디지털산업정보학회 논문지 제16권 제1호-2020년 3월
http://dx.doi.org/10.17662/ksdim.2020.16.1.041

안전한 스마트폰 앱 사용을 위한 위협 요소 검토 연구*

최 희 식* · 조 양 현**

A Study on the Threat Review to use Secure Smartphone Applications

Choi Heesik · Cho Yanghyun

〈Abstract〉

In this paper, it will study various problems such as personal information infringement from when using various useful Apps in the Smartphone environment.

It also researched the vulnerabilities Mobile Apps and the risks of personal information leakage when using Smartphone information to decrease threat and find solution. In the second chapter, it will check the existing Mobile App related Apps. In the third chapter, it will check the threats and major factors that caused by the leakage of personal information which related to the app. Then it will suggest solution and end with conclusion. This paper also looked at various problems that caused by illegal adverse effect from illegal personal information collection. Then it researched and made suggestion to make consideration on safety of personal information and privacy infringement that threat to personal information For safety of mobile banking, it proposed a safety method to separate and manage the code which has the core logic which required to run the App. For safety of direction App, when running the direction App, even if the information is collected, location information for unauthorized accessed will encrypt and store in DB, so that access to personal information is difficult. For delivery App environment, by using the national deliver order call center's representative phone to receive a telephone order then, the customer information is delivered to the branch office when it receive order and it will automatically delete information from the server when the delivery is completed by improving DB server of order. For the smart work app environment, the security solution operates automatically by separating and make independent private and work areas. Then it will suggest initialization for company's confidential business information and personal information to safe from danger even if loss.

Key Words : Smartphone App. Personal Information, Privacy Infringement, Mobile App

* 삼육대학교 컴퓨터공학부 외래교수
** 삼육대학교 컴퓨터공학부 교수(교신저자)

Ⅰ. 서론

최근 많은 사람이 신제품 출시와 함께 앞 다투어 스마트폰을 이용하여 모바일 앱을 다운받아서 금융, 배달, 쇼핑, 메신저, 카페 앱 서비스를 이용하여 이를 활용한 앱 사용이 보편화하여 가고 있다. 근래에 와서는 스마트폰 외에 갤럭시 탭이나 아이패드와 같은 휴대용 모바일 디바이스 사용도 계속해서 늘어나고 있는 추세로 정보기술이 서로 융합되어 디지털 서비스를 언제든지 편리하게 이용할 수 있는 시대가 되었다. 하지만 스마트폰에서 제공하고 있는 편리하고 유용한 다양한 스마트폰 앱들이 자신도 모르는 사이에 앱 사용에 있어서 수집되고 있으므로 개인정보 유출로 인한 사생활 침해는 심각한 사회적 문제로 급부상되고 있다.

뿐만 아니라 스마트폰의 오픈소스의 공급 및 개발로 개인정보를 이용한 다양한 공격 위협이 날로 급증하고 있으며, 스마트폰 앱 이용에 따른 사용자 정보는 사용자 계정을 비롯하여 전화번호는 물론 위치 정보 및 개인의 스케줄, 이메일, 금융정보와 같은 사생활 정보까지 자신도 모르게 불법 수집되고 있는 사실도 발생하고 있다. 이렇게 무작위로 수집된 개인정보는 제3자에게 제공되어 상업적인 마케팅에 활용되며, 실제적으로 거국적 기업 구글도 사업적 영리를 얻기 위한 마케팅 활용을 세계적 기업들과 계약을 맺고 있어 기록들에 대한 새로운 정보를 업데이트까지 하여 필요한 정보를 분석하여 정보의 가치로 활용하고 있는 것이 논란이 되었다. 본 논문에서는 스마트폰 환경에서 다양하고 유용한 앱을 이용할 때 개인정보 침해와 관련된 여러 문제점을 알아보고 이에 대처하기 위해 논문을 구성한다.

1장은 연구의 배경과 목적, 2장에서는 관련 연구로 기존의 모바일 앱과 관련된 앱에 대해서 살펴보고 3장에서는 앱과 관련된 개인정보 유출에 따른 위협적인 주요 기능 및 요소에 대해서 알아보고 4장에서는 도출된 문제점에 대한 위험 요소를 비교 분석하여 더욱더 안전한 앱 사용을 위한 개선 방안을 제시하고, 5장에서 결론으로 마무리한다.

Ⅱ. 앱의 구분

2.1 스마트폰 앱 정의

스마트폰 앱은 사용자 필요 용도에 맞게 각 카테고리의 앱을 다운로드하여 설치한 후 이용할 수 있다. 만약 컴퓨터가 윈도우, 맥 OS, 리눅스 등과 같은 기본 운영체제만 깔려 있다면, 컴퓨터 활용에 대한 이용도는 매우 낮을 것이다. 일반적으로 전문적인 사진을 편집하기 위해 필요한 '포토샵' 프로그램을 설치하고, 동영상을 편집하기 위해 '프리미어' 프로그램을, 홈페이지를 작성하기 위해서는 드림위버 등 전용프로그램을 설치하여 작업에 대한 전문성을 활용하여 해당 프로그램을 이용할 수 있다. 이와 마찬가지로 스마트폰에서 어떤 앱을 설치하느냐에 따라 스마트폰 활용과 그 가치가 달라질 수 있다. 현재 시중에 나와 있는 앱은 수십만 개에 달하며 앱을 사용하지 않고 스마트폰의 전화 기능만 이용하게 된다면 이는 진정한 스마트폰 활용을 제대로 이용하고 있다고 볼 수 없을 뿐만 아니라 값비싼 스마트폰 활용을 제대로 하지 않는 기능적인 낭비이다. 즉, 스마트폰에 앱을 설치하여 활용하는 것은 그만큼 스마트폰의 편리한 기능을 잘 활용할 수 있다고 할 수 있다[1].

2.2 앱 마켓

각 모바일 스마트폰 운영체제에서 동작하는 다양한 앱을 사용하기 위해서는 유료와 무료로 다운받을 수 있는 앱은 구글 플레이(Google Play)와 애플 스토

어(Apple Store)를 통해서 가능하다. 앱 마켓 플레이스에서 판매되는 모바일 앱 수는 너무도 다양하며 하루가 다르게 다양한 장르의 앱들이 올라오고 있으며 그 종류도 문서 작성, 음악 재생, 사진 촬영 등 기본적 기능을 수행하는 것에서부터 금융, SNS, 모바일 게임, 길 찾기, 웹툰 만화를 보는 앱 등 특별한 전문성 기능을 갖춘 수준 높은 앱까지 다양하다[2].

2.3 모바일 앱 분류

모바일 앱의 목적은 <표 1>과 같이 다양하며 4가지로 분류할 수 있다.

