스미싱 예방 및 대응 가이드

2015. 03

KISA 한국인터넷진흥원

목 차

제1장
개요

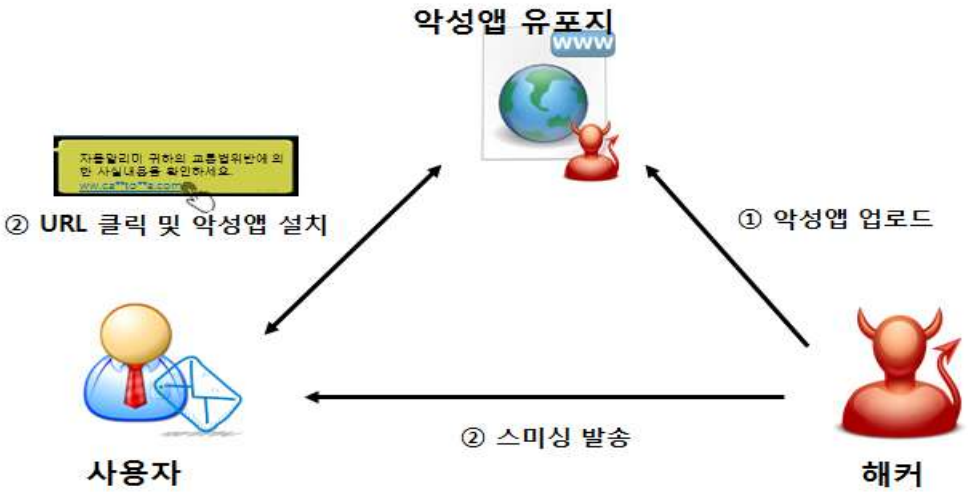
제1장 개요

1. 스미싱이란?

❍ 스미싱 개념

스미싱(smishing)은 문자메시지(SMS)와 피싱(Phising)의 합성어로 사이버사기 중에 하나입니다. 문자메시지에 포함된 인터넷주소(URL)를 클릭하면 악성앱이 설치되고, 개인정보, 금융정보 등을 탈취하여 금전적인 피해를 일으키거나 2차 공격 도구로 활용될 수 있습니다.

❍ 스미싱 유포 과정



< 스미싱 동작 개요도 >

해커는 불특정 다수에게 악성코드를 설치할 수 있는 인터넷주소가 포함된 문자메시지를 발송합니다. 문자를 수신한 사용자가 인터넷주소를 클릭하면 악의적으로 만들어진 피싱 사이트로 접속되거나 악성앱을 설치하는 설치파일이 다운로드 됩니다.

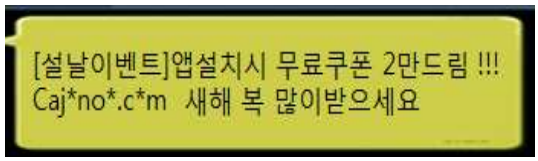
2. 스미싱 특성

스미싱은 문자메시지(SMS)에 포함되어 있는 인터넷주소(URL)를 단순히 클릭하는 것만으로 악성코드에 감염되지 않습니다. 인터넷주소를 클릭하여 다운로드 된 APK 파일을 설치하는 경우에만 악성앱이 설치됩니다.

❍ 인터넷주소

스미싱은 악성코드에 감염된 스마트폰을 이용한 사이버사기 수법으로 악성앱을 설치하기 위한 인터넷주소가 문자메시지에 포함되어 있습니다. 이러한 인터넷주소(URL)는 단축 서비스를 사용하여 이용자가 웹사이트 정보를 알기 어렵고, 정상적인 사이트와 매우 유사하게 모방하여 제작된 가짜사이트인 피싱사이트로 연결됩니다. 최근에는 정상적인 사이트와 유사한 일반적인 인터넷주소를 사용하는 경우도 있으므로 주의해야 합니다.

< 단축 URL 사용 예시 >



< 일반 도메인 악용 예시 >

❍ 악성앱

< 사칭 악성앱 유형 >

스미싱은 사용자들이 악성앱 여부를 인지하기 어렵도록 정상앱을 사칭하는 경우가 많습니다. 휴대전화에 일반적으로 많이 설치된 정상앱(예: 크롬, Play 스토어, 공공기관에서 사용하는 민원24, 유명 모바일 백신 등)을 사칭하여 악성앱 설치를 유도합니다.

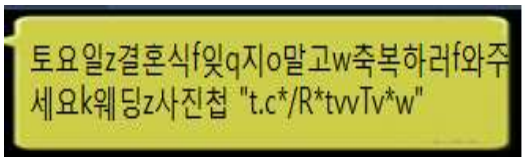
이러한 악성앱은 정상앱이 필요로 하지 않는 과도한 권한을 요구하고 있습니다. 전화, 문자메시지 관리, 개인정보 조회, 저장소 조회, 위치정보, 기기관리자 권한 요구 등 정상앱 보다 과도한 권한을 포함하고 있으므로 앱 설치 단계에서 주의해야 합니다.

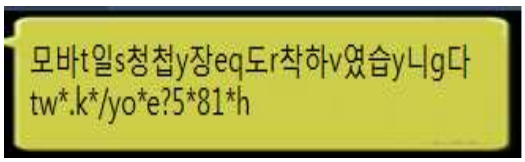
또한 악성앱이 악성코드 감염, 개인정보 유출 등 악성행위를 직접 수행하기도 하지만 별도의 악성앱을 설치하도록 유도하는 기능이 탑재된 경우도 있습니다. 크롬, 뱅킹, 백신 등 특정 애플리케이션이 실행 될 경우 '업데이트 파일입니다'라는 형태로 업데이트를 안내하여 이용자들이 악성앱을 다운로드하도록 유도하고 있습니다. 이렇게 설치된 악성앱은 중요 정보를 유출하는 등의 악성 행위를 합니다.

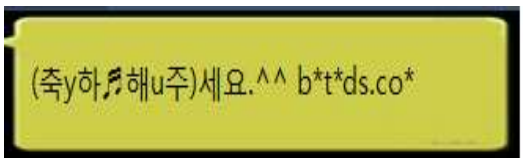
❍ 관심을 유도하는 문자메시지

사용자가 악성앱을 설치하도록 유도하기 위해 관심을 유도하는 다양한 형태의 문자메시지가 발생되고 있습니다. 대표적인 유형으로는 청첩장, 돌잔치 초대장 등 '지인 사칭', 배송지연, 수령확인 등 '택배 사칭', 검찰청, 경찰청 등 '공공기관 사칭', 명절, 국가적 행사나 각종 사건사고와 같은 '사회적 이슈 사칭'하는 내용이 포함되고 있습니다.

