情 報 保 護 學 會 誌
第23卷 第4號, 2013. 8

스마트폰 신종 Phishing의 피해사례 및 대응방안 분석

양 준 근*, 하 기 웅**, 김 학 범***

요 약

최근 정보통신기술 분야의 최대 관심사는 스마트폰 분야이다. 이러한 흐름에 발맞추어 스마트폰에 관련된 다양한 기술이 점진적으로 발달하였고, 누구나 쉽게 스마트폰을 이용하여 증권 거래 및 인터넷 검색, 인터넷 뱅킹 등의 다양한 서비스를 이용하고 있다. 이렇게 우리 생활에 점차 밀접한 관계를 맺음에 따라 그와 관련된 신종 Phishing들이 등장하게 되어 피해가 속출하고 있다. 본 논문에서는 스마트폰 신종 Phishing이 쉽게 발생할 수 있는 개방형 OS 환경의 특징과 스마트폰 환경에 새롭게 등장한 Smishing의 정의와 피해사례, 그리고 QRishing의 정의를 기술한다. 또한, 신종 Phishing의 피해사례와 그에 대한 대응방안에 대해 기술한다.

Ⅰ. 서 론

스마트폰은 휴대폰(Mobile Phone)과 PDA(Personal Digital Assistant)의 장점을 결합한 것으로, 기존의 휴대폰과 달리 수백여 종의 다양한 어플리케이션을 사용자의 기호에 따라 설치하고 추가 또는 삭제할 수 있다는 장점을 가지고 있으며, 언제 어디서나 사용자가 원하는 정보를 검색할 수 있다는 편의성 때문에 점차적으로 사용자가 증가하고 있는 추세이다.[1]

한국 방송 통신 위원회에서 발간한 [표 1]의 통계자료에 따르면 이동통신 3사(SKT, LGU+, KT)의 스마트폰 가입자 수는 약 3300만 명이며, 앞으로 더 많은 가입자들을 유치할 수 있을 거라 전망하고 있다.[2]

스마트폰 사용자가 증가함에 따라 부정적인 면도 부각이 되기 시작했다. [그림 1]에서 볼 수 있듯이 스마트폰 악성코드 피해 또한 점차적으로 증가하고 있다.[3]

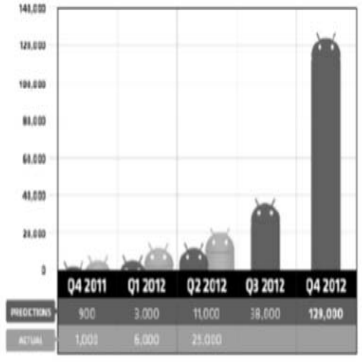
이러한 피해 사례들은 대체적으로 사회공학(Social Engineering)을 이용한 사례가 대다수이며, 개인정보 탈취 및 소액 결제 유도 등의 다양한 목적을 가지고 있다.

이 중 대표적인 사회공학 기법 중 하나인 피싱(Phishing)은 Private Data와 Fishing의 합성어로서 유명 기관을 사칭 또는 개인 정보 및 금융 정보를 수집하

〔표 1〕 국내 스마트폰 가입자 현황

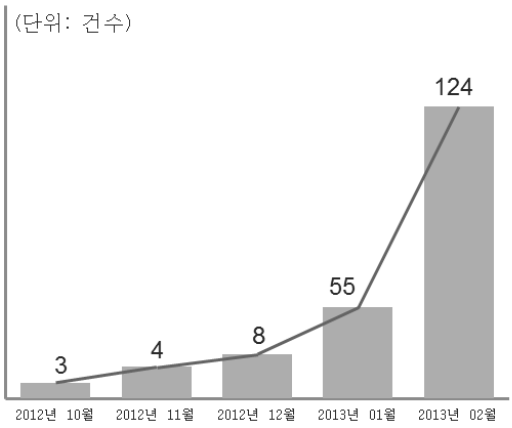
(단위: 만 명)

구분	2012.11	2012.12	2013.01
SKT	1,565	1,597	1,633
KT	1,006	1,025	1,053
LG U+	632	649	645
계	3,204	3,272	3,329