<표 1> 모바일 앱 구분 영역 [3]

구분	종류
물리적 기능을 대체하여 활용되고 있는 편리한 앱	전자사전, MP3, 카메라, 나침반, 스톱워치, 계산기 등
실생활에서 모바일을 활용한 편리한 앱	카풀, 배달 주문, 카페 사이렌 오더 주문, 택시 예약, 실시간 교통(버스, 지하철) 정보 등
관계형 소셜 네트워크 활용 앱	카카오톡, 페이스북, 트위터, 왓츠앱, 인스타그램 등
금융 관련 간편 결제 앱	애플페이, 삼성페이, 구글 월렛, 네이버 페이, 알리바바페이 등

2.4 국. 내외 유용한 앱

2.4.1 국내

국내에서 사용자들이 가장 널리 이용하고 있는 유용한 앱으로는 네이버, 카카오톡으로 조사되었다[4]. 그리고 앱을 통해 집안에서도 배달 음식을 주문할 수 있는 배달 앱은 출시된 이래 꾸준하게 이용되고 있는 인기 앱으로 분류된다. 이외에 멜론, 카카오 택시, 카카오페이지, 네이버 클라우드, 밴드, 야놀자, 네이버 웹툰, 쿠팡도 대중의 사랑을 받는 앱으로 분류할 수 있다.

2.4.2 해외

해외에서 출시된 앱이지만 국내에서 절대적인 강자로 군림할 수 있는 앱은 단연 유튜브이다. 국내에서도 한국인 중 10대 유튜브 사용 시간은 41시간 40분으로 소셜 네트워크 서비스 사용 시간을 앞질렀다는 소식이 연이어 보도되어 유튜브의 사용 빈도 율이 그 인기를 증명하고 있다. 또한 유튜브와 함께 인기를 얻고 있는 앱은 전 세계적인 SNS 강자 그룹인 왓츠앱(WhatsApp)을 비롯하여 핀터레스트(Pinterest), 텀블러(Tumblr), 인스타그램(Instagram), 스냅챗(Snapchat) 등이 그 뒤를 이어 꾸준한 사랑을 받는 앱으로 조사되었다[5].

2.5 파이낸스 뱅킹 앱

<그림 1>에 표시된 모바일 뱅킹 앱은 인터넷 접속이 가능한 스마트폰과 태블릿 등 모바일기기를 사용하여 직접 은행에 갈 필요 없이 스마트폰을 이용하여 자유롭게 유. 무선 통신 환경이 가능한 곳에서는 <그림 1>과 같은 앱을 이용하여 은행 업무를 할 수 있게 도와주는 서비스 앱이다. 모바일 뱅킹과 관련된 개인정보 침해를 다루는 연구는 꾸준히 연구되어 왔는데 그것은 무엇보다 금융적인 다양한 보안 이슈가 다른 분야에 비해 사회적 문제로 더 확대되었기 때문이다[6].

<그림 1> 모바일 뱅킹 앱 [7]

이러한 위험성의 보안 문제가 지적되고 있기는 하

나 30, 40대의 젊은 직장인의 대부분은 자신들의 스마트폰에 거래 금융 앱을 설치하여 컴퓨터를 켜지 않고도 스마트폰으로만 송금, 결제가 가능한 편리한 앱을 사용하고 있다. 스마트폰 모바일 앱은 유선 환경에 비해 무선 환경에서의 사용은 매우 보안이 취약하지만, 여전히 온라인과 오프라인 결제 환경에서도 널리 이용되고 있는 필수적인 앱으로 편리성을 제공하고 있다[8].

2.6 배달 앱

배달 앱을 이용하여 원하는 먹거리 성 서비스를 검색하게 되면 스마트폰이 현재 사용자 주변 위치 정보 시스템을 이용하여 관련 맛집과 관련된 상점 등을 검색하여 해당 음식 메뉴 서비스를 주문하고 대금결제까지 할 수 있는 신종 아이디어가 창출해낸 IT와 먹방을 융합한 새로운 고객 서비스 앱이다[9].

배달 앱은 자신이 가지고 있는 스마트폰에 배달 앱을 설치하여 가정에서도 편하게 치킨, 피자, 족발 등과 같은 배달음식을 주문할 수 있다. 대표적인 배달 앱으로는 요기요, 배달통, 배달의 민족과 같은 TOP3이 널리 이용되고 있다. 배달 앱은 냉장고에 붙어있는 자석형 스티커를 대체할 수 있는 새로운 패러다임으로 내가 사는 지역의 배달이 가능한 음식점과 사용자 리뷰를 통한 맛집 검색을 한 눈에 할 수 있다는 것이 장점으로 작용해 더욱더 많은 이용자를 끌어 모음으로 사랑받는 앱으로 분류되고 있다[10].

2.7 길 찾기 앱

스마트폰에서 가장 높은 대중성을 자랑하는 앱 중 하나가 길 찾기 앱일 것이다. 길 찾기 앱은 사용 연령층과 관계없이 스마트폰을 이용하는 사람이라면 단연 유용하고 필수 앱으로 선별되고 있다. 길 찾기 앱은 기능적으로 자동차/대중교통/도보/자전거 총 4가지 종류로 분류되어 서비스를 제공하고 있음으로 길 안내를 찾고 있는 사용자로서는 매우 높은 편리성을 제공받고 있다. 또한 차량 운전 시 국도 최단 거리, 고속도로 최단 거리, 유료 도로 무료 정보 등을 비교하여 사용자가 선택할 수 있는 서비스 정보를 제공하고 있으며, 도보로 길 안내를 받고자 할 때에도 최단 거리, 넓은 도로 등 선택에 따른 옵션을 다양하게 제공하고 있다. 또한, 대중교통 이용할 때에도 버스 출. 도착에 따른 안내는 물론 실시간으로 도착 소요 시간 및 지연 정보도 실시간으로 제공해 주고 있다.

2.8 스마트오더 카페 앱

대표적인 카페 앱으로는 커피를 주문할 수 있는 스타벅스가 대표적이라 할 수 있다. 이와 유사한 카페 메뉴로는 국내에서 론칭한 순수 국내 브랜드인 이디야 커피가 있다. 스타벅스와 이디야 카페 앱을 통해 '스마트 오더'를 이용할 수 있는데 그 중 장점의 하나는 멤버를 위한 주문 서비스로 줄을 서지 않고 앱으로 주문을 하게 되면 줄을 서서 기다리는 사람보다 빨리 음료를 받을 수 있다는 것이 장점이다. 현재 스타벅스에서는 하루 평균 10만 건, 전체의 약 18% 주문이 자체 앱을 통해 '스마트 오더'로 주문을 하고 있으며 이런 사례를 벤치마킹하여 이디야, 투썸플레이스 등 다른 커피 매장에서도 스마트 오더 카페 앱은 널리 활용되고 있다.

2.9 비즈니스 카드 관리 앱

리멤버는 명함을 스마트폰으로 촬영하면 명함정보를 입력하여 명함을 관리해 주는 서비스로, 기존의 광학문자인식(OCR) 기술 기반의 앱들과는 달리 수기 입력을 통해 정확도를 99.9%까지 높인 것이 특징이

다. 또한, 이름, 회사, 부서, 직책 등의 키워드를 통해 언제 어디서나 필요할 때 손쉽게 명함정보를 검색하실 수 있고 멤버 회원 간에는 이직이나 승진 등의 최신 명함정보가 자동으로 업데이트되며 명함을 기능적으로 관리해 주는 특징이 있다. 누적 가입자 수가 200만 명을 보유할 정도로 직장인들에게는 매우 인기 높은 필수 앱으로 자리 잡고 있다[11].