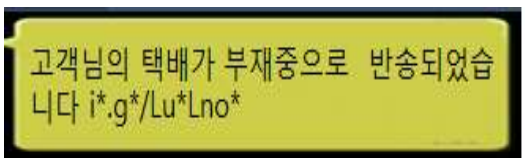
< 지인 사칭 유형 >

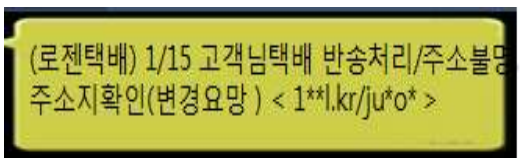


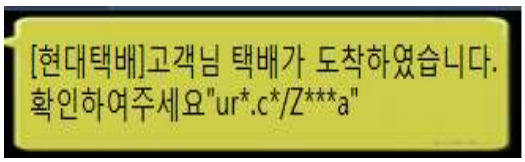




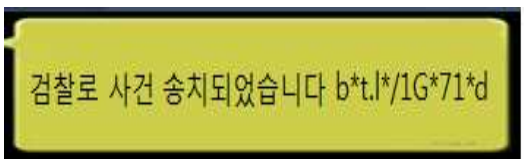
< 택배 사칭 유형 >

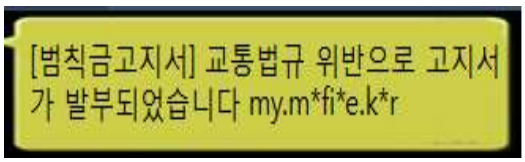


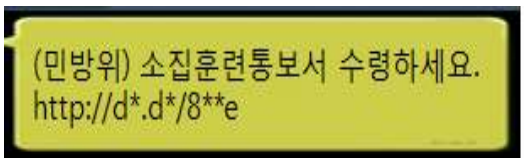




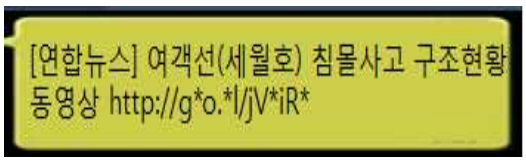
< 공공기관 사칭 유형 >

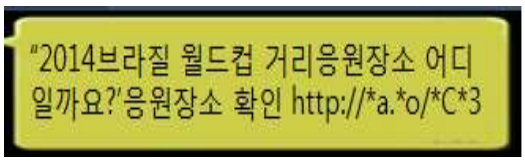


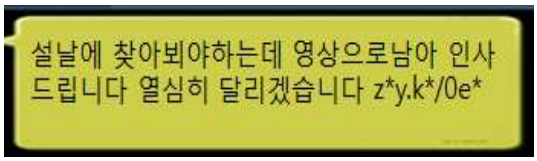


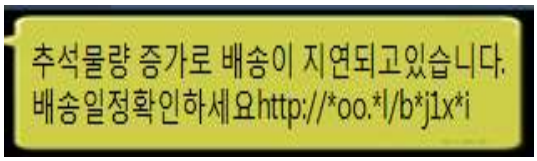


< 사회적 이슈 유형 >

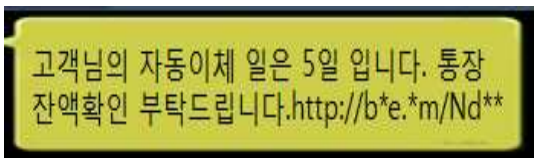


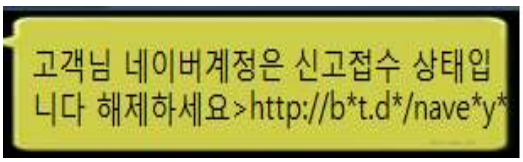


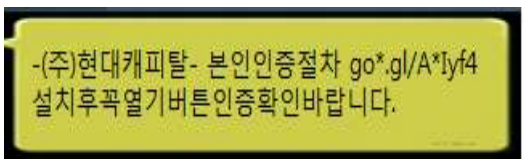


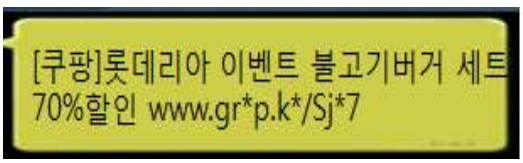


< 기타 유형 >





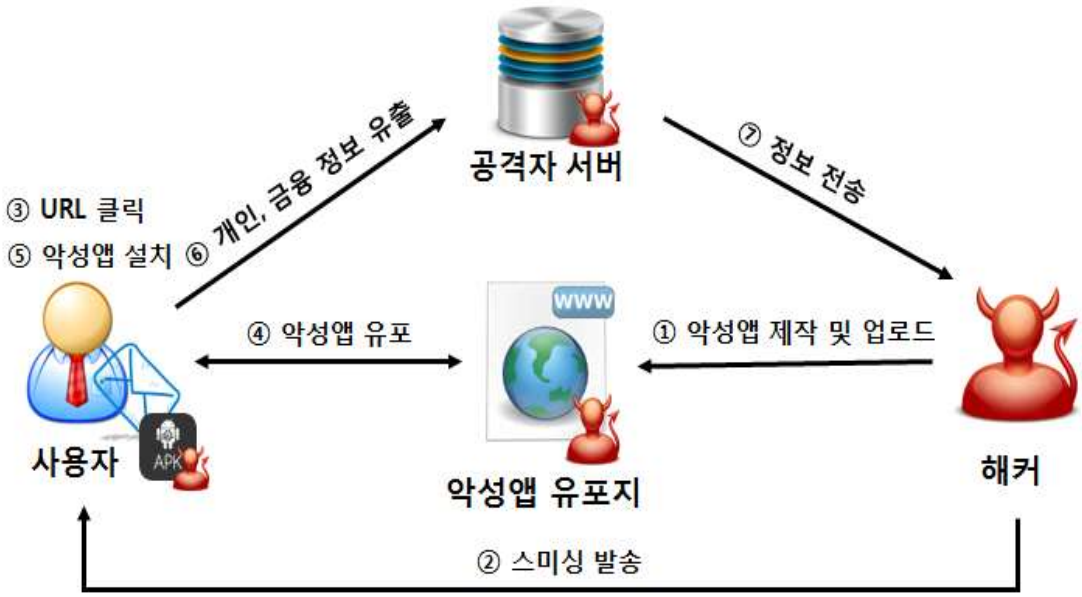




3. 스미싱 시나리오

스마트폰을 악성코드에 감염시키기 위해 악성앱을 설치하는 방법과 설치된 악성앱이 수행하는 기능에 따라 스미싱의 유포 방식에는 차이가 존재합니다.

❍ 일반적인 스미싱



< 일반적인 스미싱 개요도 >

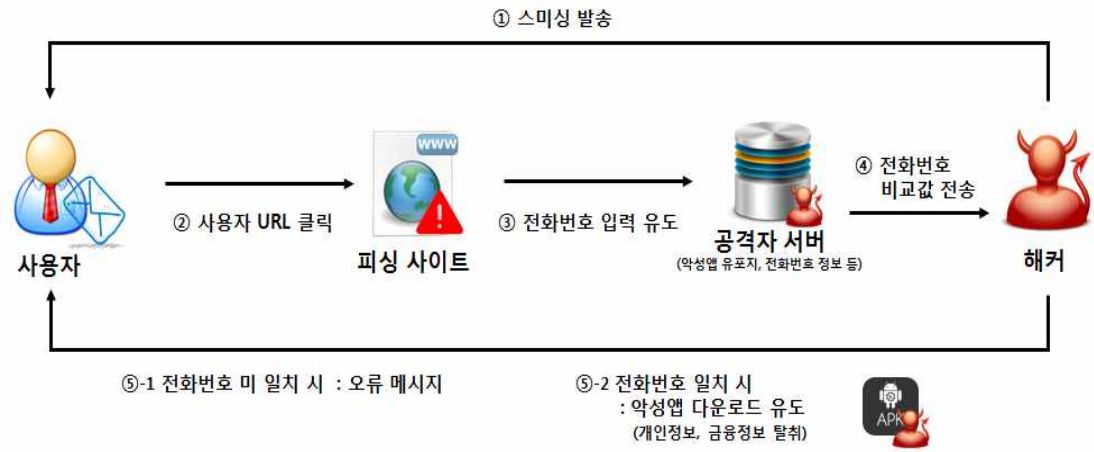
일반적인 스미싱은 해커가 목적에 맞게 악성앱을 제작하고, 사용자가 악성앱을 다운로드 받을 수 있도록 클라우드 서비스(드롭박스, 아마존)에 업로드합니다. 해커가 운영하는 자체 서버를 통해 악성앱을 유포하기도 합니다.

사용자가 문자메시지에 포함된 인터넷주소를 클릭하면 앱을 설치할 수 있는 설치파일인 ‘APK 파일’이 자동으로 다운로드됩니다. 다운로드 된 APK 파일을 사용자가 클릭할 경우 악성앱이 설치됩니다. 설치가 끝난 악성앱을 실행하면 개인정보, 금융정보 등 중요정보가 해커가 지정한 서버로 전송됩니다. 이때 해커가 결제승인번호 등 문자메시지를 탈취하게 된다면 소액결제를 이용자 몰래 시도할 수 있습니다.

❍ 피싱사이트를 이용한 스미싱

피싱사이트를 이용한 스미싱은 인터넷주소를 클릭하게 되면 정상사이트를 가장한 피싱사이트로 연결되고, 이들 가짜사이트에서는 정상앱을 설치하는 것처럼 악성앱 설치를 유도합니다.

❍ 사용자 입력 요구 스미싱



< 개인정보 입력 요구 스미싱 개요도 >

사용자 정보, 캡챠코드 등 사용자가 입력한 특정정보가 일치하는 경우에만 악성앱이 다운로드 되도록 하는 가장 진화된 방식의 스미싱입니다. 용자 접근 환경(PC, 모바일)을 구별할 뿐만 아니라 타인의 전화번호를 입력할 경우에는 악성앱이 다운로드 되지 않습니다. 피싱사이트에 포함된 이미지를 클릭만 해도 악성앱이 다운로드 되는 경우도 있으므로 주의가 필요합니다.

< 캡챠코드 입력 요구 >

■ 주요 용어

◎ APK 파일 : 안드로이드 응용 프로그램 패키지의 확장자로 안드로이드 애플리케이션 설치 파일

◎ 애플리케이션 : 응용 소프트웨어의 준말로 운영체제 위에서 동작되는 모든 소프트웨어를 뜻하고 더 줄여서 앱(App)이라고도 표현

◎ 애플리케이션 권한 : 애플리케이션이 실행될 때, 애플리케이션이 스마트폰 안에 들어있는 여러 가지 정보에 대한 접근을 가능하게 하는 정보

◎ 애플리케이션 마켓 : 스마트폰 사용자가 앱 개발자로부터 구매하여 설치 및 관리를 할 수 있도록 환경을 제공하는 앱으로써 마켓은 제조사나 통신사 등에서 운영하여 앱에 대한 검증 및 관리하는 공식 마켓과 특정 조직이나 업체에서 관리를 하지 않는 그 외에 마켓으로 구별됨

◎ 캡챠코드 : 사용자가 실제 사람인지 컴퓨터 프로그램인지를 구별하기 위해 사용하는 방법으로 컴퓨터가 쉽게 인지하지 못하게 의도적으로 숫자나 문자를 비틀거나 덧칠하면서 해당 내용을 물어보는 방법

◎ 루팅 : 안드로이드 운영체제의 기반이 된 리눅스 환경에서 모든 파일과 프로그램에 접근할 수 있는 권한을 비정상적인 방법으로 획득하여 슈퍼유저로 설정

◎ 탈옥 : 애플社의 아이폰 잠금장치를 해킹하여, 멀티태스킹 등 다양한 기능을 사용하고 유료 앱을 무료로 이용할 수 있도록 함

제2장
스미싱 사전 예방 방법

제2장 스미싱 사전 예방 방법

1. 스마트폰 안전하게 관리하기

❍ 스마트폰 권한 임의변경 금지

대부분의 안드로이드 스마트폰은 사용자에게 모든 파일과 프로그램에 접근할 수 있는 '슈퍼 유저', '최고 관리자 권한'을 부여하지 않습니다. '최고 관리자 권한'이 없는 일반 사용자는 스마트폰 파일, 설정이 제한됩니다.