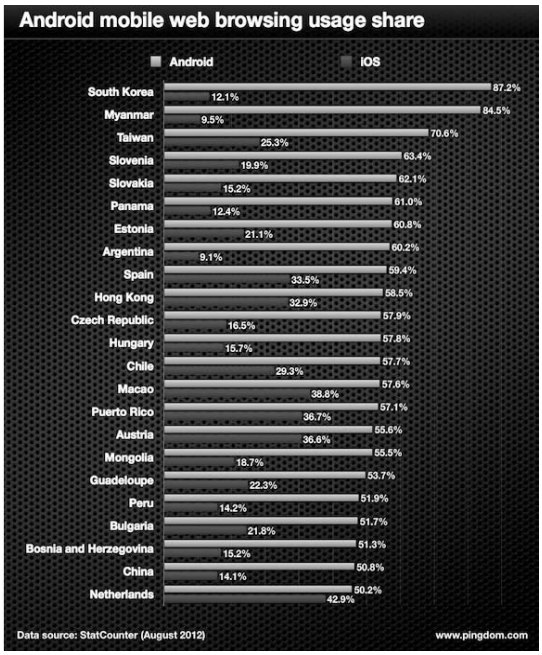


〔그림 1〕 모바일 악성 코드의 급증

* 동국대학교 국제정보대학원 정보보호학과 (junkune@gmail.com)
** 동국대학교 국제정보대학원 정보보호학과 (hkw342@naver.com)
*** 동국대학교 국제정보대학원 / ㈜이너버스 (khb0305@dongguk.edu)



〔그림 2〕 국내 모바일 악성 앱 신고 현황



〔그림 3〕 안드로이드 모바일 웹 브라우징 사용량

여 금전적인 이익을 노리는 사기 수법이다.

[그림 2]는 한국 인터넷 진흥원이 조사한 최근 국내 모바일 악성 앱 신고 현황이다.[4] 자료에 의하면 2012년 10월에는 피해가 3건으로 다소 적은 반면, 2013년 2월에는 124건으로 피해 신고 건수가 기하급수적으로 늘어났다. 따라서 악성 앱으로 인한 피해 사례는 앞으로도 지속적으로 늘어날 것으로 예상된다.

또한, 앞서 언급했던 스마트폰 악성코드 피해 사례들은 개방형 OS의 특징을 가지고 있는 안드로이드 환경에서 더 많이 발생하고 있다는 점에 주목할 만하다.

본 논문에서는 악성코드에 대한 취약점에 있어서 안드로이드와 iOS의 차이점, 스마트폰 환경에서 새롭게 등장한 신종 피싱의 유형, 각 피해와 대응방안에 대해서 설명한다. 그리고 마지막으로 결론과 향후방향에 대해서 기술한다.

Ⅱ. 스마트폰 OS의 특징

2.1 안드로이드

세계적인 통계회사 핑덤(Pingdom)이 조사한 [그림 3]의 '23개국 스마트폰 사용자들의 OS 종류에 따른 Web Browsing 사용률' 조사에 따르면 안드로이드의 사용률이 iOS의 사용률보다 압도적으로 우세함을 알 수가 있다.[5] 이러한 양상은 앞으로 꾸준히 지속 될 것이며, 전 세계적인 흐름으로 볼 수 있다.

안드로이드는 사용자의 편의성 및 다양성을 중시하는 OS로써, 프로그래밍 언어로 자바(Java)를 채택하고 있고 다양한 오픈 소스(Open Source)를 기반으로 하고 있어서 누구나 쉽게 자신의 앱(App)을 배포할 수 있다는 장점을 가지고 있다.

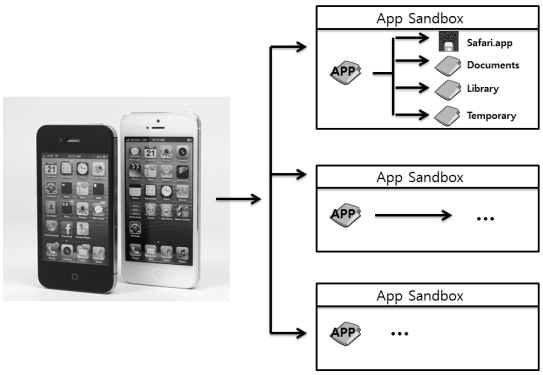
하지만 이러한 안드로이드의 특징을 악용하여 안드로이드의 배포 및 패치 등에 관련된 취약점과 사회공학을 혼합한 공격이 늘어나고 있는 추세이며, 그 피해 사례도 상당한 것으로 나타나고 있다.

2.2 iOS

반면에 iOS는 이러한 피해에 대하여 어느 정도 내성을 가지고 있다. 그 이유에는 두 가지가 있다.

하나는 앱에 바이러스 및 기타 원치 않는 기능이 포함될 가능성이 낮은 것이다. Apple사는 앱 다운로드 및 설치 과정을 '앱 스토어(App Store)'로 한정하고 등록 시 관련된 심사를 진행한다. 만약 악성코드가 포함되어 있더라도 높은 확률로 검출될 것이고, 혹시라도 발견되면 즉시 앱 스토어에서 퇴출된다.

