감지설정기능을 적용한 스미싱 차단앱의 동적 평가방법에 관한 연구

김 장 일* · 김 명 관** · 권 영 만*** · 정 용 규****

목 차

요약

모바일 기기의 발달은 삶의 여유를 가지도록 만들었지만 그 반대편에서는 이를 금융범죄의 대상으로 간주하고 공격하는 세력들이 나타나게 되었다. 스마트폰을 대상으로 하는 범죄 중에서 금융관련 범죄는 스미싱, 피싱, 파밍, 보이스 피싱 등이 있으며, 특히 모바일의 특성상 문자메시지를 이용한 스미싱이 많이 증가되고 있는 현상이다. 스미싱은 스마트폰 사용자가 급증해 짐으로 인하여 발생하는 신종범죄로서, 그들의 범죄방식도 기존의 사기행위에서 벗어나 악성 앱을 제작하는 등 그 수법이 고도화되어가고 있으며, 특히 관련법의 허점을 이용하기 때문에 외국서버를 이용하는 등의 방법을 통하여 발생시키고 있다. 스미싱 공격으로부터 안전하게 개인과 기업 및 국가의 자산이 보호되기 위해서는 사후적인 대응보다는 사전적인 예진이 더욱 중요하다. 이를 위해서는 스미싱 공격을 사전에 감지하고 차단할 수 있는 프로그램을 개발하고 배포하는 것이 필요하다. 이에 본 논문에서는 현재 배포되고 있는 차단앱의 종류와 차단과정을 조사하고 감지설정을 적용한 차단앱의 평가방법을 제시한다.

표제어: 모바일, 스미싱, 금융범죄, 차단앱, 문자메시지

접수일(2015년 8월 11일), 수정일(1차: 2015년 9월 23일), 게재확정일(2015년 9월 23일)

* ㈜디플렛폼 연구소장, gold@d-platform.com
** 을지대학교 의료IT마케팅학과, binsum@eulji.ac.kr
*** 을지대학교 의료IT마케팅학과, ymkwon@eulji.ac.kr
**** 교신저자, 을지대학교 의료IT마케팅학과, ygjung@eulji.ac.kr

1. 서론

모바일 기기의 발달은 필연적으로 모바일 기기를 활용한 범죄의 증가를 불러왔다. 정보통신기기로서 모바일 기기는 2000년대 이전의 개인용 PC를 대체하여 다양하게 진화되었다. 특히 통신기기로서의 모바일 기기는 스마트폰으로 진화하면서 범죄의 대상으로 부각되었다. 과거 2G 휴대폰에 대한 모발일 범죄는 있었지만 지능적이지 못하고 첨단화되지도 못하였다. 그렇지만 스마트폰으로 변화하면서 개인용 PC와 동일한 형태의 공격이 가능해지면서 기존 사이버 공격자(범죄자)들의 공격 대상이 되었다[5].

모바일 기기는 일반적으로 휴대용 정보통신기기를 의미하며, 휴대용 기기, 모바일 디바이스(mobile device)라는 용어도 통용된다. 모바일 기기의 종류는 모바일 컴퓨터, PDA/EDA, 그래핑 계산기(graphing calcaulator), 휴대용 게임기, 디지털 카메라, 디지털 비디오 카메라, 포터블 미디어 플레이어, 이북(e-book) 리더, 휴대 전화, 무선호출기, 개인 내비게이션 장치(PND) 등이 있다. 최근 모바일 기기는 정보통신기술의 발달로 스마트폰을 대표적으로 의미하고 있다. 즉, 스마트폰이 모바일 기기 대부분의 기능을 내장하고 있기 때문에 모바일 기기를 스마트폰으로 인식하고 있기도 하다.

구체적으로 스미싱 범죄 발생 이유에 대해 나열해 본다면, 첫째, 스마트폰 사용자들의 급격한 증가에서 찾을 수 있다.사용자가 증가한 만큼 피해자 역시도 늘어날 수 밖에 없는 것이다. 둘째, 출처가 불분명한 사이트에서 앱(App)을 다운받으면서 악성 앱이 함께 다운로드 되는 것을 들 수 있다. 셋째, 각종 개인정보(주민번호, 핸드폰번호 등)유출로 인해 사생활 정보가 노출되면서 각종 맞춤식 스팸 문자를 수신하여 자기도 모르게 문자에 포함된 URL주소를 클릭하여 악성코드가 다운로드 되는 것이다. 넷째, 온라인 게임사의 게임 아이템의 환금성으로 인해 게임사를 통한 환전이 범행에 사용되는 경우이다. 다섯째, 점점 지능화되어 가는 악성 코드의 발전으로 인해 문자에 포함되어 있는 URL 주소를 클릭하게 되면 당사자뿐만 아니라 그 스마트폰 속에 저장된 지인들에게도 스미싱 문자가 발송되는 경우도 있어 피해가 더욱 확산되고 있다. 마지막으로 제일 큰 문제는 이러한 범죄에 대해서 아직도 스마트폰 사용자들이 인지하지 못하는 경우가 적지 않다는 사실이 피해 발생의 원인이 될 수 있겠다.