그러나 일부 사용자들이 비정상적인 방법으로 '최고 관리자 권한'을 획득하는 '탈옥', '루팅'을 하기도 합니다. '최고 관리자 권한'을 획득하게 되면 기본 탑재된 애플리케이션을 삭제, 스마트폰 디자인 변경 등 임의로 스마트폰을 변경할 수 있습니다. 하지만 충분한 지식이 없이 관리자 권한을 획득할 경우 기기에 심각한 문제가 발생할 수 있습니다. 또한, 루팅 된 스마트폰이 악성코드에 감염되면 권한에 따라 자료 조회, 조작이 가능하여 루팅한 스마트폰은 보안상으로 더 많은 위협에 노출됩니다.

❍ ‘알 수 없는 출처(미인증) 앱 설치’ 기능 해제

< ‘알 수 없는 출처(미인증) 앱 설치 기능’ 해제 방법 >

출처가 불분명한 APK 파일이 다운로드 되어 애플리케이션이 설치되는 것을 방지하기 위해서는 스마트폰 환경설정에서 **‘알 수 없는 출처 앱 설치’ 기능을 해제**해야 합니다.

※ 스마트폰 ‘환경설정’ → ‘보안’ 탭에서 해당 기능 체크 해제

안드로이드 스마트폰은 공식 앱 마켓뿐만 아니라 인터넷 다운로드, APK 파일 전송 등 다양한 방법으로 애플리케이션을 자유롭게 설치 할 수 있습니다. 이러한 방법은 사용자에게 편리함을 제공하지만 애플리케이션의 안전성과 보안성을 검증하지 못하는 문제가 존재합니다.

스미싱은 이와 같은 점을 악용하여 인터넷주소(URL)로 악의적으로 제작한 APK 파일을 유포하여 사용자가 악성앱을 설치하도록 유도하고 있습니다. 따라서 '알 수 없는 출처 앱 설치' 기능을 해제하여 공식 앱 마켓인 'Play 스토어', '통신사 스토어' 외의 방법으로 애플리케이션이 설치되는 것을 방지할 수 있습니다. 설정을 해제하게 되면 경고창으로 위험을 안내받을 수 있습니다.

❍ 스미싱 차단앱 설치

< 스마트폰 기본 탑재 스미싱 차단앱 >

'**스미싱 차단앱'을 설치**하면 스미싱으로 의심되는 문자메시지를 사전에 차단할 수 있습니다.

스미싱 차단앱은 문자메시지에 포함된 인터넷주소(URL)를 분석하여 스미싱 악용 여부 및 악성 APK 파일의 포함 유무를 점검하여 사용자에게 정보를 제공하고, 스미싱을 사전에 차단하는 서비스를 제공하고 있습니다.

❍ 모바일 백신 설치

모바일 백신, 스마트폰 점검 앱(예: 폰키퍼) 등을 설치하여 스마트폰의 보안 상태를 주기적으로 점검하고, 설치된 애플리케이션에 악성코드가 포함되었는지 사전에 확인해야합니다.

모바일 백신의 '실시간 감시' 기능을 이용해 새로운 애플리케이션을 설치할 때마다 보안 상태를 점검하여 스마트폰에 악성앱이 설치되지 않도록 주의가 필요합니다.

❍ 안드로이드 운영체제 최신 업데이트

스마트폰 제조사에서는 운영체제의 취약점, 오류 등을 지속적으로 개선하여 수정 버전을 배포하고 있습니다. 스마트폰 운영체제를 항상 최신 버전으로 업데이트하여 보안 취약점이 없도록 관리해야 합니다.

❍ 보호되지 않는 무선 공유기(WiFi) 사용 금지

스마트폰 사용자는 암호 설정이 되어 있지 않는 무선 공유기를 사용할 때 보안 취약점에 노출되지 않도록 주의해야 합니다. 공공장고, 식당, 카페, 도서관 등에서 사용자 편의를 위해 **무료로 제공하는 무선 공유기를 사용할 때 주의**해야 합니다. 보안 설정이 되어 있지 않은 무선 공유기를 사용할 경우 스마트폰이 감시당하거나 파밍 등의 사이버 위협에 노출될 수 있습니다.

2. 의심스러운 문자메시지 주의하기

스미싱은 스마트폰에 설치된 악성 애플리케이션으로 개인정보, 금융정보 등을 탈취하는 사이버사기 수법으로 앱을 설치하기 위한 설치파일을 다운로드 받는 인터넷주소가 문자메시지에 반드시 포함되어 있습니다.

해커는 인터넷주소를 클릭을 유도하기 위해 지인, 택배, 공공 기관 등을 사용자들이 관심 있어 하는 것을 사칭하며, 국제적 행사, 각종 사건 사고, 이벤트 등 사회적 이슈를 활용하여 스미싱을 유포하고 있습니다. 또한 스미싱 의심 문자로 분류되어 사전에 차단되지 못하도록 문구 사이에 의미 없는 알파벳이나 숫자, 특수문자 등을 삽입하는 경우도 있습니다.

- **출처가 불분명한 전화번호로 발송된 문자메시지**
- **결혼식, 공공기관, 택배, 사회적 이슈 등을 포함하는 문자메시지**

※ 공공기관의 경우 go.kr, or.kr, kr로 끝나는 경우가 대부분이며, com, co.kr 등으로 끝날 경우 각별한 주의가 필요

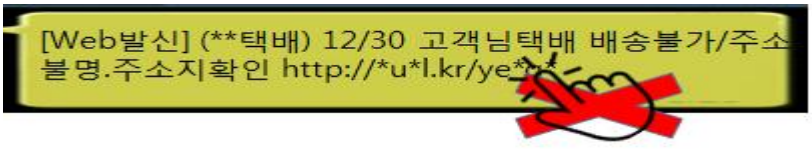
- **문구 사이에 의미 없는 알파벳이나 숫자, 문구 등이 포함된 경우**

< 의미 없는 문구를 포함 경우 >

수신한 문자가 이러한 내용에 해당된다면 인터넷주소를 클릭하기 전에 스미싱을 의심해야 합니다. 특히 인터넷주소(URL)에서 연결된 사이트에서 전화번호 등 사용자의 개인정보를 입력하도록 요구한다면 정보를 입력하지 마시고 해당 사이트를 즉시 종료해야 합니다.

< 사용자 정보 입력을 요구하는 피싱사이트 >

스미싱으로 의심되는 문자메시지를 수신하였을 경우 한국인터넷진흥원(☎118)으로 신고하고, 해당 문자메시지는 즉시 삭제하여야 합니다.



< 의심되는 문구 및 URL 포함 시 절대 클릭 금지 >

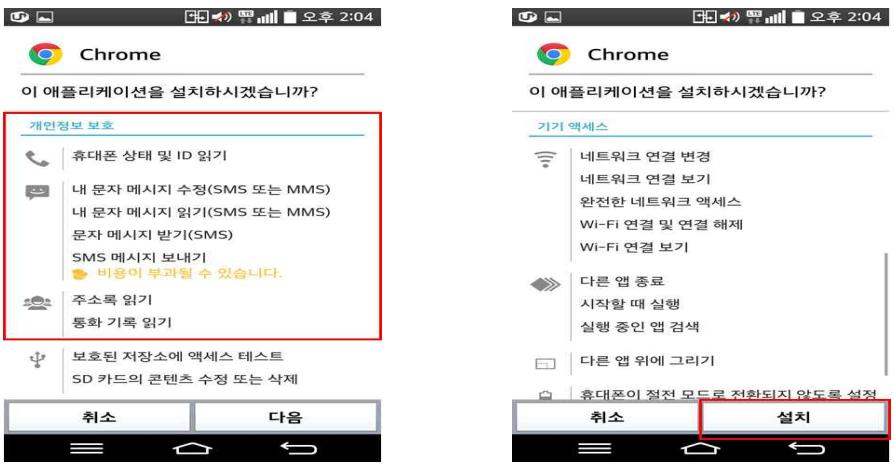
3. 애플리케이션(앱) 설치 관리하기

문자메시지에 포함되어 있는 인터넷주소(URL)을 단순히 클릭을 한다고 해서 악성코드에 감염되는 것은 아닙니다. 인터넷주소 클릭 한 후 다운로드 된 APK 파일로 악성앱이 설치될 경우 스마트폰이 악성코드에 감염됩니다.