2.10 스마트워크 앱

4차 산업혁명이 도래되면서 스마트 워크는 불필요한 업무 영역을 줄이고 꼭 필요한 것에 집중할 수 있도록 회사와 집에서 근무적인 환경에서 시간적 활용을 잘 할 수 있도록 도와주는 비즈니스 기반의 새로운 서비스 앱으로 많은 인기를 독차지하고 있다. 스마트워크 앱은 시간과 장소에 얽매이지 않고 언제 어디서나 일할 수 있는 체제 (재택근무+ 모바일근무 + 스마트워크센터)의 클라우드 기반의 재택근무를 모바일 환경에서 제공하고 있음으로 스마트워크 클라우드 기반의 구글 드라이브, 네이버 클라우드와 같은 스토리지를 통해 문서, 스프레드시트, 프레젠테이션 작성과 같은 중요한 문서 등을 시간에 구애받지 않고 근무환경을 자유롭게 할 수 있다는 것이 장점이며 스마트환경을 통해 원격 회의, 관련 문서를 공유하고 수정, 출력이 가능하다.

Ⅲ. 앱 취약에 따른 개인정보 위협

스마트폰 앱은 많은 사람이 일상생활 속에서 잘 활용되고 있지만, 특히 안드로이드 계열의 스마트폰은 오픈 마켓 안드로이드 플랫폼을 대상으로 서비스가 제공되고 있음으로 보안 위협이 더 높다. 안드로이드 계열의 앱이 애플보다 보안 위협이 증가하고 있는 이유는 안드로이드 플랫폼이 개방성, 휴대성, 다중 처리 동시 접근성의 기능을 제공하기 때문에 다양한 유형의 공격 유형이 발생하고 있다[12].

수집된 개인정보의 공격 유형의 대부분이 불법적인 행위에 활용되고 있는데 대포통장을 만들어 보이스피싱 범죄에 이용될 뿐만 아니라 SMS 문자 메시지를 보내 메시지 내 링크된 인터넷 주소 등을 클릭하도록 유도하여 사용자가 링크된 주소를 클릭하면 악성코드가 설치되어 사용자도 모르는 사이에 소액결제가 이루어지는 금융 절취 범죄에 이용되고 있다[13]. <표 2>는 다양한 스마트폰 공격 유형이다.

<표 2> 스마트폰 공격 유형 [14]

보안 위협	공격 시도
Spyware 공격	- 사용자를 광범위하게 감시 - 최고 권한을 획득 - 모바일 기기 침투
RCSAndroid 공격	- 표적 감시를 위한 도구 - 온라인 계정 수집 - 기기정보 수집 - 마이크를 이용한 녹음 - 전방 후방 카메라를 이용한 사진 캡처
APT(Advanced Persistent Thread) 공격	- 특정 개인이나 기업을 공격 타겟으로 한 스피어피싱 공격 - 모듈 화된 악성코드 - 피해자와 통화 내용을 녹취 - 안드로이드 기반의 스마트폰 공격

3장에서는 모바일 앱에 대한 취약점과 앱 사용으로 인한 스마트폰 정보에 대한 개인정보 위협과 관련된 문제점을 알아본다.

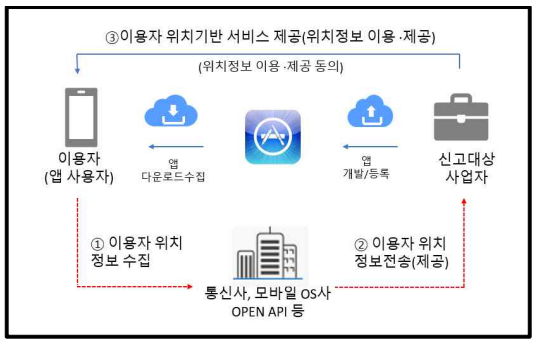
3.1 모바일 뱅킹

스마트폰 이용 시 많은 사용자가 모바일 금융 앱을 이용하여 모바일 뱅킹을 이용하고 있다. 하지만 스마

트폰 이용 시 개인 정보보안 유출 사고 및 금융 사고가 많이 발생하는 분야가 단연 모바일 뱅킹 앱 사용이다. 그것은 개인정보와 금융정보라는 재산적 가치가 더해져 사회적으로 미치는 부가가치 영향력이 높게 작용되기 때문이다. 그러나 금융 앱을 이용하는 사람이 안전과 관련된 보안에 대해서는 그리 많은 상식을 가지고 있지는 않다. 또한 금융 앱 이용과 관련된 개인정보 유출 사고 위험성에 대한 인지 조사 결과 많은 사람이 위험성에 대해서는 알고 있으나 그다지 관심이 없는 것이 대부분이다. 즉, 모바일 뱅킹 서비스 이용자가 외부 위험으로부터 정보보안 관련 사고를 미연에 방지할 수 있는 예방대책이 소홀한 나머지 정작 본인이 보이스피싱이나 스미싱과 같은 사고를 당하는 피해자로 전락하는 경우도 있다. 실제적으로 공격자는 모바일 뱅킹 이용자를 공격 대상으로 기회만 생기면 호시탐탐 공격할 기회를 엿보고 있으므로 어느 누구든지 정보 유출과 관련된 위협적인 부분을 피할 수 없는 위협적인 요소로 남아있다[15].

3.2 위치기반 서비스

스마트폰과 내비게이션 시스템의 대중화로 다양한 위치 기반 서비스(Location Based Service, LBS) 앱들이 등장하고 있다. 위치 기반 서비스를 위해서는 단말의 위치 정보들을 저장 및 관리하고 위치 정보를 이용하여 다양한 응용 서비스를 지원하는 위치기반 서비스에서 보안 서비스의 역할이 매우 중요하다고 볼 수 있다. 위치기반서비스에서는 스마트폰, PDA, 노트북 PC 등 모바일 이동통신망을 기반으로 사람이나 사물의 위치를 정확하게 파악하고 이를 활용하는 응용시스템 서비스를 제공하게 되는데 최근 들어 이를 이용하는 사용자들의 위치 정보를 위치 기반 서비스를 담고 있는 개인정보가 방대하고 그 민감도도 높으므로 보안 투자가 필수적이지만 실제로는 그렇게 운영되지 않음으로 보안상 개인정보 침해 사고 건수도 증가하고 있다. 실제로 한국인터넷진흥원(KISA)에 신고된 전체 개인정보 침해 건수는 기술적 관리적 조치 미비로 인한 개인정보누출이 차지하는 비율은 0.5%에서 2.5%로 폭증했다. 특히, 해커들이 노리는 개인정보는 이들 서비스 대부분이 고객의 특성을 고려한 타겟마케팅을 하다 보니 소비 행태를 저장하고 있다. 개인정보가 유출되면 범죄자가 특정인이 특정 시간에 특정 장소에 나타나는지 분석해 납치하거나 사생활 폭로 협박에 사용할 가능성을 배제할 수 없다. 실제로 포털 사이트에서 해킹된 정보를 이용해서 등급 높은 고객 명의로 비대면 신용카드 발급한 경우도 있다. 위치기반 서비스에서 불법으로 수집된 개인정보는 개인의 사생활적인 민감 정보가 유출되면서 <그림 2>과같이 위치 기반 서비스의 심각성을 제기하고 있으며 이들 서비스가 저장하고 있는 각종 개인정보를 이용하여 납치, 금품 협박, 유괴 등 2차 범죄가 발생할 수 있는 위험성이 초래되고 있다[16].