2. 악성 앱 형태와 유포 방법

안드로이드 악성 애플리케이션은 크게 정상적인 애플리케이션을 사칭하여 제작된 경우와 악성 행위를 숨기고 제작된 경우로 나누어 볼 수 있다[1].

2.1 정상적인 애플리케이션을 사칭하여 제작된 경우

가장 일반적인 형태로 스마트폰 테마, 금융, 게임 관련 등 사용자가 이용할법한 애플리케이션을 사칭하고 있다. 공격자는 정상적인 애플리케이션(각종 스마트폰 뱅킹 서비스)과 겉으로 보았을 때 유사하게 애플리케이션을 새로 제작하고 이 안에 과금 서비스, 개인정보 유출 등의 악성행위를 추가하고 있다.

또한 공격자는 기존의 정상 애플리케이션 APK (Android Application Package) 파일을 분석하여 여기에 악성코드를 추가한 후 리 패키징 해서 새로 만든 APK 파일을 유포하기도 한다. 이때 리 패키징 과정에서는 암호화 서명 키 값 파일(keystore)과 패스워드가 요구되는데, 이 키 값이 애플리케이션 최초 제작자의 것과 일치(서명 파일 탈취 등의 방법을 통해)한다면 업데이트를 통해 기존의 애플리케이션을 악성 애플리케이션으로 대체할 수 있다.

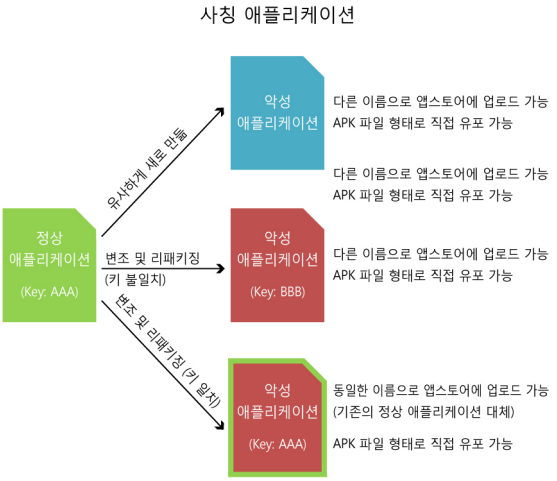


그림 1. 정상적인 애플리케이션 사칭하여 제작하는 경우
Fig. 1. Case of Impersonating Normal Application

2.2 악성행위를 숨기고 제작된 경우

공격자는 스마트폰 테마, 게임, 유틸리티 등 겉으로 보이는 기능 안에 악성코드를 숨겨놓고 이를 APK 파일로 온라인상에 직접 배포하거나 안드로이드 앱 스토어(주로 애플리케이션 보안검증이 허술한 서드파티 앱 스토어)에 등록한다.

대부분의 경우 사용자가 기대하는 기능을 제대로 수행하지 못하며, 접속 장애가 발생하였다고 가짜 에러 메시지를 띄우거나 아무것도 실행되지 않은 것처럼 위장하는 형태이다.

위와 같은 안드로이드 악성코드(악성 애플리케이션)가 주로 유포되는 경로는 ① 앱 스토어를 통한 경우와 ② 애플리케이션 파일(APK 파일)을 다운받아 설치하는 경우로 나눠 볼 수 있다.

① '구글플레이'나 서드파티 앱 스토어를 통한 경우

안드로이드는 서드파티 앱 스토어 덕분에 iOS나 다른 모바일 플랫폼보다 애플리케이션 시장이 훨씬 넓게 만들어져 있고, 또한 이를 통해 악성 애플리케이션이 주로 유포되고 있다. 특히 중국 앱 스토어에서 가장 많은 악성 애플리케이션이 유포되고 있다. 구글 공식 앱 스토어인 '구글플레이'에서도 나름대로 악성코드 탐지 기능을 추가하며 보안을 강화하고 있지만, 여전히 많은 악성 애플리케이션이 유통되고 있는 상황이다.