❍ 공식 애플리케이션 마켓 이용하기

악성앱은 정상앱과 구분을 어렵게 하기 위해 정상앱의 기능을 수정하여 악성코드를 삽입하는 하는 방법을 사용합니다. 악의적인 목적으로 수정된 애플리케이션의 경우 사설 앱마켓에서 정상앱을 사칭하여 유포되고 있습니다. 따라서 정상앱을 사용하기 위해서는 공식 애플리케이션 마켓인 Play 스토어, 통신사 마켓에서 앱을 다운로드 받아 사용하는 것이 안전합니다.

❍ 애플리케이션 권한 확인하기



< 악성 앱의 경우 과도한 권한을 요구 >

안드로이드 스마트폰에서는 애플리케이션을 설치할 때 앱의 접근 권한에 대하여 사용자의 동의를 반드시 요청합니다. 사용자는 애플리케이션을 설치하기 전에 앱이 요구하는 기능이 무엇인지 자세히 살펴보아야 합니다.

설치하려는 애플리케이션의 기능과 다른 과도한 접근 권한을 요구한다면 주의해야합니다. 예를 들어 게임 애플리케이션이 통화 내역, 문자 및 통화 기능, 저장소 조회 등 필요 이상의 권한을 요구하는 경우 악성앱을 의심할 수 있습니다.

공식 애플리케이션 마켓에서 설치한 앱이라도 사용자들의 정보 수집을 위해 과도한 정보를 요구하는 경우가 있기 때문에 요구하는 접근 권한을 확인하고 설치를 진행해야 합니다.

❍ 휴대폰관리자 권한 활성화 금지하지

< 기기관리자 권한 요구 화면 >

안드로이드 스마트폰에서는 스마트폰 분실 시 위치 정보 확인, 하드웨어 제어, 기기 설정 등을 원격으로 제어하기 위해 ‘휴대폰 관리자 기능’을 제공하고 있습니다. 휴대폰 관리자 기능이 활성화된 앱은 휴대폰 관리자 기능을 해지한 후에야 앱 삭제가 가능합니다.

스미싱으로 유포되는 악성앱은 휴대폰 관리자 기능을 획득하면 일반적인 앱보다 삭제가 어렵다는 점을 이용하여 휴대폰 관리자 권한 활성화를 요구하기도 하므로 주의해야 합니다. 이러한 앱은 안전모드로 부팅해야 악성앱을 삭제할 수 있습니다.

※ 자세한 사항은 [부록 : 스마트폰에 설치된 악성앱 삭제 방법]을 참조

❍ 모바일 백신 점검하기

모바일 백신의 ‘실시간 감시’ 기능을 활성화하면 새로운 애플리케이션이 설치될 때 보안 상태를 자동 점검해줍니다. ‘실시간 감시’ 기능을 설정하지 않은 경우에는 애플리케이션 실행 전 반드시 모바일 백신으로 스마트폰 보안 상태를 점검하고 실행하는 것이 안전합니다.

4. 스미싱 예방 서비스 가입하기

이동통신사에서는 스미싱 피해 예방 및 방지를 위해 다양한 부가서비스를 제공하고 있습니다. 해당 부가서비스들은 통신사 고객센터를 통해 무료로 가입 가능합니다.

❍ '웹 발신 확인 서비스' 가입(무료)

< 웹 발신 확인 서비스 형태 >

수신된 문자메시지가 인터넷 또는 문자발신 전용프로그램 등을 이용하여 발신된 경우 '[Web발신]'으로 표기해 대량 발송 문자메시지임을 알려주는 서비스입니다. 스미싱은 대량 유포를 위해 대량 발송 및 웹을 통해 발송되는 경우가 있으므로 '[Web발신]' 문자메시지에 인터넷주소가 포함된 경우 주의해야 합니다.

❍ '번호도용 문자차단 서비스' 가입(무료)

자신의 전화번호가 스미싱이나 스팸에 도용되는 것을 방지하기 위하여 평소 인터넷으로 문자를 발송하지 않는다면 자신의 전화번호로 인터넷 문자 발송 서비스를 이용하지 못하도록 '번호도용 문자차단 서비스'에 가입할 수 있습니다. 웹에서 대량 발송되는 스미싱, 스팸에 도용되는 것을 방지 할 수 있으나, 자기 자신도 인터넷 문자 발송 서비스를 통해 문자를 발송할 수 없으므로 불가피

하게 인터넷으로 문자를 발송하고자 할 경우, 해당 서비스를 일시적으로 해지해야합니다. 해당 통신사 고객센터 및 홈페이지에서 가입 가능합니다.

※ SKT : 홈 > 부가서비스 > 이동전화 > 부가서비스 > 문자 > 문자편리서비스
※ KT : My올레 > 모바일 > 부가서비스 신청/변경 > 서비스 추가 신청
※ LGU+ : 홈 > 개인 > 모바일 > 부가서비스 > 문자메신저 > 번호도용 문자차단

❍ '소액결제 차단 서비스' 가입(무료)

평소 휴대전화 소액결제 서비스를 이용하지 않는 사용자라면 '소액 결제 차단 서비스'에 가입하여 휴대폰으로 자동 결제되는 소액 결제 피해를 예방할 수 있습니다. 소액결제 서비스를 차단하지 않고 소액결제 한도를 조절할 수 있으므로 사용자의 결제 습관에 따라 소액결제 서비스 이용 범위를 설정할 수 있습니다.

5. 스미싱 의심 문자 신고하기

스미싱으로 의심되는 문자메시지를 수신하였을 경우에는 인터넷 주소(URL)을 클릭하지 마시고 한국인터넷진흥원(☎ 118)로 즉시 신고해주시기 바랍니다.

한국인터넷진흥원 해당 문자메시지로 발생할 수 있는 추가적인 피해 및 피해자를 예방하기 위해 악성앱 발견, 신고 시 인터넷서비스 사업자(ISP)를 통해 악성앱 유포지와 정보유출지를 즉시 차단하고, 백신개발사에 악성앱 샘플을 제공하여 백신을 개발하도록 조치하는 등 스미싱 피해를 예방하기 위해 노력하고 있습니다.

제3장
스미싱 피해 시 대응 방법

제3장 스미싱 피해 시 대응 방법

1. 악성 애플리케이션 삭제하기

문자메시지에 포함된 인터넷주소를 클릭한 것만으로는 악성코드에 감염되지 않습니다. 하지만 인터넷주소를 통해서 특정 애플리케이션을 설치했다면 악성코드 감염을 의심해야합니다. 악성앱 감염이 의심되면 다음과 같은 방법으로 스마트폰을 점검해야합니다.

❍ 모바일 백신으로 악성앱 삭제하기

모바일 백신, 스마트폰 점검 도구(예: 폰키퍼)를 이용하여 스마트폰 보안 상태를 검사하여 악성앱 설치 여부를 확인합니다. 모바일 백신, 스마트폰 점검 도구가 최신 버전으로 업데이트하여야 악성앱 탐지율이 높아집니다.

❍ 악성앱 수동 삭제하기

모바일 백신, 스마트폰 점검 도구 외에 스마트폰 애플리케이션 관리 창을 통해 사용자가 직접 악성앱 또는 사용하지 않는 앱을 수동으로 삭제할 수 있습니다. 정상앱으로 위장한 악성앱은 설치일자, 설치 용량 등을 확인하여 악성앱인지를 확인할 수 있습니다.

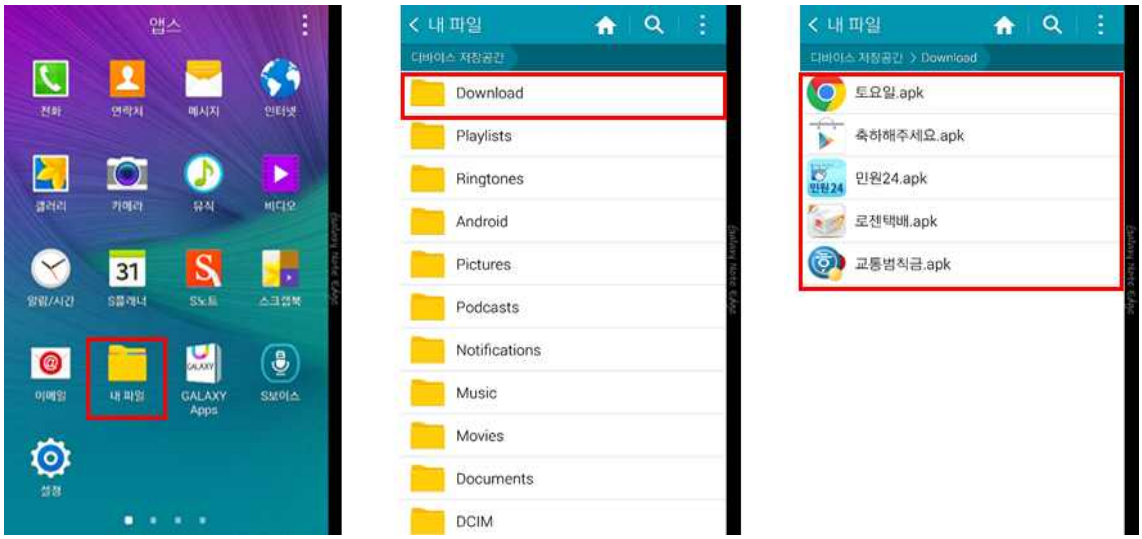
스마트폰에 기본 설치된 애플리케이션을 사칭한 악성앱은 눈으로 구별하기 어렵습니다. 기본 탑재된 정상앱을 삭제하려는 경우 삭제가 불가능하고 '사용중지'로 표시되지만 악성앱을 삭제할 경우는 '삭제' 버튼이 정상 동작하여 삭제가 가능합니다.