다른 하나로는 바이러스 앱을 제공하기 어려운 iOS 구조를 들 수 있다. iOS용 앱은 [그림 4]와 같이 샌드박스(Sandbox) 환경에서 실행되기 때문에 하나의 앱이 사용하는 파일을 다른 앱에서 사용하는 경우 분명한 허



〔그림 4〕 iOS 환경에서 샌드박스의 적용

가가 필요하기 때문이다.[6][7]

Ⅲ. 신종 피싱의 등장 및 피해분석

3.1 Smishing

3.1.1 정의

스미싱(Smishing)은 SMS(Short Message Service)와 피싱의 합성어로서 새롭게 등장한 사회공학 기법 중 하나이다. 스미싱은 피해자들의 관심을 끌기 위해 공공기관 및 쿠폰발송 등의 내용을 가장한 SMS 메시지를 보내어, 모바일 사용자들의 개인정보 탈취 및 무단 소액결제를 이용한 금전적인 피해 등을 일으킨다.

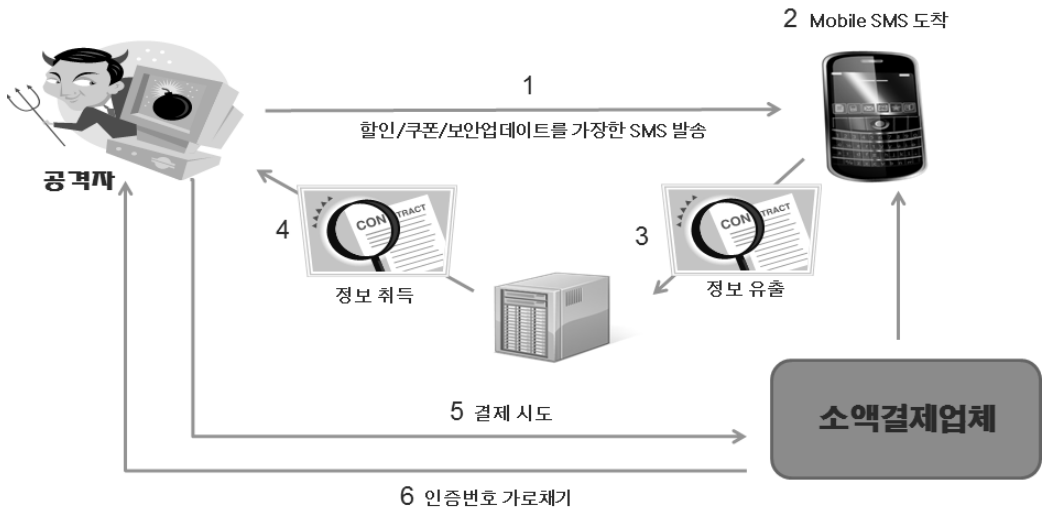
이러한 스미싱의 공격 방식은 첫째로 SMS에 URL을 첨부하여 접속을 유도하는 방식과 둘째로 SMS에 전화번호를 첨부하여 Calling을 유도하는 방식이 있다.

외국에서는 주로 전화번호를 첨부하는 Calling 방식을 이용한 피해 유형이 대부분이며 피해 사례는 아직 적은 편이다. 반면에 한국에서는 주로 URL을 첨부하는 방식을 이용한 유형이 대부분이다.

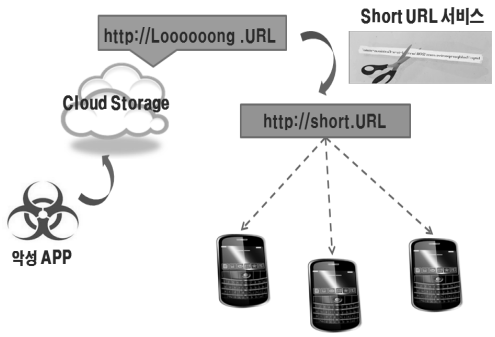
3.1.2 동작 절차

앞서 설명한 바와 같이 국내 스미싱 피해 사례들은 SMS에 URL을 첨부하는 방식을 사용하는 것이 주를 이룬다. 이러한 방식의 절차는 [그림 5]와 같다.

[그림 5]를 보면 먼저 공격자는 희생자에게 악성 앱을 다운로드 받을 수 있는 URL을 첨부한 SMS를 발송한다. 공격자는 희생자가 스마트폰에 전달된 SMS의 URL을 클릭하여 악성 앱을 다운 및 설치하도록 유도한다. 이렇게 설치된 악성 앱은 감염된 스마트폰의 여러 정보 및 SMS의 수신내용을 공격자에게 전달하며, 특정 SMS를 희생자가 보지 못하도록 차단한다. 공격자는 수집된 해당 스마트폰의 정보로 소액결제를 진행한다. 소액결제 업체는 결제요청을 받아 해당 스마트폰에 소액결제 인증문자를 발송하며 악성 앱은 이를 피해자가 보지 못하도록 차단하고 공격자에게만 인증메시지를 전달한다. 공격자는 탈취한 소액결제 인증번호를 입력하여



〔그림 5〕 스미싱의 동작 절차



〔그림 6〕 스미싱의 최근 공격 유형

감염된 스마트폰의 희생자 명의로 결제를 진행한다.