<그림 2> 위치기반 서비스 제공 [17]

3.3 배달 앱

스마트폰 보급과 함께 배달 앱 서비스 이용에 대한 시장 경쟁력을 확보하는 데에는 스마트폰 하나로 주문시스템, 결제시스템, 배달시스템을 하나로 통합하

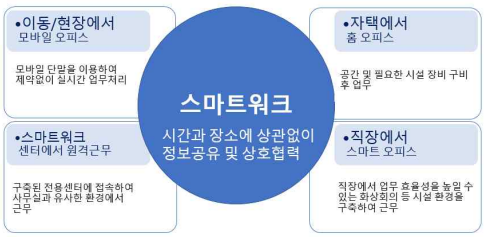
여 저렴한 수수료로 이용할 수 있는 편리성과 맛있는 맛집 정보를 쉽게 검색하고 이용할 수 있는 접근성이 용이하기

때문이다. 하지만 배달 앱을 통해 음식을 주문하면 고객 개인정보 관리가 허술하게 관리되고 있는 것이 사회적 문제로 지적되고 있다. 그것은 바로 고객이 주문 시스템을 이용하여 배달음식을 주문하면 주소와 전화번호, 결제내역 등이 기록에 남게 되는데 영업 점포에서는 점포의 이익을 극대화하기 위해 고객들의 정보를 마케팅에 이용하고 있다. 즉, 고객들의 정보를 신제품 출시 소개, 이벤트 사은품 소개 등 SMS 문자 메시지 전송 등으로 적극적인 마케팅 활용에 이용하고 있기 때문이다. 특히 앱상에서 즉시 결제할 경우 카드 정보까지 남게 되는 것은 고객 개인정보 취급상의 심각한 개인정보 유출 사고로 이어질 수 있다[18].

3.4 스마트워크 정보 수집 위협

4차 산업이 도래되면서 각 기업에서는 정보통신기술을 이용하여 시간과 장소의 제약 없이 자택에서 회사 업무를 볼 수 있거나 출장이 잦은 직원에게도 스마트 환경에서 회사 업무를 볼 수 있는 환경이 제공되고 있다. 즉, 스마트워크는 <그림 3>과 같이 모바일 환경에서 동료 직원들과 원활하게 협업하고 회사 업무를 지속해서 수행하는 근로 형태로 많은 기업이 근무 환경을 스마트환경으로 연계 운영하고 있다. 일부 기업에서는 스마트워크가 도입함에 따라 근로 장소에 대한 제약 없이 전 세계가 근무 환경이라는 점에서 큰 반응을 얻고 있다. 하지만 스마트워크 도입의 가장 큰 장애 요인 중 하나는 보안 문제로 뭐니 뭐니 해도 각종 회사 일과 관련된 기밀 유지가 외부로 유출될 수 있다는 관건이 새로운 보안 이슈로 부상하고 있다.

또한 스마트워크는 사무실 밖에서 사내 망에 접속하기 때문에 기밀 사항 등 중요한 정보가 외부로 유출될 수 있는 위험성이 서버를 통해 유출될 수 있는 위험성도 제기되고 있다. 스마트워크와 함께 모바일 오피스가 실현되면서 내부 직원들의 단말을 이용한 스마트워크에 대한 업무처리량은 점차 늘고 있다. 하지만 단말기 이용이 높아짐에 따라 단말기의 도난 및 분실로 인한 보안 위협도 높아졌다. 만약, 단말기를 분실했을 경우, 개인정보나 회사의 중요한 업무정보 유출, 시스템과 관련된 불법 접속 및 해킹과 관련된 업무적 위험이 초래될 수 있기 때문이다. 또한 정보화시대 최고의 기업 자산인 기업의 기술정보, 기밀정보가 내부 직원의 단말기 분실만으로도 위태로울 수 있는 위험성이 충분히 발생할 수 있다[19].



<그림 3> 스마트워크 work flow [20]

IV. 위험성 문제점 분석 대응 방안

최신 유행하고 있는 신형 스마트폰을 이용하여 오픈마켓이나 블랙마켓을 통해 검증되지 않은 다양한 앱에 의해 모바일 앱을 이용하고 있는 사용자 스마트 환경에서 개인정보 유출이 발생하게 된다. 최근에는 유명한 연예인들의 스마트폰의 클라우드나 메신저 등을 해킹하여 정보유출을 빙자로 금융을 협박하거나 개인정보를 제3자에게 제공되어 마켓팅에 활용되는 다양한 개인정보 유출로 인한 사회적 물의를 발생하고 있다.

오픈마켓이나 블랙마켓을 통해 유통되고 있는 앱은 안드로이드 플랫폼 기반 모바일 단말을 대상으로 인기 있는 정상 앱을 타겟팅하여 많은 사람이 이를 오인케 하여 정상 앱으로 위장한 악성 앱의 형태가 오픈 마켓플레이스 카테고리에 포함되어 있는 경우가 많으며 특히 모바일 앱을 활용한 모바일 뱅킹은 특성상 보안에 대한 심각한 우려를 안고 있는 것이 현실이다[21].

4장에서는 앱 사용 시 불법적으로 이루어진 개인정보 수집과 관련된 위협적인 악영향에 대해서 살펴보고. 스마트폰 이용 시 안일한 생각 때문에 개인정보에 대한 위험이 그대로 유출될 수 있는 위험을 알리고 개인정보 및 사생활 침해에 대한 안전성을 고려하기 위한 방안을 연구하여 제시한다.

우선적으로 아이폰 사용자와 안드로이드 계열 스마트폰 사용자는 필요한 앱을 얻기 위해 애플 스토어와 구글 플레이 스토어에서 검증된 앱을 구매하게 된다. 애플 스토어나 구글 플레이 스토어에서는 사용자가 앱을 다운로드하기 전에 앱이 안전한지를 우선적으로 검사하도록 진단한다. 또한, 사용자 기기에 악성코드와 같은 멀웨어 바이러스와 같은 앱이 검출되는지도 우선적으로 확인하게 된다. 만약, 잠재적으로 위험을 유발할 수 있는 사용자 디바이스에서 앱이 감지되면 경고 메시지를 표시하게 되며, 발견된 유해 앱 속에 포함된 악성코드 등은 기기에서 곧바로 삭제된다. 각 앱 마켓 플레이스에서는 사용자 기기에 안전하고 검증된 앱이 설치되도록 최선의 노력을 하고 있다. 이렇게 안전을 고려한 마켓 플레이스의 보안 정책 노력에도 불구하고 소비자에게 제공된 다양하고 유용한 앱에는 스미싱 차단 성능 저하와 인증 절차 미흡, 개인정보 정책 미흡 등으로 보안에 대한 정책을 무력화하여 사회에 문제가 되는 보안 이슈가 자주 발생하는 문제점이 발견되고 있다.