② APK 파일을 다운받아 설치하는 경우

안드로이드 애플리케이션은 APK 파일을 직접 다운받아 설치하는 것으로도 가능하다. 악성 APK 파일은 사용자가 특정 링크를 클릭할 때 [*.APK] 파일을 다운로드하는 방식으로 유포되는데, 이러한 링크는 스팸메일, SNS, 불법 도박 및 성인 사이트, 그리고 스미싱 등을 통해 주로 연결된다.

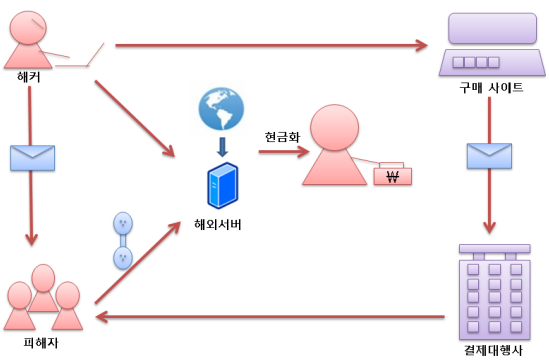
특히, SMS을 통한 스미싱은 모바일 청첩장, 택배배송, 불법 주차, 법원 출두 안내 등의 문구를 이용해 이제는 더 이상 대놓고 스팸메시지가 아닌 경우가 많아졌고, 최근에는 유출된 개인정보를 이용하여 000씨 등의 문구를 삽입해 사용자로 하여금 더 많이 악성 링크를 클릭하도록 유도 하고 있다.

3. 스미싱 공격과 차단과정

스미싱은 스마트폰 사용자가 급증함으로 인하여 발생하는 신종범죄로서, 그들의 범죄방식도 기존의 사기행위에서 벗어나 악성 앱을 제작하는 등 그 수법이 고도화되어가고 있으며, 관련법의 허점을 이용하기 때문에 외국서버를 이용하는 등의 방법을 통하여 발생시키고 있다. 스미싱의 발생구조를 살펴보면 아래 그림에서 나타난 바와 같이 악성 앱 제작자가 사전 수집한 개인정보를 기반으로 특정 사용자들에게 악성 앱 설치용 문자메시지 발송 → 이용자가 무심코 문자메시지 속 단축 URL을 클릭해 앱을 설치하면서 감염→ 악성 앱에 감염된 이용자가 단말기에서 정보를 수집해 해외서버로 전송 → 게임사이트 등 각종 인터넷 구매사이트 등에서 소액결제 서비스 진행 → 구매사이트에서 결제대행사 등을 통해 본인인증용 승인 문자번호를 사용자 휴대폰으로 발송 →

이미 설치된 악성 앱에 의해 사용자 휴대폰은 수신된 문자번호가 보이지 않도록 조작됨 → 악성 앱이 승인번호 문자메시지를 해외 서버로 몰래 전송 → 서버에 수집된 승인 번호를 가로채 정상적 구매절차를 수행 → 적립된 사이버머니 등을 불법적으로 현금화해 부당이득을 취한다.

모든 사기범죄가 그러하듯 본인의 의사와 상관없이 범죄가 이루어지지만, 스미싱의 발생구조에서 나타난 것과 같이 스미싱의 경우 피해자의 의사 혹은 기망하는 기술의 수준이 높고 피해자가 피해를 예방할 수 있는 기회가 다른 사기범죄에 비하여 적은 특성을 가지고 있다. 그러한 이유는 피해를 입힐 수 있는 자료유출과정에서 피해자가 개입할 상황을 차단하기 때문에 그러한 성향이 더욱 강하다.



출처: 신재헌, 김상운(2014).

그림 2. 스미싱 발생 구조

Fig. 2. Generation Structure of SMS Phishing

스팸 및 스미싱에 이용되는 SMS발송경로 유형으로는 다음 그림과 같이 통신사에서 제공하는 웹페이지를 통해 개별 및 대량전송을 하는 SMS Web 서비스, 고객 자체 서버 및 DB프로그램을 이용하여 실시간으로 개별 및 대량 전송을 하는 SMS 서버연동 서비스, 통신사에서 제공하는 메신저 프로그램을 이용하여 전송하는 SMS 메신저 서비스, 이통사 휴대전화를 이용하여 개인이 직접 발송하는 유형이 있다. SMS Web 서비스에는 웹메시징 서비스, SMS 서버연동 서비스에는 C2P나 BIZ-SMS가 있으며 앞에서 언급했듯이 이중 C2P(대량 문자발송 서비스)를 가장 많이 이용되는 것으로 조사 되었다.