이와 같은 절차는 최근에 [그림 6]과 같이 클라우드 서비스(Cloud-Service) 환경과 단축 URL(Short-URL) 서비스를 이용하는 방식으로 좀 더 발전하였다.

공격자는 클라우드 서비스를 이용하여 악성 앱을 클라우드 스토리지에 업로드하는 용도로 사용하고 있다. 이는 서비스 사용자에게 종적을 쉽게 감출 수 있는 특징을 가지고 있기 때문에 공격자에게 저렴한 비용으로도 강력한 해킹을 시도할 수 있는 공간을 제공한다.[8]

공격자가 단축 URL 서비스를 이용하는 주된 이유는 URL을 메시지로 보낼 시 SMS의 최대 한계 크기인 80Bytes를 넘지 않고 보낼 수 있기 때문이다.

원래 단축 URL은 트위터(Twitter)의 용도로 개발된 것이다. 트위터의 경우 게시판에 입력할 수 있는 최대 크기가 140Bytes이기 때문에, 이러한 제약에서 자신이 가진 정보를 최대한 표시하기 위해 단축 URL이 파생되었다.

또한 단축 URL의 경우 [표 2]와 같이 동일한 주소를 나타내는 변칙적인 단축 URL을 제공하기 때문에 공격자는 계속하여 악성 앱의 단축 URL을 변경할 수 있다. 그리고 희생자가 직접 접속하기 전까지는 URL 제공자의 설명만을 믿고서 URL에 연결해야하는 맹점을 가지고 있기 때문에 공격자는 이 점을 악용한다. 단축 URL을 제공하는 대표적인 서비스 제공업체는 [표 3]과 같다.

〔표 2〕 단축 URL의 예

동국대학교(www.dongguk.edu)	
http://goo.gl/Ap8rN	http://goo.gl/1vRsn
http://goo.gl/VFnNW	http://goo.gl/7949L
http://goo.gl/nzjpj	http://goo.gl/LCTWS

〔표 3〕 단축 URL 서비스 제공업체

Short-URL 서비스 제공업체
TinyURL.com
shorl.com
notlong.com
google.com
bit.ly
urlshort.me

3.1.3 피해사례 분석

스미싱을 이용한 피해사례는 앞으로도 계속하여 증가할 것으로 예상되며 그 방식은 [그림 7]과 같이 점점 더 교묘해지고 다양화되고 있다.[9]

그와 관련된 몇 가지 사례들을 설명하자면, 먼저 금융기관 및 중요기관들을 사칭하는 유형이 있다. 스마트폰 보안 강화를 위해서 프로그램 설치를 기관들이 제안하는 것처럼 제안하는 형식이다. 다음으로 할인 쿠폰과 기프트콘(Giftcon) 등의 피해자들의 관심을 이끌어 낼 수 있는 문자를 보내어 쿠폰 및 경품 수령을 하도록 유도하는 방식이 있다. 이 외에도 동창회 및 결혼식 E-청첩장 등으로 유도를 하는 방식이 있으며, 소액결제 피해사례가 접수가 되었다는 등의 메시지로 피해자들의 불안감을 자극을 시키는 방식이 있다.

〔그림 7〕 스미싱의 일반적인 사례

경찰청이 조사한 바에 의하면 2013년 3월까지의 스미싱 휴대폰 소액결제 사기사건의 피해사례는 5천 여 건이며, 피해금액은 11억 원에 이른다. 하지만 게임업계에서는 피해 규모가 30억 원에 달하는 것으로 추정하고 있어 이 외에도 더 많은 피해사례가 있을 거라 예상되고 있다.[10]

3.2 QRishing

3.2.1 정의

크리싱(QRishing)이란 QR코드(Quick Response Code)와 피싱의 합성어로서 스미싱과 더불어 새롭게 등장하고 있는 사회공학 기법이다.

QR코드는 흑백 격자무늬 패턴으로 정보를 나타내는 매트릭스 형식의 바코드로, 기존 바코드가 용량 제한에 따라 가격과 상품명 등 한정된 정보만 담는 데 비해 QR코드는 넉넉한 용량을 강점으로 3차원적인 다양한 정보를 담을 수 있다. 또한 손쉽게 만들 수 있다는 이점을 가지고 있기 때문에, 현재 누구든지 쉽게 사용하고 있다. 스마트폰의 발달로 인하여 점차 QR코드에 대한 사용도가 높아짐에 따라, 기업에서는 이를 이용하여 다양

〔표 7〕 안드로이드 바코드 어플리케이션

순위	App	판매자	Auto Visit
1	Barcode Scanner	ZXing	n
2	ShopSavvy	ShopSavvy, Inc.	y
3	QuickMark Barcode Scanner	eBay, Inc.	n