4.1 모바일 뱅킹 안전

모바일 뱅킹 사용에 대한 앱이 안전하지 않다는 사회적 논란과 함께 많은 사람들이 사용에 대한 여부를 지속적으로 유지할지 삭제할지에 대한 고민이 높아가고 있다. 결제 수단이 카카오뱅크, 케이뱅크와 같은 국내 최초의 인터넷뱅크가 몇 해 전 론칭되면서 모바일 스마트폰 앱 사용에 대한 경쟁은 더욱더 뜨거워지고 앱 사용에 대한 적극적인 시장 흡수를 위해 경쟁 유치가 대단하다. 신규 인터넷뱅크 업체는 스마트폰에 쓰이는 모바일뱅킹 앱은 PC와 달리 내가 갖고 있는 스마트폰을 통해서만 거래가 이루어지므로 상대적으로 안전하다고 사용자에게 보안에 대한 안정성을 고취시키고 있다. 또한 스마트폰 고유의 정보를 활용한 기기인증이 추가되기 때문에 공격자가 내 스마트폰을 훔쳐가거나 악성 앱을 설치해 집요하게 공격하지 않는 이상 해킹 가능성이 극히 적다고 금융앱 사용에 대한 장려를 권장하고 있다.

또한, 최근 은행마다 모바일뱅킹을 통해 공인인증서나 복잡한 보안 프로그램을 거치지 않고 송금 등 거래가 가능하도록 절차를 간소화하고 있다. 또한 대부분의 모바일 뱅킹 등이 비대면 으로 처리되면서 너무 편리성과 간편성을 내세우고 있을 뿐만 아니라 공인인증서 없이 처리되는 은행업무로 많은 금융 업무가 처리 시스템을 변경하고 있기에 안전한 모바일 뱅킹 사용에 대한 불안은 날로 심각해 질 수밖에 없다.

아래는 금융 앱 사용 시 매우 위험했던 피해 상황에 대한 case 사례를 가상으로 알아보도록 한다.

사례 1 : 금융 앱을 이용하여 송금 결제를 사용한 직후에, 해당 금융기관을 사칭한 문자를 받은 경험이 있다. 이 앱은 기술적으로 평상시에는 일시적으로 비활성해 있다가 A씨가 금융 앱을 사용할 경우는 활성상태로 바뀌어 '보안 알리미' 같은 형태로 보안 프로

그램을 업데이트하라는 악성코드가 심어진 메시지를 보내온다.

사례 2 : 안전을 위한 금융 앱 강화 업데이트를 요청하는 사례도 발생했다. 공격을 시도하기 위해 공격자는 공격 타겟을 정한 사용자 앱에 보안 앱을 업데이트하라는 스미싱 문자를 보낸다. 보안 위협이 있으니 링크된 보안 앱을 설치하면 안전하다는 것이다. 링크 안에는 모바일 보안 앱과 거의 비슷하게 생긴 앱이 포함되어 있기에 일반 사용자가 실제 금융 앱과 위장한 앱을 분별하기는 매우 어렵다.

사례 3 : 회사원 A 씨는 카페앱을 모바일에 탑재하여 바쁜 일상생활에서 카페앱을 아주 잘 활용하고 있다. 카페앱을 통해 빠른 주문, 멤버십 포인트 혜택, Happy Hour 등 다양한 혜택을 받고 있는데, 앱 사용을 위해 밸런스 잔액이 20,000원 미만일 경우, 자동으로 금융 기관에서 30,000원이 자동 인출이 되는 시스템이다. 하지만 A 씨는 우연히 카페 앱에서 결제가 이루어진 상황을 알게 되어 이상히 여기게 되었다. 최근 연예인 스마트폰 유출과 관련한 사고처럼 회사원 A 씨의 스마트폰 역시 해킹된 사고였다. 처음에 A 씨는 금융 결제가 카페 앱에 의해 자동으로 이루어진 것으로 인지하였으나 실제로는 모바일 금융 앱에 대한 정보가 해커에 의해 유출되어 금융 결제가 이루어진 사고였다.

아래 <표 3>는 사용자 자신의 앱이 악영향으로부터 보호받을 수 있는 사용자 기기 환경에서 기존에 사용해 오던 보안카드 보안 방식을 최근에 도입되어 보급되기 시작한 안전한 모바일 OTP 인증 방식으로 전환하여 이용하는 것을 권고한다. 또한 공격자인 해커가 기기를 무력화하고 자신의 공격기기로 전환하여 금융적인 절취 공격을 시도하는 것을 방지하기 위해 스마트폰 기기마다 국제 이동 단말식별 번호인 IMME 고유 번호를 등록하여 사용할 것을 권고한다. 기술적으로는 스마트폰 이용자의 습관 및 이용 각도, 문자 스피드, 평상시 활용하는 용도 및 사용자의 위치 동선을 크게 벗어날 경우 사용자 기기를 의심하여 2차 인증을 요구한다든지 사용자가 평상시 이용하는 이용 패턴에 따른 행태를 인식하는 이용행태에 따른 기술적 도입을 제안한다.

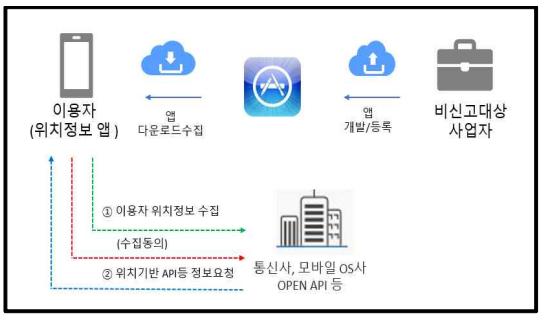
<표 3> 안전한 금융 앱 사용 권고

구분	방안	설명
사용자 기기 환경	보안카드를 모바일 OTP로 대체	사용자에게 6자리 난수 형태의 숫자를 발생시켜서 인증하는 모바일 OTP 사용 권장
	사용자 기기를 금융기관에 IMME 등록	자주 사용하는 금융 앱에 사용자 스마트 폰 기기의 IMME 국제 이동 단말기 식별 번호 등록 사용 권장
기술적 처리	금융 앱 사용 시 가상 키보드 작동	패스워드나 인증번호 입력 시 자동으로 입력 숫자에 대한 키보드 배열을 무작위 순서 방식으로 배열 처리
	코드 난독 처리	악의적인 조작 공격에 대하여 앱을 이용하여 전달되는 텍스트 기반의 문자를 식별할 수 없도록 비정상적으로 해석될 수 있도록 난독 처리
	행태 처리	사용자가 평상시 이용되고 있는 앱과 사용자가 자주 사용되고 있는 문자를 입력하는 속도, 사용자가 스마트폰을 쥐고 있는 방향 등을 학습화된 패턴을 인식하여 사용자의 기기임을 인식하는 행태 처리 기술 도입 권장