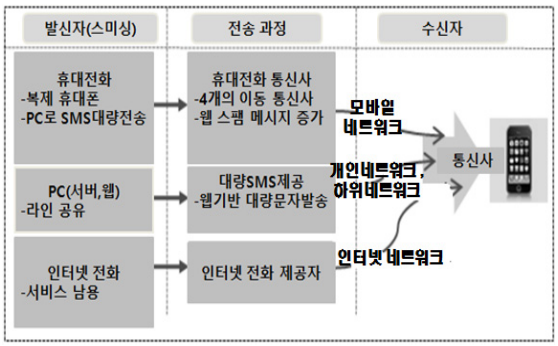


그림 3. 스미싱 SMS 송신 과정

Fig. 3. Sending Procedure of SMS Phishing

다음은 스미싱을 이용한 해킹 공격의 예이다. 스미싱을 이용한 안전결제 해킹공격 과정을 분석한 것으로 스미싱 이용한 해킹 공격 분석의 예(안전결제해킹공격)이다.

스미싱 공격은 문자 메세지 내 인터넷 주소를 클릭하게 하여 악성코드를 자동 설치하고, 해커에게 소액결제 인증번호를 전송함으로써 해커가 게임 아이템 및 사이버머니를 결제할 수 있다. 그로 인해 소액 결제 대금이 청구되는 것이다. 위 그림은 androAPKinfo.py를 이용하여 smishing.APK의 API권한을 살펴본 모습이다.

4. 스미싱 차단앱 평가 시스템

스미싱 차단앱 평가 시스템의 작동 흐름은 Database에 기록된 스미싱 문자를 해당 App에 검증 요청하면 신규 상태 처리(NEW) 된다.

NEW 처리된 문자를 찾아 전송 전에 전송시도상태 처리(SENDING) 상태로 변경 후 Emulator에 문자를 전송한다. 전송이 제대로 이루어지지 않을 경우 SENT_FAILED 처리를 하며 만약 정상 수신 되었을 경우 전송 완료 상태 처리(SEND)를 한다.