〔표 6〕 iOS 바코드 어플리케이션

순위	App	판매자	Auto Visit
1	Barcode Scanner	Versolab	n
2	ShopSavvy	ShopSavvy, Inc.	y
3	RedLaser Barcode and QR Scanner	eBay, Inc.	n

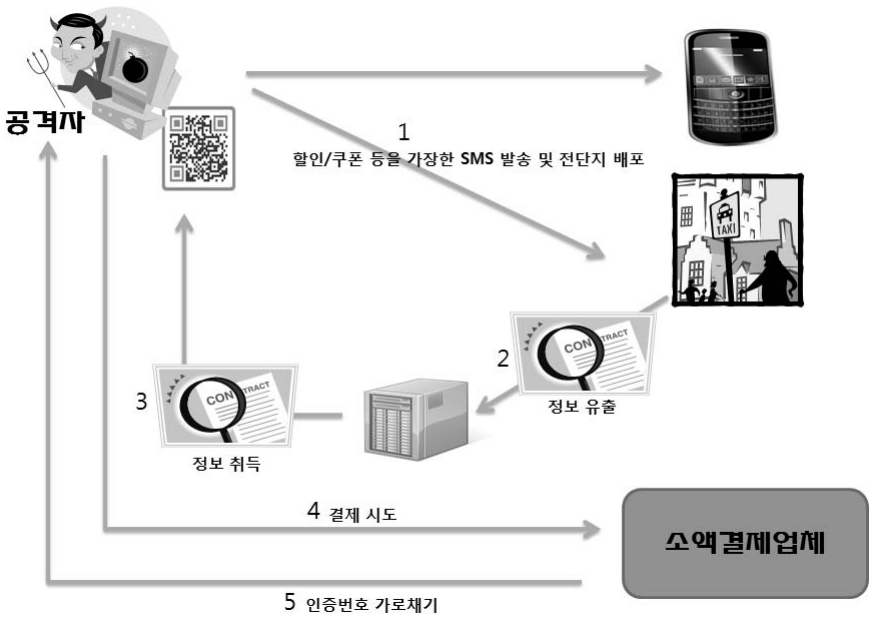
한 업무 마케팅의 용도로써 많이 사용하고 있으며 다양한 바코드 스캐너 어플리케이션이 등장하기 시작했다.[11]

크리싱은 이를 악용하여 악성 웹사이트로 접속을 유도하거나 유용한 프로그램으로 위장하여 악서 앱을 설치하도록 하여, 개인정보 및 금융정보들을 유출을 하도록 하는 공격을 일컫는다.[12]

3.2.2 동작 절차

크리싱의 동작 절차는 스미싱의 동작절차와 다소 유사하다. 여기서는 이러한 절차를 시나리오 형식으로 표현하겠다.

공격자는 클라우드 스토리지에 악성 사이트 또는 악성 프로그램을 저장하고서 원래의 URL을 단축 URL로



〔그림 8〕 크리싱의 동작 절차

변경한다. 이러한 서비스를 이용하여 단축 URL을 사용하는 이유는 필터링 및 백신에 걸리지 않기 위해서이다.

이렇게 생성된 단축 URL을 이용하여 QR코드를 생성한다. QR코드는 인터넷 서비스 및 어플리케이션으로 손쉽게 생성이 가능하다. 또한 이렇게 생성된 QR코드는 [그림 9]에서 볼 수 있듯이 같은 URL을 입력하여도 각각 다른 QR코드를 생성하기 때문에 추적이 어렵다.

생성된 QR코드는 SMS 및 전단지 등에 부착된 형태로 배포가 되며, QR코드를 스캔한 스마트폰 사용자들은 자신의 스마트폰에 악성 앱이 설치된다. 설치된 악성 앱은 스미싱과 동일한 방식으로 피해자의 개인정보를 훔치며, 소액결제 시 인증에 관련된 문자 메시지를 공격자에게 곧바로 전달하여 희생자의 명의로 결제를 진행할 수 있도록 한다.

크리싱은 스미싱과 다르게 아직 뚜렷한 피해 사례는 없는 것으로 사료된다. 하지만 이를 이용한 피해사례는 앞으로 머지않아 나타날 것이라 예상된다.

〔그림 9〕 동일한 URL의 QR코드 생성

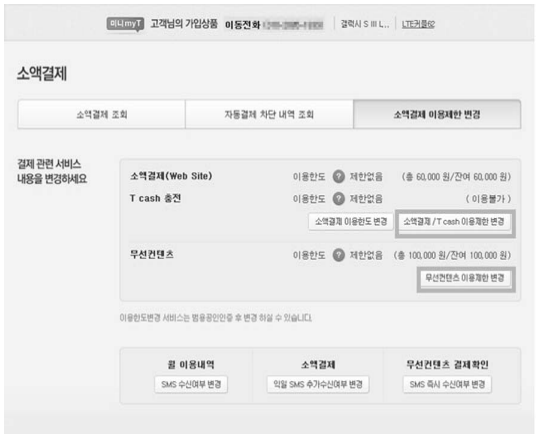
Ⅳ. 신종 피싱의 대응방안

4.1 통신사의 소액결제 차단 서비스

스마트폰에서 발생하는 신종 피싱들은 구매자가 공인인증 절차를 거치지 않아도 되는 소액결제를 이용한 사회공학 기법을 사용한다. 따라서 소액결제 서비스를 원천적으로 차단해버리면 이러한 피해는 일어날 수 없게 된다.