4.2 위치기반 개인정보 수집 제한

모바일 위치기반 앱 사용만으로 연인의 위치정보를 알려주는 '오빠 믿지' 앱이 사회적으로 큰 파장을 일으켜서 문제가 되어 개발자가 구속되고 앱 서비스가 중단되는 사건이 발생하였다. 스마트폰 위치기반 서비스는 사용자에게 현재 위치를 자동으로 인식하여 찾고자하는 목적지를 표시해주는 내비게이션 역

할은 물론, 사용자 위치 주변의 주유 할인, 유명 맛집, 할인 이벤트 행사 등 다양한 지역 맞춤형 정보 서비스를 제공하고 있다. 하지만 내 주변의 편의시설과 지리정보를 알려주는 동시에 소셜네트워크 서비스 사용 시에도 내가 방문했던 식당, 유명 명소에서 촬영지를 거침없이 노출하게 된다. <그림 4>는 앱 자체에서 위치정보가 수집된 후, 제 3자에게 여과 없이 개인 사생활 정보와 관련된 정보를 활용한 뒤, 수집된 모든 정보가 앱 자체에서 삭제되어 위치 정보 수집에 대한 문제가 없는 것처럼 편법으로 이용되는 문제점이 거론되고 있다. 유출된 위치기반 서비스의 개인정보는 공격자에게 보이스피싱, 스미싱, 기타 스마트폰 정보 이용 내역 공개 등 사회적 범죄의 표적이 될 수도 있는 심각한 문제점의 원인이 될 수 있다.



<그림 4> 비 신고 위치정보 수집 [17]

최근에는 O2O(online to offline)와 같은 모바일기기를 통해 오프라인 매장과 온라인 사용자를 연결해주는 위치 정보를 활용한 서비스가 유행이다. 이 서비스는 매장 주변을 자주 이용하는 멤버 회원들에게 고객의 위치를 파악하여 모바일 스마트폰을 이용하여 특별 이벤트 행사 쿠폰을 전달하게 되는 서비스이다. 매장의 입장에서는 고객의 위치 정보를 수집하여 판매 활용에 활용할 수 있지만 고객의 동의가 없는 개인정보 수집에 대한 활용은 엄연한 불법에 해당된다. 모바일 앱을 이용하는 이용자들은 스타벅스나, 이디야와 같은 국내 카페 앱을 이용할 시 반드시 위치정보 동의 및 활용에 대한 충분한 약관을 살펴본 후, 해당 서비스를 안전하게 이용하는 것이 좋다. <표 4>는 이용자 중심의 개인정보 유출 예방을 위해 교통정보, 길 안내와 같은 위치기반 서비스를 이용할 때에는 사용자 위치에 대한 개인정보를 SSL 보안 프로토콜이나 해쉬함수를 이용하여 사용자의 위치 값을 암호 처리하여 위치 값을 변경한 후, 서버로 저장되도록 하는 보안기술을 권고한다. 또한 사용자가 필요에 따라 일시적으로 이용되는 배달, 카카오택시, 실시간 교통서비스와 같은 비인가 접근 시 수집될 수 있는 위치정보는 마켓팅 활용에 제공되지 않도록 이용 후, 곧바로 삭제할 수 있는 강력한 개인정보 정책 마련이 국가적인 법제도적 차원에서 반드시 필요한 시기라고 본다.

4.3 배달 앱 개인정보 방안 마련

배달 앱 서비스 운영자의 경우 국내 정보통신망법에 따르면 무엇보다 앱 개발 시 개인정보관리서버에

<표 4> 안전한 위치정보사 사용 권고

구분	이용 서비스	보안 권고
교통정보	사용자의 위치기반을 인식하여 알려주는 실시간 교통정보 제공	사용자 위치정보를 서버로 전달 할 때 해쉬함수 암호 기법을 이용하여 위치 값을 바꾸어 저장
길 안내	사용자 차량 주행 안내 및 보행자 길 찾기 등 빠르고 안전한 길 안내 서비스	
O2O(online to offline)	대리기사, 콜택시, 배달 서비스 주문, 카폴 서비스 연계, 실시간 교통 서비스	비인가 접근 및 사용자가 필요시 사용한 개인위치정보 서비스는 서버로부터 곧바로 삭제해야 되는 강력한 개인정보 대책 마련 정책 필요
플랫폼 제공 서비스	카카오맵, T맵, 원내비 등 플랫폼에서 제공하고 길 안내 서비스	

침입차단 및 침입탐지시스템을 설치·운영하여야 하는 보안상의 등의 기술적·관리적 조치를 취할 의무가 부과된다고 한다. 배달 앱 업체 측에서도 앱을 이용하는 스마트폰 이용자들의 고객 개인정보 보안 유지와 유출을 막기 위한 자체 시스템 개발을 운영하고 있다. 하지만 많은 배달 앱들이 보안 기준을 지키지 않고 보안을 고려하지 않고 개발되었기에 개인정보에 대한 정보가 암호화되지 않고 제3자에게 전달되고 있어서 위험이 노출되고 있다. 사용자들이 주문 시 사용한 배달 앱 사용 시 자동으로 수집되는 개인정보는 서비스를 이용하고 있는 동안은 지속적으로 보관되어 영업점을 통해 활용되고 있는 것으로 조사되었다. 즉, 많은 앱 관련 기관에서 이와 같은 방식으로 개인정보를 이용하고 있으므로 고객의 정보는 돈이 되는 일종의 가치를 창조하는 수단이 되고 있다. 결국 배달 앱을 통해 주문하는 자녀와 부모의 주소와 관련된 개인정보들이 고스란히 해커들 손에 넘겨지고 있는 셈이다.

전국 각 점포 영업매장에서 수집되는 고객들의 개인정보를 안전하게 본사에서 관리하는 체제는 쉽지 않을 것이다. 하지만 본사에서 고객의 개인정보에 대한 개인정보 취득에 대한 교육이나 권고 등은 영업의 매출 증대를 위해 쉽게 지켜지지 않거나 본사의 규제에도 큰 변화가 없을 것으로 판단된다. 배달 앱이 론칭된 이후, 배달 앱 3사 모두 더 이상 개인정보 유출로 인한 브랜드 이미지 실추와 신뢰가 무너지지 않도록 배달 앱으로 인한 개인정보침해 및 유출사고가 발생하지 않도록 다음과 같이 안전한 방안을 제시한다.

배달 앱이 아닌 일부 외식 주문업체에서도 시행되고 있기는 하지만 전국 대표전화를 이용하여 전화 주문을 받도록 주문 시스템을 변경하도록 한다. 또한, 프랜차이즈 가맹주는 점주들의 기업 매출에 대한 경영 교육에만 신경 쓸 것이 아니라 고객 개인정보 관리 정책 및 이용에 따른 교육도 시행 되어야 한다. 예를 들어 고객이 배달 앱을 통해 주문을 하게 되면 점주가 소비자 정보를 마케팅 용도로 수집하는 것이 아니라 배달이 완료된 고객의 전화번호 및 주소가 저장된 개인정보는 완전히 삭제 처리되도록 정책마련이 시행되어야 한다. 만약, 점주가 이를 어길 때에는 프랜차이즈 계약 취소 및 영업 정지에 대한 페널티 이행도 포함되어야 하며, 배달 앱 관련 업계에서는 프랜차이즈 개인정보 관리 원칙이 조속히 마련되어야 한다.