※ 자세한 사항은 [부록 : 스마트폰에 설치된 악성앱 삭제 방법]을 참조

❍ 서비스 센터 방문

악성앱 삭제가 어려울 경우스마트폰 데이터를 다른 보관 장소에 안전하게 저장한 후 가까운 서비스센터를 방문하여 스마트폰 포맷 및 초기화를 진행하셔야합니다.

2. 악성 애플리케이션 설치 파일(APK) 삭제하기



< APK 파일 삭제 방법 >

스마트폰에 악성앱이 설치되기 위해서는 해당 악성앱을 설치하는 설치 파일(APK 파일)이 필요합니다. 스미싱 문자메시지에서 인터넷주소를 클릭하면 APK 파일이 다운로드되고, 해당 APK 파일을 실행하면 악성앱이 설치됩니다.

악성앱 뿐만 아니라 해당 APK 파일까지 삭제해야 추후 악성앱이 재설치 될 가능성을 예방할 수 있습니다.APK 파일은 스마트폰에

기본적으로 설치되어 있는 ‘파일관리자’, ‘내파일’ 등 파일관리 애플리케이션에서 ‘Download 폴더’를 확인하여 삭제가 가능합니다.

3. 모바일 결제 확인 및 취소하기

스미싱 악성앱에 감염되면 모바일 결제 피해가 발생할 수 있습니다. 따라서 이동통신사에 모바일 결제 내역이 있는지 확인해야 합니다. 모바일 결제 확인 방법과 피해 발생 시 대응 방법은 다음과 같습니다.

① 통신사 고객센터를 통하여 최근 모바일 결제 내역 확인

② 모바일 결제 피해가 확인되면 피해가 의심되는 스미싱 문자 캡쳐

③ 통신사 고객센터를 통해 스미싱 피해 신고 및 ‘소액결제확인서’ 발급

④ 소액결제확인서를 지참하여 관할 경찰서 사이버수사대 또는 민원실을 방문하여 사고 내역 신고

⑤ 사고 내역을 확인받고 ‘사건사고 사실 확인서’ 발급

⑥ 사건사고 사실 확인서 등 필요서류를 지참하여 통신사 고객센터 방문 또는 팩스나 전자우편 발송

⑦ 통신사나 결제대행 업체에 사실 및 피해 내역 확인 후 피해 보상 요구

4. 공인인증서 폐기 및 재발급하기

악성앱에 감염되었던 스마트폰으로 모바일 금융서비스를 이용했다면 공인인증서, 보안카드 등 금융거래에 필요한 정보가 유출되었을 가능성이 존재합니다. 따라서 해당 정보를 폐기하고 재발급을 받아야 유출된 금융 정보로 인한 2차 피해가 발생하는 것을 예방할 수 있습니다.

스마트폰에 공인인증서가 저장되어 있지 않았더라도 보안카드 등 금융 거래에 필요한 정보를 사진첩, 메모장에 기록했다면 폐기 처분하고 재발급을 받아야 합니다.

5. 2차 피해 예방하기

해커는 악성코드에 감염된 스마트폰을 새로운 사이버범죄 도구로 사용합니다. 악성앱이 주소록을 조회하여 다른 사람에게 유사한 내용의 스미싱을 발송하는 등 2차 피해가 발생할 수 있으므로 주변 지인들에게 스미싱 피해 사실을 알려야합니다. 또한 특정 악성앱에는 전화 수신 및 문자메시지 수신을 차단하는 기능을 포함하고 있어 악성앱 삭제 방법을 확인 후 삭제를 해야 추가적인 2차 피해를 예방할 수 있습니다.

부록

부록. 스마트폰에 설치된 악성 앱 삭제 방법

■ 스마트폰에 설치되는 일반적인 앱(악성 앱 포함)은 설정 → 애플리케이션에서 앱 목록을 확인한 뒤, 삭제할 앱을 선택 후 삭제가 가능

※ 1. 일반적인 악성 앱 삭제 방법 참고

■ 대부분의 악성 앱은 관리자 권한을 요구하여 일반적인 앱 삭제와 달리 관리자 권한 해제 과정이 필요

※ 2. 기기 관리자 권한 해제 후 삭제 방법 참고

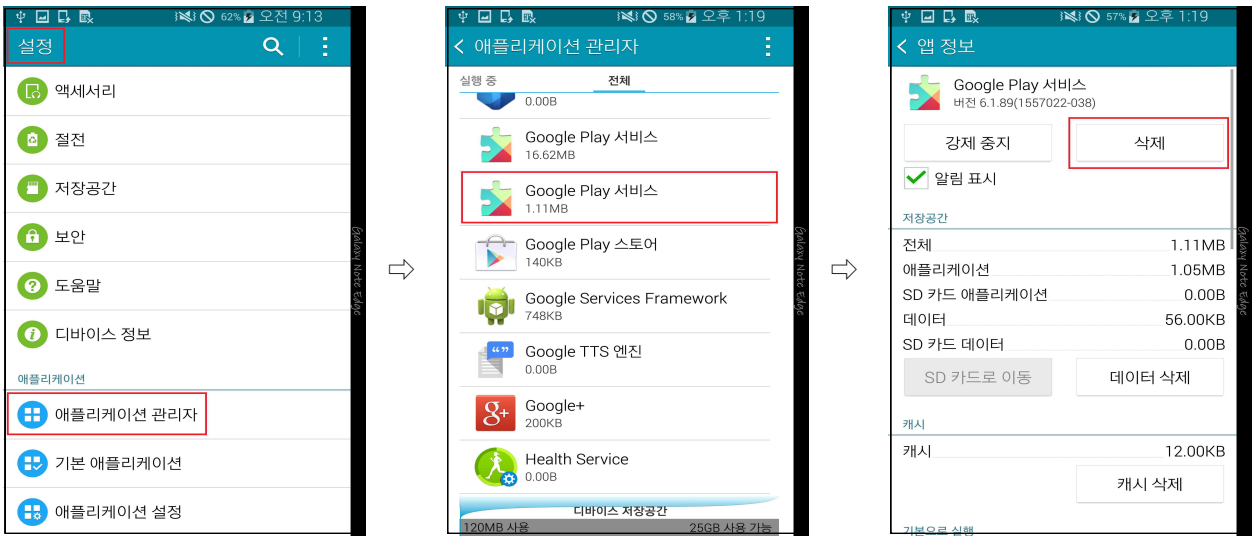
■ 최근 탐지되는 악성 앱은 기기 관리자 권한 해제를 방해하는 기능이 있어, 안전모드 부팅을 통한 기기 관리자 권한 해제가 필요

※ 3. 안전모드 부팅을 이용한 삭제 방법 참고

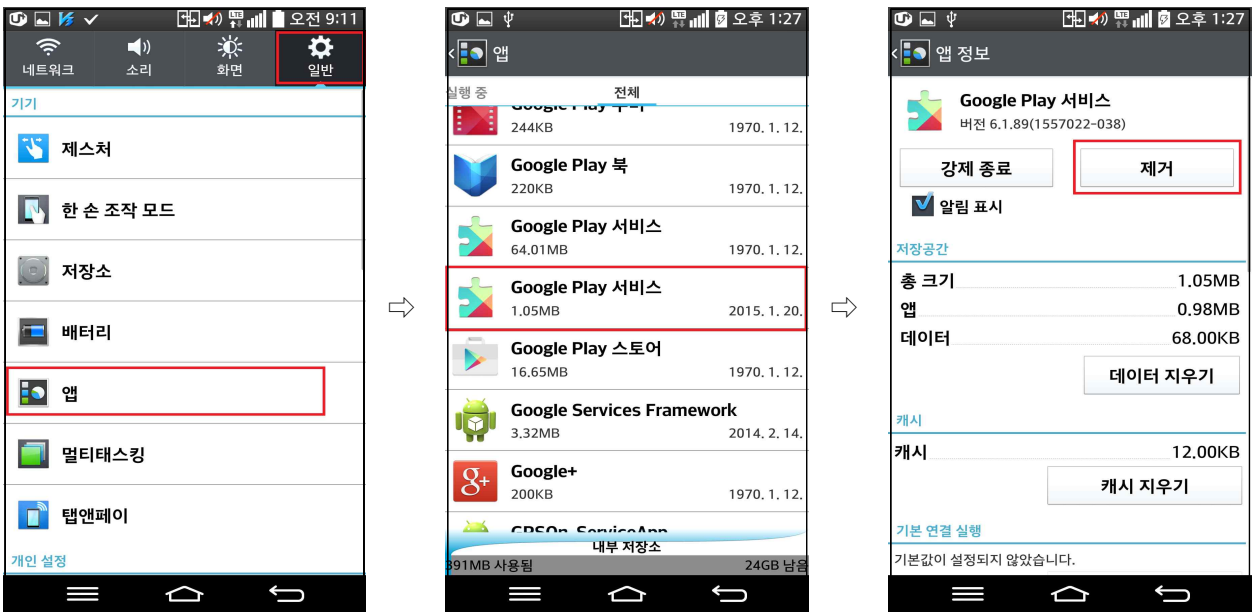
1. 일반적인 악성 앱 삭제 방법(Google Play 서비스 사칭 사례)