이렇게 적용하기 위해서, 스마트폰 사용자는 [그림 10]과 같이 각 3사 통신사의 홈페이지에 접속해서 소액결제 차단 서비스를 이용할 수 있으며, 소액결제 서비스가 필요한 경우 자신에게 맞는 소액결제 금액한도를 직접 지정하여서 최대한의 피해를 막을 수 있다.[13]

하지만 이러한 서비스는 먼저 일반적인 사용자가 손쉽게 사용할 수 있는 설정 부분에 위치하고 있지 않아 대다수의 사용자들은 이러한 기능을 모르고 있다. 더불어 국내의 경우 은행 어플리케이션 등에서 차단 서비스를 해제하여야 설치할 수 있도록 의무적으로 권장하거나 자동으로 해지하는 기능을 제공하고 있어서 서비스가 제대로 된 기능을 발휘하지 못하고 있는 실태이다.



〔그림 10〕 통신사 소액결제 이용제한 서비스

4.2 출처가 불분명한 APP 설치 차단

안드로이드는 출처가 분명하지 않은 어플리케이션의 설치를 차단하는 서비스를 자체적으로 제공하고 있다. 따라서 사용자는 악성 앱이 스마트폰에 설치되는 것을 방지할 수 있게 된다.

하지만 이러한 서비스는 먼저 일반적인 사용자가 손

〔그림 11〕 알 수 없는 소스 차단 설정화면

〔그림 12〕 스미싱 차단 어플리케이션

쉽게 사용할 수 있는 설정 부분에 위치하고 있지 않아 대다수의 사용자들은 이러한 기능을 모르고 있다. 더불어 국내의 경우 은행 어플리케이션 등에서 차단 서비스를 해제하여야 설치할 수 있도록 의무적으로 권장하거나 자동으로 해지하는 기능을 제공하고 있어서 서비스가 제대로 된 기능을 발휘하지 못하고 있는 실태이다.

4.3 스미싱 차단 어플리케이션

스미싱은 앞서 설명한 내용과 같이, 단축 URL을 SMS에 첨부하는 방식으로 이루어진다. 이러한 해킹을 차단하기 위해서 개발된 어플리케이션이 있다.

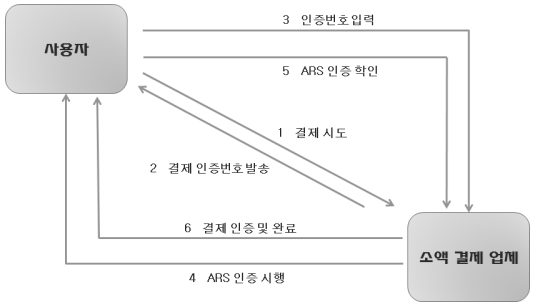
에스이웍스(SEWORKS)사의 '스미싱가드(S-G-UARD)'는 사용자의 스마트폰을 스미싱으로부터 보호하기위한 목적을 가진 어플리케이션이다. 이 앱은 문자메시지에 첨부된 URL을 클라우드 데이터베이스를 기반으로 체크한 후 악성 URL에 해당될 시 이를 차단하는 서비스를 제공한다.[14]

하우리에서도 안드로이드용 '스미싱 디펜더(Smishing-Defender)'를 출시했다. 이 어플리케이션도 스미싱가드와 마찬가지로 클라우드 서버의 데이터를 기반으로 하여 메시지에 첨부된 URL을 검열하는 기능을 제공한다.[15]

그밖에도 잉카인터넷의 '뭐야 이문자'와 인포뱅크의 '엠엔 메시지통' 등도 모두 같은 방식의 서비스를 제공하며, 스미싱 차단 어플리케이션들은 현재 구글 마켓에서 무료로 다운받을 수 있다.[16]

4.4 Two-channel Authentication

2채널 인증(Two-channel Authentication)은 인증에



〔그림 13〕 2채널 인증 휴대폰 결제

2가지 타입 이상의 인증 요소들을 이용하는 방식이다. 인증에 사용되는 타입들은 'Something the user knowledge, Something the user has, Something the user is'를 의미하며 새로운 방식이 아닌 우리가 이미 많이 사용하고 있는 수단이다.