4.4 스마트워크 앱 방안 마련

스마트워크 앱 활용 시 개인정보 침해가 발생하는 문제 는 사용자가 스마트폰을 분실했을 때, 공격자가 분실된 스마트폰을 습득했을 때 습득한 스마트폰의 위치기반서비스, 카메라, 마이크와 같이 모바일 단말기에 내장된 기능의 사용 권한을 획득하여 원격에서 사생활을 감시하는 위협이 발생할 수 있다. 안전한 스마트워크 환경 조성 및 스마트워크 환경을 활성하기 위해서는 무엇보다 보안 사고를 미연에 방지하고 단말기 분실 사고에 무엇보다 주의를 기울이는 것이 좋다. 만약 부득이하게 분실 사고가 발생한 경우라면 신속한 대응 및 복구 대책이 필요한데 그것은 바로 1차적 대책 마련으로 스마트워크에 이용되고 있는 단말 장치 이용에 기능적 제한을 걸어두어 일부 기능이 작동되지 않도록 한다. 또한, 2차적으로 기업의 기밀정보 및 업무적 문서 정보를 취급하는 단말기가 분실된 경우라면 스마트워크 서버와 단말기가 연결되어 있는 서버가 해킹될 수 있는 위험의 소지가 발생할 수 있다.

일단 우선적으로 클라이언트 단말기가 자동으로 시스템에 접근되는 권한을 박탈하고 원격으로 단말기에 저장되어있는 콘텐츠를 강제 삭제하고 단말기를 공장 초기화시켜서 기기 사용을 불가능하게 하도

<표 5> 안전한 스마트환경 관리 영역 권고

사용 영역	기능적 제한 조치
인증 도입	자체 도입한 PIN 입력 및 사용 단말기 식별로 자동 접근 방지
작업 단말기	개인이 사용하고 있는 단말기 사용을 중단하고 회사에서 지급한 최신의 노트북, 모바일 단말기 사용
	사용자 단말기에서 업무와 관련된 파일 복사, 및 개인 메일 전송 등의 행위를 무력화는 솔루션 탑재
	사용자 단말기 분실 시 강제로 콘텐츠 삭제, 공장 초기화 강행
작업 영역	업무용 데이터는 기기에 저장되지 않도록 사적/업무적 작업 영역을 완전 차단하여 분리하고, 완성된 업무에 대해서는 서버로 암호화 하여 전송
솔루션 탐지	IDS 방화벽 솔루션을 탑재하여 사전에 허가되지 않는 IP를 추적하여 내부 유출에 대한 네트워크 기술적 관리 영역 확대

록 강제 조치해야 한다. 또한 이용에 있어서 사용자 업무 보안 영역에 따라 레벨 등급을 부여하는 방법인데 레벨이 낮은 등급의 스마트워크 이용자에게는 외부 인터넷 망의 접속을 허락하지 않도록 방법을 변경하는 것도 좋다. 만약, 재택근무자들이 부득이하게 외부 망을 통해서 서버에 접근하여 업무적 작업을 진행하고자 한다면 자체에서 개발한 인증 PIN을 도입하여 스마트워크 환경에 이용하는 작업자인지를 확인한다든가, 회사 시스템에 등록된 단말기 인지를 철저하게 검증하는 것이 좋다. 또한 스마트워크 환경을 지원하는 작업 환경에 대한 IP를 실시간으로 추적·감시하는 네트워크 보안을 강화하여 인·허가되지 않는 네트워크 IP에 대해 사전에 이를 탐지하는 IDS 솔루션을 탑재하여 문서 유출 방지 및 허가되지 않는 사용자에 대한 시스템 접속을 사전에 차단하는 것도 좋은 방법으로 판단된다. 이와 관련하여 스마트 환경 구축을 고려하는 스타트업 회사나 글로별 규모로 회사 업무적 영역을 확장할 계획이 있는 경우에는 적극적으로 외부 망에 접속을 열어두는 것보다는 외부망 접속을 제한 한 후, VPN과 같은 자체 사설망을 구축하여 안전한 스마트 워크 환경에 접속하여 업무를 할 수 있도록 적극 권장한다. 다음은 안전하게 스마트환경의 사용 영역에 대한 기능적 제한을 표로 정리하였다.

Ⅴ. 결론

본 논문에서 살펴본 바와 같이 스마트폰에서 사용자가 필요한 앱 사용 시 대부분의 앱은 자동적으로 개인정보를 수집하고 있는 문제점을 안고 있다. 또한 해당 서비스 앱 수집 기관에서는 해당 서비스가 끝나면 서버에서 자동 삭제를 해야 하는 개인정보 관리에 대한 의무를 져버리고 영구적/반영구적으로 고객의 개인정보를 보관하여 활용하고 있는 것이 문제점으로 지적되었다.

본 논문 연구를 통해 모바일 앱을 사용 시 개인정보 유출이라는 위험을 초래할 수 있는 다양한 개인정보 침해 위협을 분석함으로 써 예방과 동시에 모바일 사용자들의 신뢰를 떨어뜨리는 불안 요소를 제거함과 동시에 심리적인 안정을 찾아 줌으로써 스마트폰 앱 사용을 보다 안전하게 실생활에서 사용할 수 있는 개선 방안을 제시하였다. 특히, 사용자 스마트 폰 금융 앱을 안정적으로 사용하기 위해서는 IMME 식별번호 등록 사용 권장과 앱을 통한 사용자 계정 및 비밀번호에 대한 텍스트 입력 시 난독 처리되는 기술적 도입과 사용자 스마트폰에 대한 행태 처리를 사용자 기기에서 인식하여 사용자가 스마트폰 이용 상황을 인지하여 스마트폰을 잡았을 때의 평상시 각도, 스마트폰을 잡는 압력의 세기, 손가락 길이 등을 인공지능으로 분석하여 이를 인지 상황에 대한 패턴으로 만드는 후, 암호학적으로 이용하는 것이다. 즉, 평상시 이용자의 사용 습관과 다른 행태의 이상 징후에 대한

모션을 감지하는 기술적 방안을 제시하여 모바일 앱 사고 위협으로 부터 국내 환경에 맞게 적절한 예방 방안을 제시하여 인터넷뱅크의 간소화 문제로 위험해 질 수 있는 다양한 스마트폰 뱅킹 앱 서비스의 위험 상황에 대한 예방을 검토하였다. 또한, 사용자의 위치적 정보를 제한하는 부분에 있어서도 현재 일부 시행되고는 있지만 많은 업체들이 규칙을 위반하고 서라도 개인의 위치 정보가 수집되는 논란에 대해서도 본 논문을 통해 길 찾기, 배달 앱, 교통정보 이용 시 발생한 플랫폼 회사의 위치정보 서비스는 사용자가 이용한 직후 서버로부터 곧바로 삭제해야 되는 강력한 개인정보 정책 마련을 법적인 제도 면에서 정부기관 및 각 부처.에서 실행해 줄 것을 강조하였다. 마지막으로 이동수단 발전과 함께 작업 영역이 스마트 환경으로 점차 변모되면서 회사의 업무적인 영역이 사적인 영역과 구분 없이 이용되다 보니 알게 모르게 회사의 중대한 기밀문서가 개인의 전자적 메일 및 휴대장치에 전송되어 문제가 될 수 있는 부분이 초래되기도 하였다. 이에 본 논문에서는 재택 업무를 진행되는 부분에 있어서도 업무적 영역과 사적인 영역을 구분토록 하여 회사에서는 반드시 보안 솔루션이 탑재된 노트북, 이동 단말기를 제공하여 업무적으로 활용하도록 권고하였고, 등록된 위치 한계를 벗어날 경우에는 IP를 탐지하여 IDS 솔루션에 의해 서버 접속이 차단 되게 하는 등 안정성을 고려하는 방안도 함께 제시하였다.