※ 메뉴(탭)명은 스마트폰 제조사별 상이(아래 그림 참고)

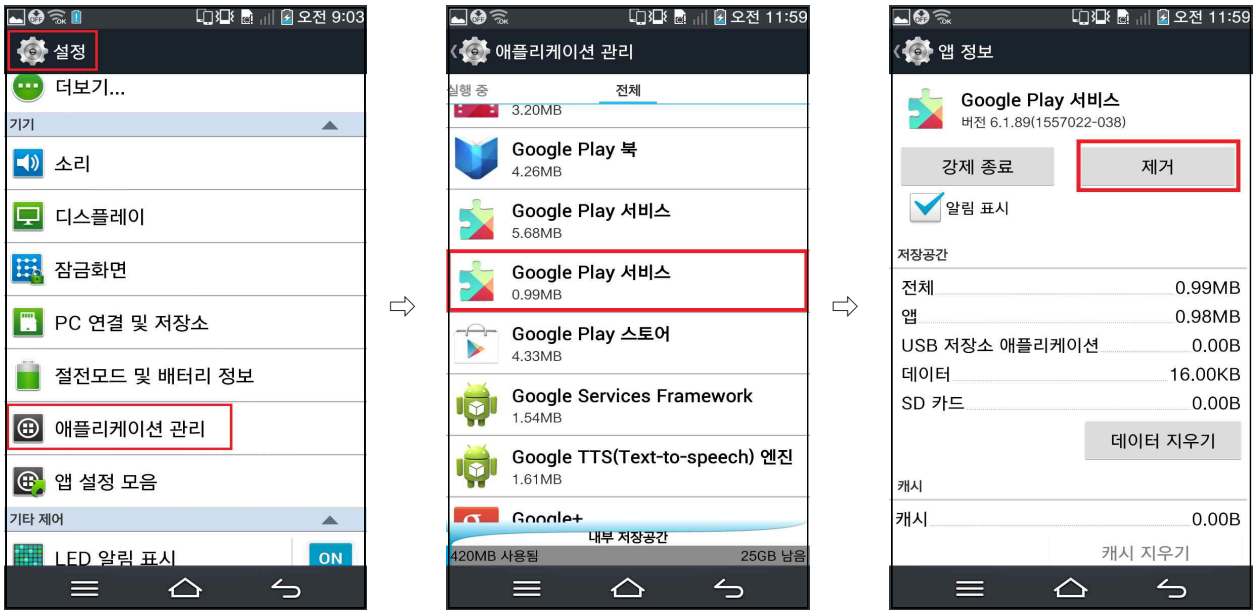
① 삼성 : 설정 → 애플리케이션 → 애플리케이션 관리자(삭제할 앱 선택) → 삭제



② LG : 설정 → 일반 → 기기 → 앱(삭제할 앱 선택) → 제거



③ 펜택 : 설정 → 기기 → 애플리케이션 관리(삭제할 앱 선택) → 제거

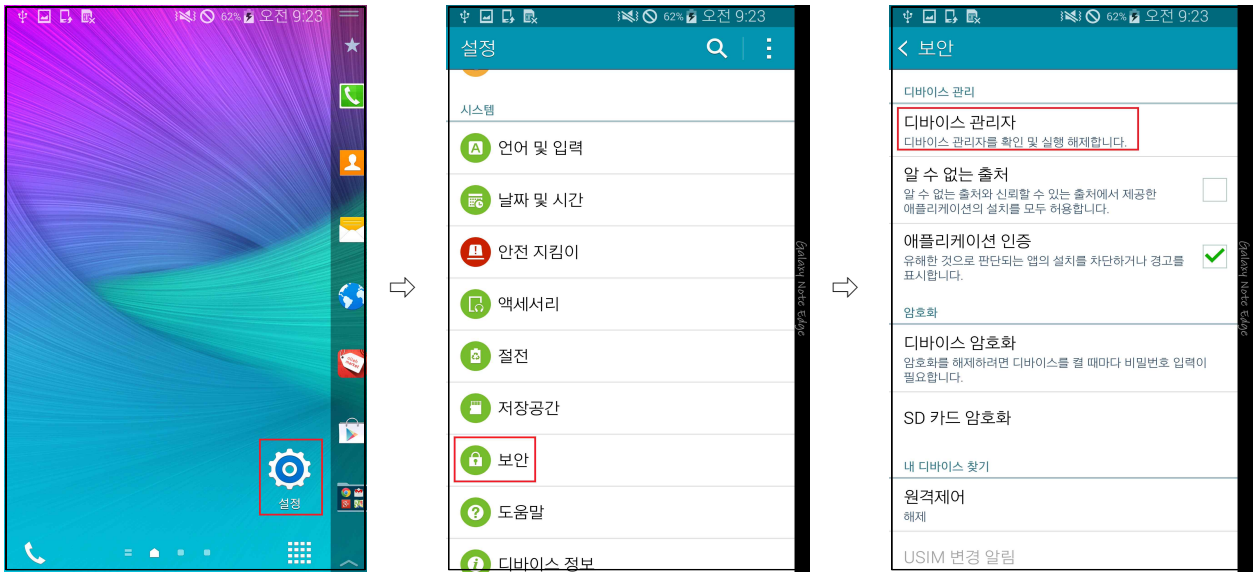


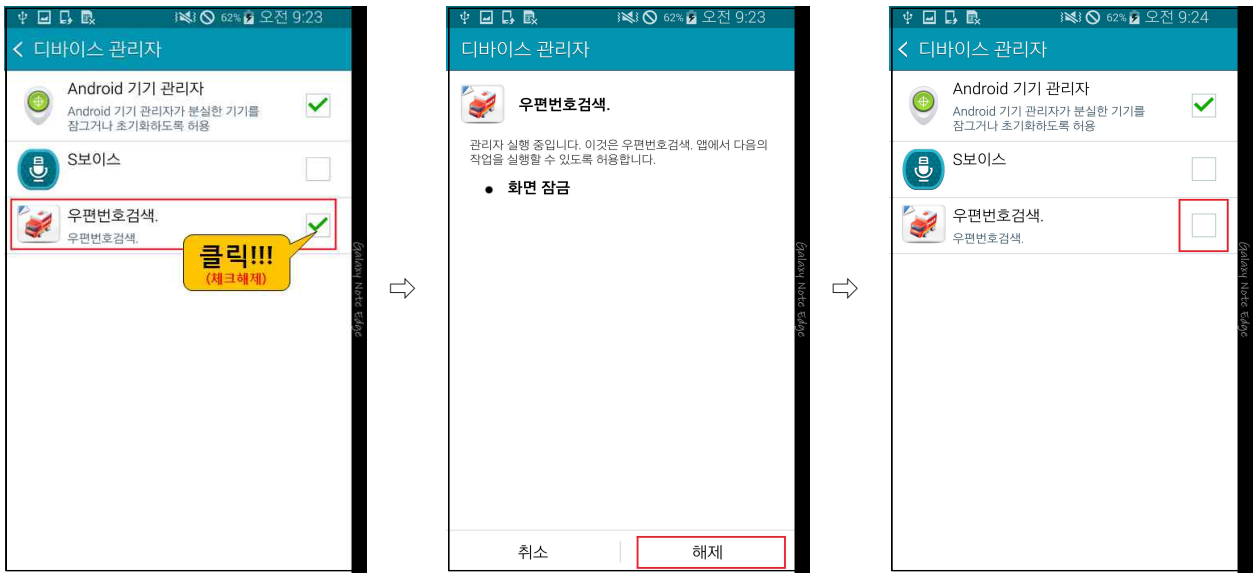
2. 기기 관리자 권한 해제 후 삭제 방법(우편번호검색 사칭 사례)