예를 들어 ATM(Automatic Teller Machine)에서 돈을 인출할 때, 우리는 카드(Something the user has)를 이용하고, 키패드를 이용해서 비밀번호(Something the user know)를 입력한다. 이러한 2가지 타입의 인증을 거치고 나서 현금 인출 및 송금 등의 다양한 금융정보 활동을 할 수 있다.

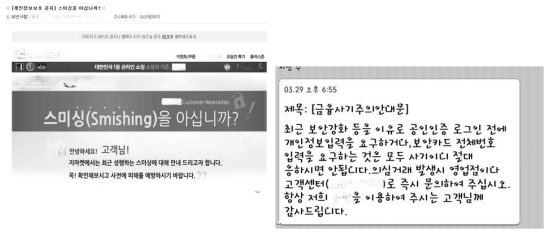
2채널 인증은 모바일, 인터넷 뱅킹 및 금융정보 교환 시 안전한 거래를 위해서 처음 사용하였고, 현재는 가장 많이 쓰이는 방식으로 자리 잡았다.

최근에 스미싱 피해가 계속적으로 발생하기 시작하자, 2채널 인증을 [그림 13]과 같이 소액결제 서비스에 적용하는 결제 서비스가 제안되었다. 사용자는 문자메시지를 통하여 인증번호를 전송받고, 이렇게 받은 인증번호를 휴대폰으로 걸려오는 ARS를 통해 입력함으로써 인증을 진행한다.

2채널 인증은 2가지 타입의 인증을 이용하여 더욱 안전한 소액 결제 서비스를 제공한다. 만약 공격자가 스마트폰의 정보를 획득하더라도 ARS 인증에 대한 또 다른 공격방식을 고안하지 않는 이상 피해는 발생하지 않을 것이다. 따라서 2채널 인증은 무단 소액 결제 서비스를 원천적으로 차단할 수 있는 수단이다.

4.5 보안위험 인식 교육

앞서 다양한 스미싱을 차단하기 위한 방안들에 대하여 기술하였다. 하지만 어떠한 기술보다 더 효과적인 대응방안은, 소액 결제 서비스를 이용하는 사용자들의 인



〔그림 14〕 서비스 업체들의 안내 서비스

식을 개선하고 스미싱에 대한 경각심을 심어줄 수 있는 전체적인 교육을 진행하는 것이다.

어느 인터넷 쇼핑몰 회사는 자신의 회사에 가입되어 있는 회원들에게 스미싱에 관련된 교육용 E-mail을 보내어, 2차적인 피해가 일어나는 것을 막고 있다.

또한 금융권 회사들은 '인터넷 텔레뱅킹 보안 업그레이드'를 가장한 설치 유도 URL에 대해 주의를 요하고 있다. 그리고 신종 피싱의 목적으로 제공되는 URL 정보를 수집하기 위해서 자발적인 신고를 당부하고 있으며, 계속하여 고객들에게 스미싱 위험을 알리는 문자 및 메일링 서비스를 실시하고 있다.

경찰은 이러한 피해사례가 늘어남에 따라 스미싱에 관련된 수사 및 피해에 대한 조사를 점차적으로 실시하고 있으며, 매스컴을 통해서 스미싱의 피해와 주의를 계속적으로 알리고 있다. 2013년 4월에는 스미싱을 이용한 범죄조직들을 검거하는 성과를 올리기도 했다.

소액 결제 서비스를 제공하는 이동 통신사도 고객들에게 스미싱에 대한 주의를 계속적으로 알리고 있다. 그리고 인터넷으로 스미싱에 관한 예방절차 및 피해를 입었을 시 구제방안과 신고절차에 대해 계속적으로 홍보하고 있으며, 현재 스미싱 피해를 입은 고객들을 위한 구제 서비스를 시행하고 있다.

Ⅴ. 결 론

본 논문에서는 가장 대표적인 신종 피싱 방법 중 하나인 스미싱에 대한 정의를 기술하였으며, 그에 따른 방식과 절차에 대해 자세히 기술하였다. 또한 현재 스마트폰 환경에서 많이 사용되고 있는 QR코드를 이용한 크리싱의 정의 및 공격시나리오에 대해서 서술하였다.

스마트폰을 이용한 신종 피싱 공격은 점차 다양화 되고 있으며, 피해사례도 계속하여 증가하고 있다. 피해금액과 피해경로에 대한 전반적인 조사가 필요한 시점이다. 점차 이러한 위협이 나타나면서 스마트폰 보안의 필요성이 부각되고 있다. 또한 기술적인 측면과 법률적인 측면에서 신종 피싱 구제 방안에 대한 다양한 지원이 계속되고 있다.

아직 신종 피싱에 대한 뚜렷한 해결책은 존재하지 않으며, 미봉책(彌縫策)에 불과한 방법을 사용하고 있다. 현재로서 가장 좋은 방안은 보안에 대한 스마트폰 사용자들의 인식을 개선하는 것이다.