끝으로 많은 스마트폰 사용자들이 실생활에서 다양하고 편리한 앱을 보다 안전하고 유용하게 이용하기 위해서는 다양한 카테고리 앱 장르에 강력한 보안 탑재와 이용자들의 안전한 스마트폰 사용에 대한 보안 의식이 무엇보다 중요하며 개인정보 유출로 인해서 발생할 수 있는 금융적 피해 및 위험한 요소 등에 대한 예방의식이 무엇보다 신장되어야 하고 고취되어야 할 매우 중요한 시점이라고 여겨진다.

참고문헌

[1] 박병우 · 장석은 · 이은경 · 이상준, “BYOD 환경의 모바일 오피스 보안 위협에 대한 개인정보 보안 방안,” 한국컴퓨터정보학회 동계학술대회, 제26권, 제1호, 2018, pp.167.

[2] 서이종 · 김수종, "스마트폰 애플리케이션을 통한 재현적 개인정보 누적성과 개인정보보호 정책적 함의," 한국정보사회학회, 제16권, 제1호, 2015, pp.3.

[3] Bansook Nam, "모바일 어플리케이션이란," https://medium.com/@bansooknam/%EB%AA%A8%EB%B0%94%EC%9D%BC-%EC%96%B4%ED%94%8C%EB%A6%AC%EC%BC%80%EC%9D%B4%EC%85%98%EC%9D%B4%EB%9E%80-443de3b201fb, Jun. 2018.

[4] 한겨레신문, “국내 최장 시간 이용 앱, ” http://www.hani.co.kr/arti/economy/it/909212.html, Sep. 2019.

[5] I tworld, “소셜미디어 베스트 앱 Top 5,” http://www.itworld.co.kr/print/88218

[6] 이찬희 · 김인석, “모바일커머스에서 보안과 개인정보의 요성에 한 연구,” 한국정보학회논문지, 제.27호, 제4호, 2017, pp.914.

[7] snews, “모바일 뱅킹 앱,” http://www.consumernews.co.kr/?mod=news&act=articleView&idxno=528523, Nov, 2018.

[8] 한승진 · 김낙현 · 김재성, “모바일 장치에서 바이오인식을 이용한 개인정보 등록,” 콘텐츠학회추계학술대회, 2014, pp.49.

[9] 안수현, "배달앱 서비스 산업을 둘러싼 법적 이슈와 과제," 경제법연구회, 제15권, 제2호, 2016, pp.51.

[10] gangjung1, “배달앱 Top 전격 비교,”

https://gangjung1.tistory.com/47
[11] ITworld, “명함 관리 앱,” http://www.itworld.co.kr/t/62085/%EC%9B%B9%EC%84%9C%EB%B9%84%EC%8A%A4/110083#csidx5cd2d2f6c52ac0cbf5c0f84cfd39bc4, Jun. 2018.
[12] 함유정 · 이형우, “안드로이드 모바일 정상 및 악성 앱 시스템 콜 이벤트 패턴 분석을 통한 유사도 추출 기법,” 한국인터넷정보학회, 제14권, 제6호, 2013, pp.126.
[13] 이기수, “최근 보이스피싱의 범죄수법 동향과 법적 대응방안,” 범죄수사학연구회, 제4권 제2호, 2018, pp.5.
[14] Cyber Security, “모바일 보안 위협 및 대응방안,“ https://sudeky.tistory.com/28?category=868679, May. 2019.
[15] 김정덕 · 임세현, “모바일 뱅킹 이용자의 개인정보 유출사고 인지가 개인정보리 수행동에 미치는 영향에 관한 사전 연구,” 정보보호학회, 제26권, 제3호, 2016, pp.739.
[16] 최희식 · 조양현 · 김정숙, "위치기반 서비스에 따른 개인정보보안 취약점의 사례분석," 디지털산업정보학회 논문지, 제10권, 제3호, 2014, pp.165~pp.166.
[17] 위치정보지원센터, “위치기반서비스사업,” https://www.lbsc.kr/front/content/contentViewer.do?contentId=CONTENT_0000081
[18] news1, “배달통 앱,” http://news1.kr/articles/?2794566, Oct, 2016
[19] 박용준 · 이윤정, “모바일 오피스 개인정보 보호 방안에 대한 연구,” 한국멀티미디어학회 논문지, 제18권, 제2호, 2015, pp.181.
[20] 스마트워크, “스마트워크 개념,” http://worksmart.or.kr/smartwork/swIntroduce.do;jsessionid=1D9EDEC377093C68D4FD44693E67CED3
[21] 박진성 · 강인양 · 한필구 · 전병호, "금융 MVNO 환경에서의 소비자의 모바일지급결제서비스 이용의도," 디지털산업정보학회 논문지, 제8권, 제2호, 2012, pp.217.
[22] 이클루시큐리티, “난독화와 코드 가상화,” hhttp://www.igloosec.co.kr, Dec. 2019.

■ 저자소개 ■

최 희 식
Choi Heesik

2008년 9월~현재 삼육대학교 컴퓨터공학부 외래교수
2002년 2월 숭실대학교 컴퓨터학과(공학박사)
2006년 2월 숭실대학교 컴퓨터공학과 (공학석사)

관심분야 : 정보보안, 클라우딩컴퓨터, IoT, 핀테크 금융보안
E-mail : dali3054@ssu.ac.kr

조 양 현
Cho Yanghyun

1997년 9월~현재 삼육대학교 컴퓨터공학부 교수
2011년 2월 광운대학교 전자통신학과 (공학박사)
1985년 2월 광운대학교 전자통신학과 (공학석사)
1982년 2월 광운대학교 전자통신학과(공학사)

관심분야 : 컴퓨터네트워크, 통신망(BcN), GMPLS
E-mail : yhcho@syu.ac.kr

논문접수일 : 2019년 11월 25일
수 정 일 : 2019년 12월 10일
수 정 일(2차) : 2019년 12월 28일
수 정 일(3차) : 2020년 1월 22일
수 정 일(4차) : 2020년 2월 17일
게재확정일 : 2020년 3월 9일