※ 관리자 메뉴에서 악성(의심) 앱의 관리자 권한 해제 후, 일반적인 악성 앱 삭제 방법과 동일

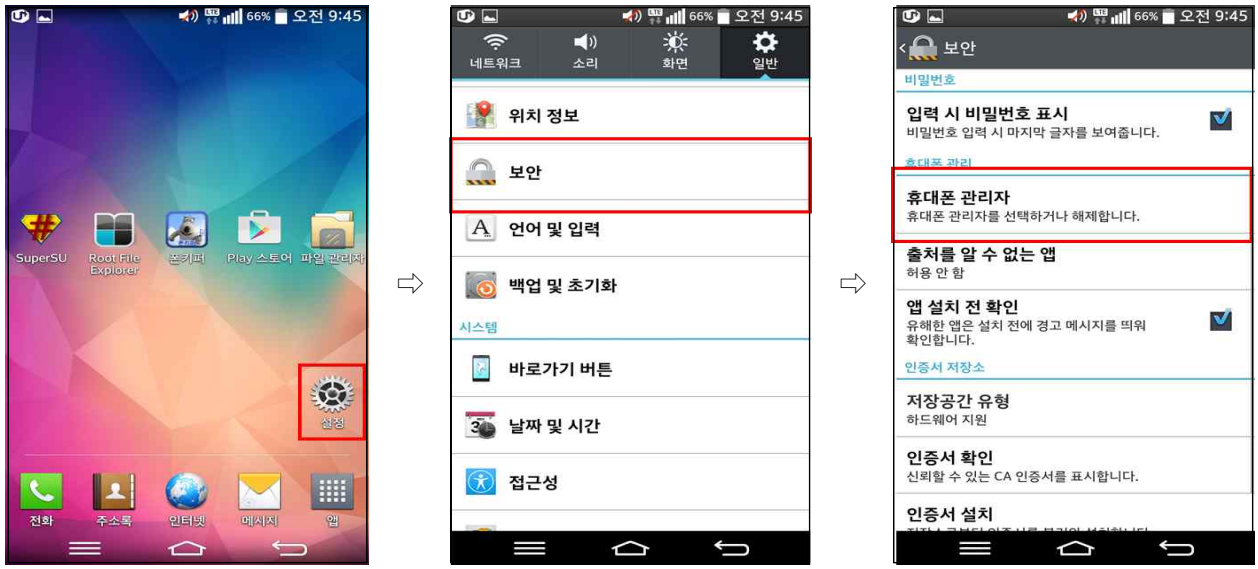
※ 메뉴(탭)명은 스마트폰 제조사별 상이(아래 그림 참고)

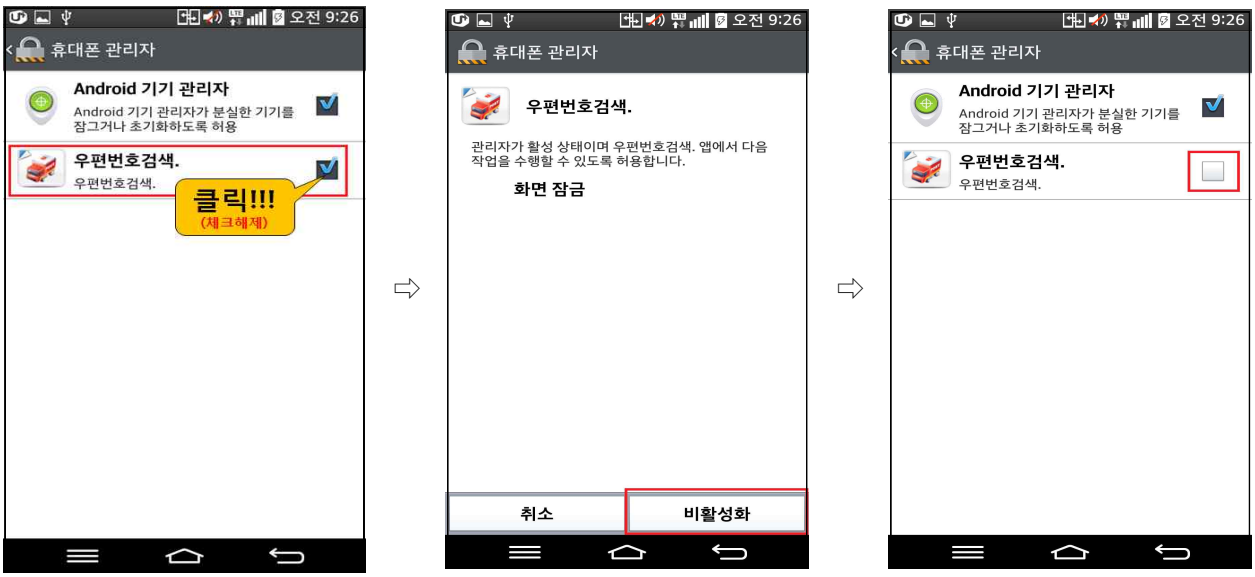
① 삼성 : 설정 → 시스템 → 보안 → 디바이스 관리자(삭제할 앱 선택) → 해제



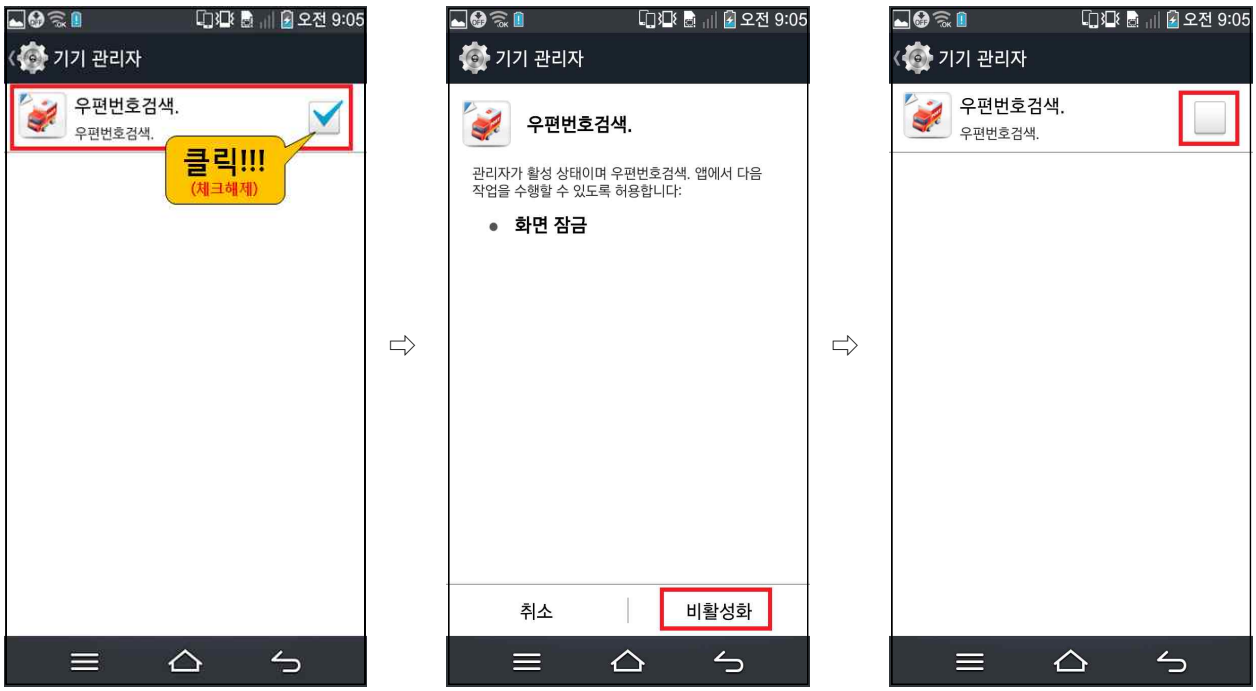


② LG : 설정 → 일반 → 보안 → 휴대폰 관리자(삭제할 앱 선택) → 비활성화





③ **펜택** : 설정 → 개인 설정 → 보안 → 기기 관리자(삭제할 앱 선택) → 비활성화



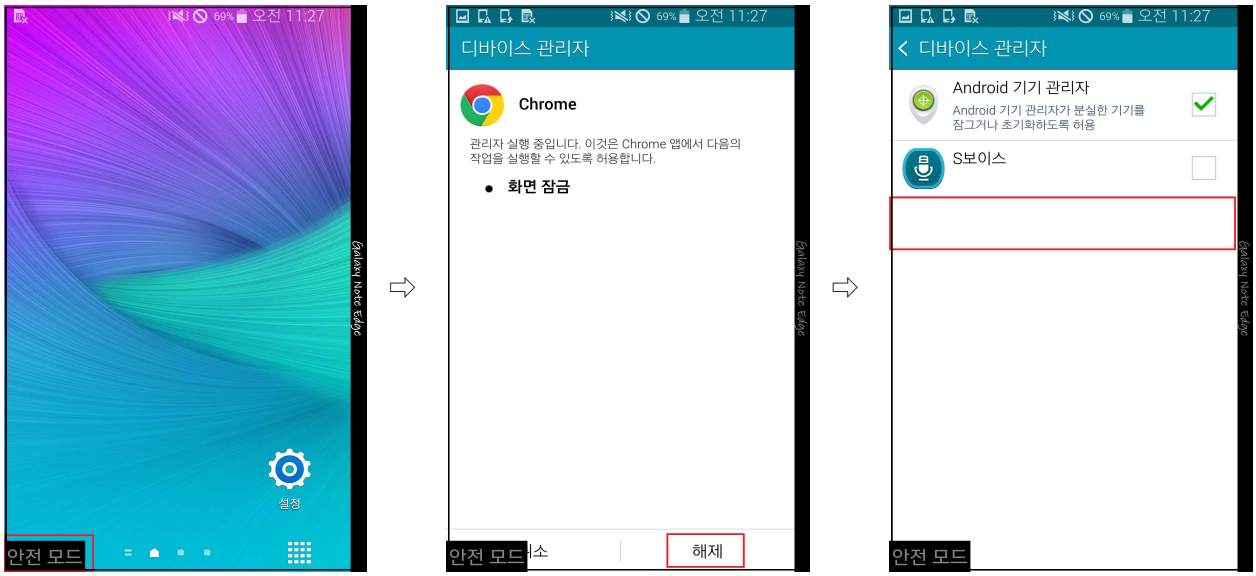
3. 안전모드 부팅을 이용한 삭제 방법(크롬 사칭 사례)

