3, Issue 2 (December 2009), pp.1-26, 2009.12.30

[9] Gong Myeongjae, A study on a small payment and settlement systems, No. 41 No. 1 (February 2008), pp.17-32, 2008.02.28

유 순 덕(Soonduck Yoo)

- 1991년 2월 : 국민대학교 수학과졸업
- 1994년 8월 : 연세대학원 수학(이학석사)
- 1995년 12월 : 영국뉴카슬 대학응용수학(석사)
- 1996년 6월 ~ 1997년 12월 : 삼성, LG 영국 법인 근무
- 1999년 1월 ~ 2007년 12월 : 통인물류정보통신, 오토웍스 외 근무
- 2008년 1월 ~ 2012년 7월 : KG 모빌리언스 근무
- 2010년 3월 ~ 2013년 2월 : 한세대학교 IT융합박사
- 2013년 9월 ~ 현재 : 한세대학교 겸임교수
- 관심분야 : 전자결제, PG(Payment Gateway), 기업 지원 정부정책, 보안, 인증
- E-Mail : harry-66@hanmail.net

김 정 일(Jungil Kim)

- 1998년 3월 : OSAKA CITY UNIVERSITY 경영학과(경영석사)
- 2002년 3월 : OSAKA CITY UNIVERSITY 경영학과 (상학박사)
- 2002년 4월 ~ 현재 : OSAKA University of Economics and Law Asian Research Institute 객원연구원
- 2005년 3월 ~ 현재 : 한세대학교 경영학부 부교수
- E-Mail : cityuni05@hansei.ac.kr