스마트폰 보안에 대한 관심을 사용자가 스스로 가질 수 있도록 노력한다면, 스마트폰 피싱에 관한 피해를 최대한 줄일 수 있을 것이다.

참고문헌

[1] "스마트폰", http://terms.naver.com/entry. nhn?cid=200000000&docId=1199937&mobile&categoryId=200000777

[2] "국내 스마트폰 가입자 현황", 한국 방송 통신 위원회

[3] "모바일 악성 코드의 급증", 한국 침해 사고 대응 협의회, Dec. 2012.

[4] "국내 모바일 악성 앱 신고 현황", 한국 인터넷 진흥원

[5] "Android Mobile Web Browsing Usage Share", S-tar Counter, 2012. http://royal.pingdom.com/2012/09/06/south-korea-android-heaven/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+RoyalPingdom+%28Royal+Pingdom%29

[6] 이상우, "아이폰5, 스미싱에서 안전한가?", ebuzz, May. 2013. http://www.ebuzz.co.kr/news/column/2770076_4845.html

[7] "File System Basics", iOS Developer Library, http://developer.apple.com/library/ios/#documentation/FileManagement/Conceptual/FileSystemProgrammingGUide/FileSystemOverview/FileSystemOverview.html

[8] 이민형, "클라우드의 충격 반전, 범죄집단의 해킹에 활용된다?", 디지털데일리, Jul. 2012. http://www.ddaily.co.kr/news/news_view.php?uid=92578

[9] 변현준, "기자도 당했다! 기기묘묘 '스미싱' 사기", 다정다감, Apr. 2013. http://reporter.korea.kr/reporterWeb/getNewsReporter.do?newsDataId=148757

742
[10] 임광복, “휴대폰 ‘공짜쿠폰’의 달콤한 함정”, 파이낸셜뉴스, Apr. 2013. http://www.fnnews.com/view?ra=Sent0901m_View&corp=fnnews&arcid=201304220100225160012695&cDateYear=2013&cDateMonth=04&cDateDay=21
[11] “QR코드”, http://terms.naver.com/entry.nhn?cid=209&docId=21001&mobile&categoryId=209
[12] Timothy Vidas, Emmanuel Owusu, Shuai Wang, Cheng Zeng and Lorrie Cranor, “QRishing: The Susceptibility of Smartphone Users to QR Code Phishing Attacks”, Carnegie Mellon University, May. 2012.
[13] “통신사 소액결제 차단 서비스”, SKT
[14] “스미싱가드”, SEWORKS
[15] “스미싱 디펜더(Smishing Defender)”, ㈜하우리, May. 2013. http://www.hauri.co.kr/customer/support/hauri_notice_view.html?intSeq=303&page=1
[16] 김국배, “소액결제 피해 막는 스미싱 차단 앱 속속 등장”, 아이뉴스24, May. 2013. http://news.inews24.com/php/news_view.php?g_serial=744927&g_menu=020310&rrf=nv

〈著者紹介〉

양 준 근 (Jun-Keun Yang)
학생회원

2013년 2월 : 한림대학교 전자물리학과 졸업
2013년 3월~현재 : 동국대학교 정보보호학과 석사과정
<관심분야> 디지털포렌식, 암호

하 기 웅 (Gi-Ung Ha)
학생회원

2012년 2월 : 동아대학교 컴퓨터공학과 졸업
2013년 3월~현재 : 동국대학교 정보보호학과 석사과정
<관심분야> 클라우드보안, 네트워크보안

김 학 범 (Hak-Beom KIM)
정회원

1990년 8월 : 중앙대학교 대학원 전자계산학과 졸업(공학석사)
2001년 2월 : 아주대학교 대학원 컴퓨터공학과 졸업(공학박사)
1991년 10월~1996년 6월 : 한국전산원 주임연구원
1996년 7월~2001년 8월 : 한국정보보호진흥원(KISA) 기술표준팀장
2001년 9월~2003년 1월 : (주)드림시큐리티 상무이사
2003년 2월~2005년 3월 : (주)장미디어인터렉티브 상무이사
2008년 4월~2009년 6월 : 인포섹(주) 수석컨설턴트
2009년 7월~2010년 12월 : 에스지에이(주) 연구소장
2011년 9월~2013년 3월 : (주)지엔에스인증원 ISMS본부장
2001년 3월~2009년 2월 : 순천향대학교 정보보호학과 겸임교수
2005년 9월~현재 : 동국대학교 국제정보대학원 겸임교수
2011년 7월~현재 : 한국정보보호학회 이사
2013년 4월~현재 : ㈜이너버스 연구소장
<관심분야> 통합로그 시스템, K-ISMS, PIMS, 클라우드컴퓨팅 보안, 개인정보보호