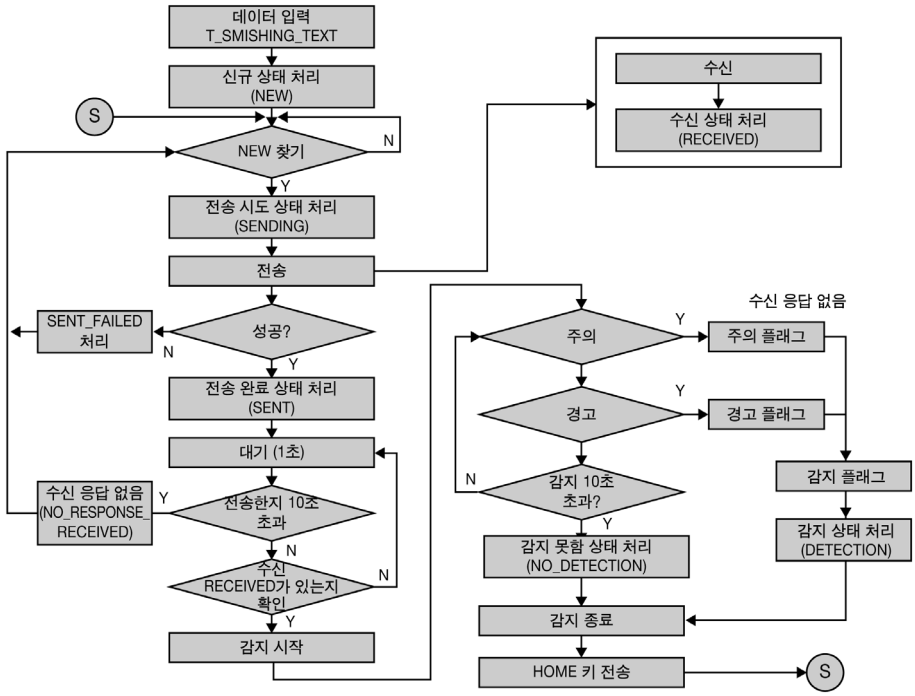


그림 4. 스미싱 차단 APP 작동 흐름도
Fig. 4. Flow Chart of SMS Phishing Blocking App

Emulator에 문자가 수신되면 설치된 SMS Receiver Checker App 이 동작하여 수신 상태 처리(RECEIVED)를 하게 되며 감지를 시작하게 된다. Emulator에 이미 설정된 주의, 경고 화면 상태와 같은가를 비교하여 감지상태(DETECTION) 처리를 하게 된다. 특정 시간이 지나도 감지를 못할 경우 감지 못함 상태 처리(NO_DETECTION)을 하게 되며 다음 검사를 위해 Emulator에 Home 키 정보를 전송 후 다음 SMS 문자를 처리하기 위한 NEW를 찾는 부분으로 이동하게 된다.

다음은 진단 할 CSV 파일을 추가하는 화면이다.

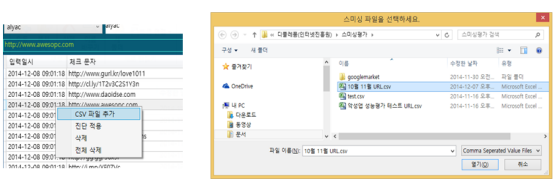


그림 5. 진단 CSV 파일 추가
Fig. 5. Additional Diagnostic CSV File

진단할 SMS 문자 리스트에서 오른쪽 마우스 클릭하면 Context 메뉴가 나타나며 CSV 파일 추가를 선택한 후 진단할 SMS 문자가 담겨져 있는 CSV 형태로 되어있는 파일을 선택하면 Database에 저장한다. 이때 이미 저장된 SMS 문자가 있으면 중복 오류 메시지가 표시되고 진행하지 않는다.

5. 감지설정기능 적용 및 평가

스미싱 차단 APP 평가 시스템은 최종적으로 각각의 APP에 전송된 스미싱 URL/APK에 대하여 악성 유무 및 위험성을 판발하고 있는지를 확인해 주게 된다. 즉, 평가 대상 스미싱 차단 APP이 정상적으로 작동을 하고 있는지를 확인하는 것이다. 최종적으로 개발한 시스템이 출력해주는 감지 설정 및 이를 실시간으로 출력해주는 장면은 다음과 같다.

그림 6. 감지 설정 및 라이브 화면
Fig. 6. Detection Settings and Live Screen

진단을 시작하기 전에 App들이 진단 표시되는 화면의 일부 영역을 지정 저장 하면, 진단 동작시에 화면 일치 여부를 통해 감지 상태를 처리하게 된다. 실제 동작하고 있는 내용이 에뮬레이터의 화면을 통해 볼 수 있으므로 보다 직관적이게 확인 할 수 있다. 최종적으로 출력해주는 화면에서 '스미싱 의심 메시지가 도착'하였음을 알려주고, 이를 확인하고 정상적으로 스미싱 의심 문자로 판별하고 있음을 보여주고 있다.

6. 결론

스미싱 공격으로부터 안전하게 개인과 기업 및 국가의 자산이 보호되기 위해서는 사후적인 대응보다는 사전적인 예진이 더욱 중요하다. 이를 위해서는 스미싱 공격을 사전에 감지하고 차단할 수 있는 프로그램을 개발하고 배포하는 것이 필요하다. 또한 현재 전 세계 악성코드 유형은 해마다 증가하고 있는데, 이들 중 대부분은 안드로이드 플랫폼 기반 악성코드이다. 안드로이드 플랫폼 기반 악성 코드가 많은 것은 다른 모바일운영체제보다 높은 시장점유율과 악성 APP제작 및 유포가 용이하기 때문이다. 또한 각각의 APP이 APK 파일 형태로 되어 있어서, 이 APK 파일을 다운로드를 통하여 모바일 기기에 저장하여 실행하기만 하면 쉽게 해당 Application이 설치가 되며, 많은 앱스토어에서 강력한 검증절차 없이 등록 가능하도록 되어 있다. 즉, 이용자들이 편리하고 무료로 사용할 수 있도록 제공된 서비스가 악성 금융범죄의 표적이 된 것이다. 이에 현재 배포되고 있는 차단앱의 종류와 차단 과정을 조사하고 감지설정을 적용한 차단앱의 평가방법을 제시하였다.