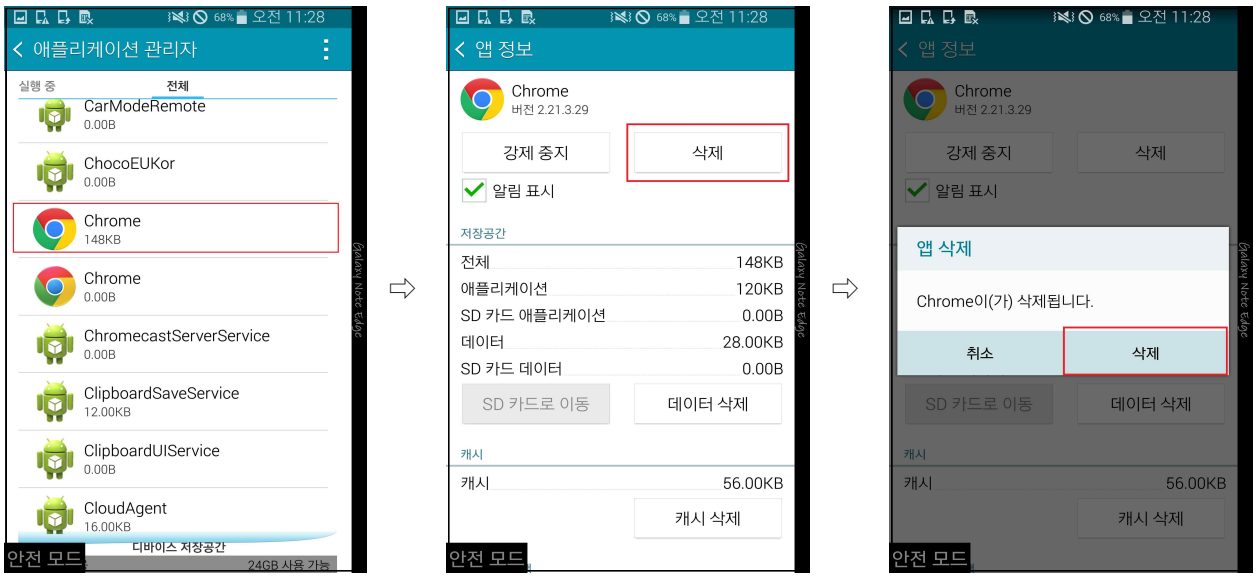
■ 스마트폰을 재부팅하고 통신사 로고가 표기될 때 소리줄임 버튼을 4초 이상 (부팅이 완료될 때까지) 누르고 있으면 안전 모드로 접근 가능

※ 안전모드 부팅을 통한 기기 관리자 권한 해제 이후 절차는 일반적인 악성 앱 삭제 방법과 동일

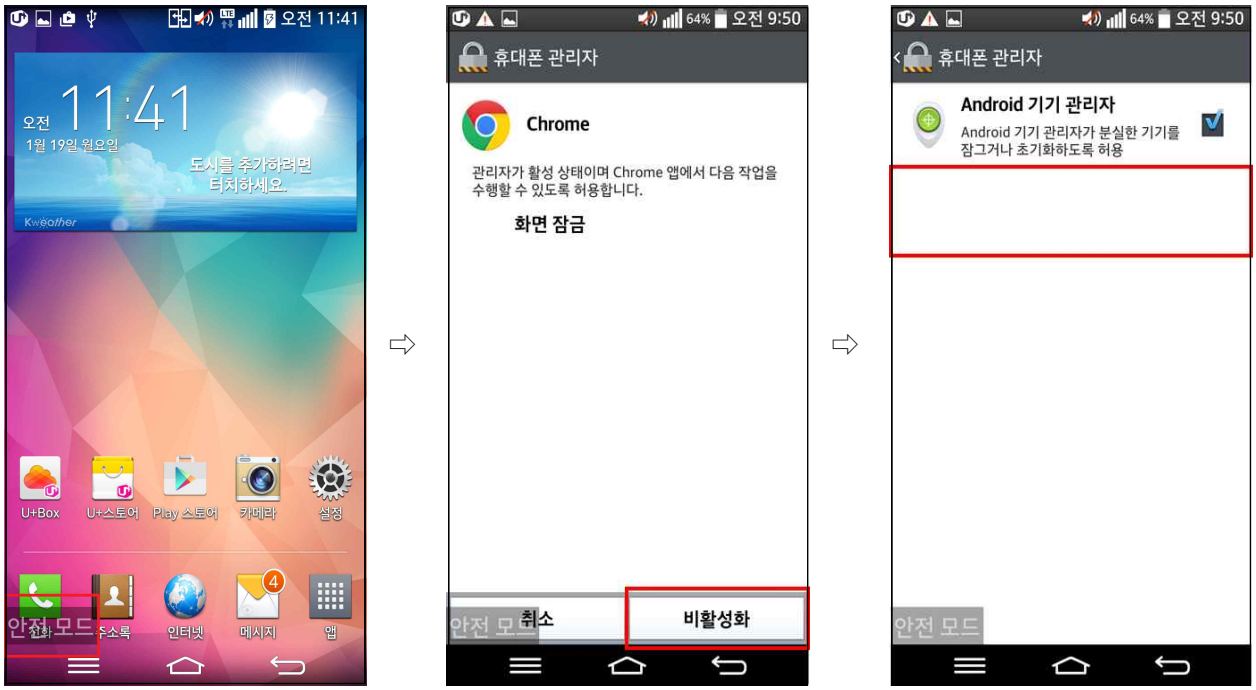
※ 메뉴(탭)명은 스마트폰 제조사별 상이(아래 그림 참고)

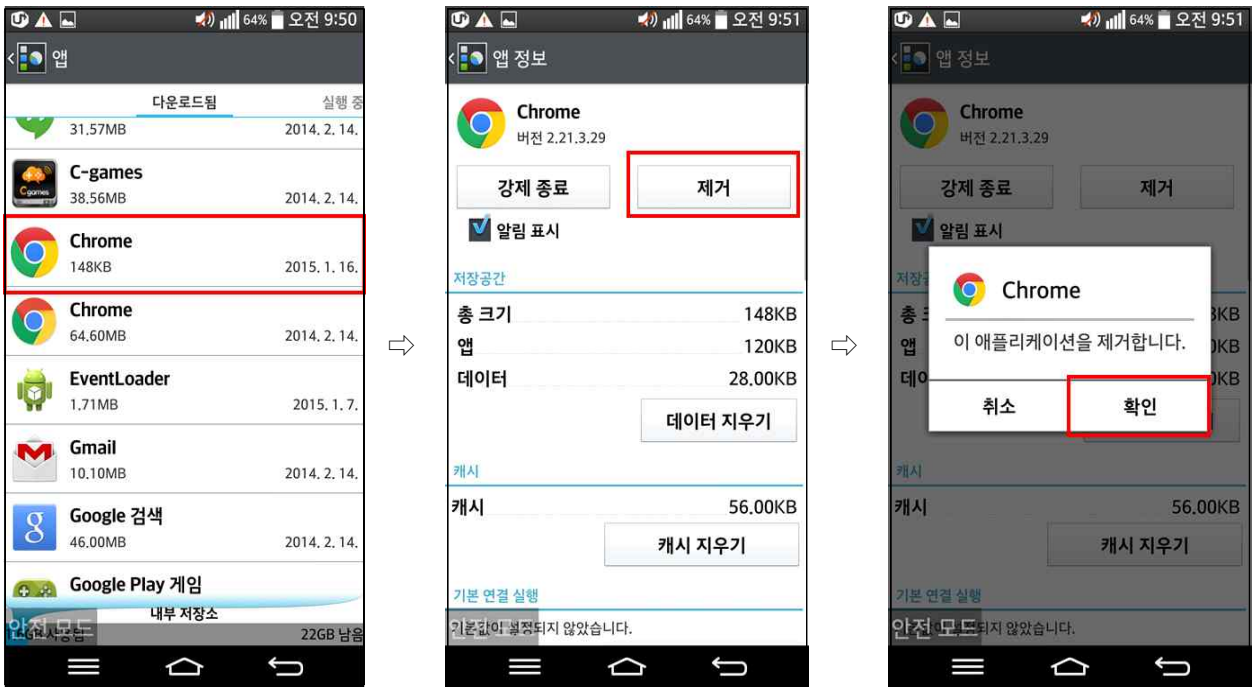
① 삼성 : 안전모드 부팅 → 디바이스 관리자(권한 해제) → 애플리케이션 관리자(악성 앱 삭제)





② LG : 안전모드 부팅 → 휴대폰 관리자(권한 비활성화) → 앱(악성 앱 제거)





③ 펜택 : 안전모드 부팅 → 기기 관리자(권한 비활성화) → 애플리케이션 관리(악성 앱 제거)