참 고 문 헌

〔국내 문헌〕

[1] 공간 POC (2013), 안드로이드 악성코드 분석 현황, 주간정보분석.
[2] 김형휘 (2014), 안드로이드 악성 애플리케이션 차단 서비스, 고려대학교 공학대학원 석사학위논문.
[3] 박상호, 이준형 (2013), 인증 및 사전검증을 통한 스미싱 방지 시스템 제안, 정보보호학회지, 23(6), 5-12.
[4] 박인우 (2014), 스마트폰에서 Smishing 해킹과 침해사고 Forensic 분석, 호서대학교 벤처전문대학원 석사학위논문.
[5] 신재헌, 김상운 (2014), 모바일 범죄의 특성과 예방에 관한 연구, 경찰논총, 9(1), 127-143.

김 장 일 (Jang Il Kim)

순천대학교 물리학과에서 학사를 취득하였고, 을지대학교 의료IT마케팅학과 대학원에서 석사를 취득하였다. 현재는 주식회사 디플랫폼 부설 연구소장으로 재직하고 있으며, KISA 피싱센터 자문 컨설턴트로 활동 중이다. 보안과 관련한 정책과 기술이 관심분야이며, 특히 사이버블랙박스 구현, 스미싱 차단앱 평가시스템 등 보안과 관련한 시스템 구현업무에 참여하고 있다.

김 명 관 (Myung Gwan Kim)

숭실대학교에서 학사, 석사, 박사학위를 취득하였고 현재 을지대학교 의료IT마케팅학과 교수로 재직하고 있으며, 한국전자통신연구원 자연어처리연구실 UI 개발팀장을 역임하였으며, 현재 중기청 정보화경영원 IMS 위원, 한국 직업 능력 개발원 e-Training 심사위원을 역임하고 있다. 2차원 바코드 시스템개발, 멀티미디어 채팅프로그램 개발, 멀티미디어 정보검색 시스템 개발, 계몽사 영상정보검색 시스템 개발에 관심이 많다.

권 영 만 (Young Man Kwon)

KAIST, 광운대학교에서 각각 석사, 박사학위를 취득하였고 현재 을지대학교 의료IT마케팅학과 교수로 재직하고 있으며, 듀폰코리아 포토마스크(주) CAD실 실장, LG반도체 ASIC 개발팀 팀장을 역임한바 있다. 현재 한국 직업 능력 개발원 e-Training 심사위원으로 있다. 온라인 미디플레이어 시스템 개발, 유통관리 인트라넷 개발, 기업인트라넷을 위한 멀티자료실 개발을 한바 있다.

정 용 규 (Yong Gyu Jung)

서울대학교, 연세대학교, 경기대학교에서 각각 학사, 석사, 박사학위를 취득하였고, 현재 을지대학교 의료IT마케팅학과 교수로 재직 중이다. ISO, UN의 전자거래분야 한국대표위원으로 활동하였으며, 의료정보, 전자무역, 물류유통의 국제표준화에 관심이 많다. 특히 Semantic Web, Process Modelling, ebXML 등의 표준 기술의 비즈니스 적용에 관심이 많다.

Dynamic Evaluation Methods for SMS Phishing Blocking App Based on Detection Setup Function

Jang Il Kim* · Myung Gwan Kim** · Young Man Kwon*** · Yong Gyu Jung****

ABSTRACT

Although the development of mobile devices are made us a free life, they were displayed the subject of this financial crime and attacking forces in the other side. Among finance-related crime is become a serious crime that are targeting smartphones by SMS phishing, phishing, pharming, voice phishing etc. In particular, SMS phishing is increased according to phenomenon using the nature of a text message in the mobile. SMS phishing is become new crime due to the burden to the smartphone user. Their crime is also the advanced way from the existing fraud, such as making the malicious apps. Especially it generates loopholes in the law by a method such as using a foreign server.

For safe from SMS phishing attacks, proactive pre-diagnosis is even more important rather than post responses. It is necessary to deploy blocking programs for detecting SMS phishing attacks in advance to do this. In this paper we are investigating the process of block types and block apps that are currently deployed and presenting the evaluation of the application of the detection block setting app.

Keywords: Mobile, SMS Phishing, Financial Crimes, Blocking App, Text Message

* CIO, Research Institute, D-platform Co., Ltd., gold@d-platform.com
** Medical IT Marketing Department, Eulji University, binsum@eulji.ac.kr
*** Medical IT Marketing Department, Eulji University, ymkwon@eulji.ac.kr
**** Corresponding Author, Medical IT Marketing Department, Eulji University, ygjung@eulji.ac.kr