컴퓨터 사용자를 위한 월간 정보보호 인식 뉴스레터

OUCH!

이달 호 주제..

- 개요
- 앱 설치
- 권한 허가
- 앱 업데이트

모바일 앱 안전하게 사용하기

개요

태블릿 및 스마트폰과 같은 모바일 기기는 개인 및 직장 생활에서 사용하는 주요 기술 중 하나가 되었다. 모바일 기기가 유용한 이유는 모바일 기기에서 수백만 개의 앱을 사용할 수 있기 때문이다. 이러한 앱을 통해 생산적인 일을 할 수 있고, 다른 사람과 통신하고 공유하고, 교육을 받을 수 있고, 게임도 할 수 있다. 하지만 이러한 모바일 앱에도 위험이 함께 있다. 이번 달 호에는 모바일 앱을 안전하게 사용하고 유지하기 위해 취할 수 있는 단계를 소개한다.

객원 편집자

크리스 크롤리는 독립적인 컨설턴트, SANS 공인강사 및 과정 저자이다. 크리스는 트위터 @CCrowMontance 및 구글 플러스 +ChrisCrowley에서 활동하고 있다.

모바일 앱 설치

첫 번째 단계는 안전하고 신뢰하는 곳에서 앱을 다운로드하는 것이다. 누구나 모바일 앱을 만들 수 있다는 점을 기억해야 한다. 그래서 어디서 앱을 다운로드 받는 지 유의해야 한다. 사이버 범죄자들은 합법적인 것처럼 보이는 악성 모바일 앱을 만들어 배포하고 있다. 만약에 악성 앱을 설치하면, 범죄자들이 우리 모바일 기기를 통제할 수 있고, 이메일을 읽고, 통화내용을 엿듣고, 연락처를 수집할 수 있다. 잘 알려지고, 신뢰하는 곳에서 앱을 다운로드 하면 이러한 악성 앱을 설치할 수 있는 확률을 줄여준다.

아이패드 또는 아이폰과 같은 애플 기기의 경우 애플 앱 스토어라는 곳에서만 앱을 다운로드 받을 수 있다. 이곳의 장점은 애플에서 모바일 앱 및 개발자에 대해서 보안성을 확인한다. 애플이 나쁜 사람들 또는 악성 앱 모두를 잡지 못하지만, 앱 스토어는 감염된 앱을 설치할 수 있는 위험을 굉장히 줄여준다. 추가로 만약에 애플에서 스토어에서 악성 앱을 찾는다면, 바로 삭제한다. 윈도 폰의 경우에는 이와 유사한 방법을 사용한다.

안드로이드 모바일 기기는 좀 다르다. 안드로이드는 유연하게 인터넷에서 아무 곳에서나 앱을 다운로드할 수 있다. 하지만 이러한 유연성에는 책임감도 따라온다. 즉 모든 앱이 검사 받지 않으므로 어떤 모바일 앱을 다운로드하고 설치해야 하는 지 좀더 유의해야 한다. 구글은 애플과 유사한 구글 플레이라는 앱 스토어를 운영하고 있다. 구글 플레이에서 다운로드하는

모바일 앱 안전하게 사용하기

모바일 앱은 기본적인 검사를 수행한다. 그래서 안드로이드 기기의 경우에는 구글 플레이와 같은 안전한 곳에서 다운로드하기를 권고한다. 사이버 범죄자를 포함하여 누구나 악성 모바일 앱을 만들고 배포할 수 있으며, 그래서 모바일 기기를 감염시킬 수 있으므로 다른 웹사이트에서 안드로이드 모바일 앱을 다운로드하는 것을 피하는 것이 좋다. 추가적인 보호방법으로 모바일 기기에 안티 바이러스를 설치하는 것도 고려할 수 있다.

모바일 앱을 안전하게 이용하는 핵심내용은 신뢰할 수 있는 곳에서 앱을 설치하고, 최신의 앱을 사용하고, 권한을 확인하는 것입니다.

위험을 좀더 줄이기 위해서는 새로 출시되는 앱과 많이 다운로드 하지 않는 것 그리고 긍정적인 평가가 적은 것은 피하는 것이 좋다. 앱이 오래 되었을 수록, 긍정적인 평가 글이 많은 것일수록 앱의 신뢰성이 높아진다. 추가로 사용자가 필요하고 사용하는 것만 설치하는 것이다. 즉 정말 이 앱이 필요한가라는 질문을 해 보는 것이 좋다. 앱에는 잠재적으로 새로운 취약점이 있을 수 있고, 프라이버시 문제가 있을 수도 있다. 만약에 앱을 사용하지 않으면 모바일 기기에서 삭제하는 것이 좋다(나중에 필요하면 다시 설치하면 된다.)

마지막으로 모바일 기기를 탈옥(jailbreak)하거나 루팅(root) 유혹에 빠질 수 있다. 이 방법은 모바일 기기를 해킹하여 비인가 앱을 설치하고 기본 탑재 기능을 변경하는 것이다. 그렇게 하면 모바일 기기에 탑재된 많은 보안 기능을 우회하거나 삭제할 뿐만 아니라, 기술 지원을 받을 수 없게 되므로 탈옥하거나 루팅하는 것을 추천하지 않는다.

권한 허가

일단 모바일 기기에 신뢰하는 곳에서 앱을 설치한 후에는 안전하게 설정하고 프라이버시를 보호하는 것이다. 모바일 앱을 설치하고 환경 설정하는 것은 권한을 설정하는 것이다. 앱이 어떤 정보에 접근하고자 하는 것을 승인하기 전에 이 앱이 이러한 권한이 정말 필요한지를 고민해봐야 한다. 예를 들어 일부 앱은 위치정보를 이용한다. 만약에 이 앱에 우리의 위치를 알게 하면, 앱 개발자가 우리의 이동을 추적할 수 있게 된다. 그래서 이 위치정보를 다른 사람에게 판매할 수 있다. 만약에 앱이 요청하는 권한을 허가하기 싫다면, 다른 앱을 구하는 것이 좋다. 유사한 기능을 가진 다른 앱도 굉장히 많다. 애플 기기의 경우 위치 정보에 접근하는 것과 같은 접근 권한이 설정 또는 실행 시 변경되도록 하고 있다. 윈도와 안드로이드 모바일 기기는 전체 허가 아니면 전체 불가 방식으로 사용자게 보여준다. 만약에 모든 특정 권한을 허가하지 않는다면 앱을 설치할 수 없게 된다.

모바일 앱 안전하게 사용하기

앱 업데이트

컴퓨터와 모바일 기기 운영체제와 마찬가지로 모바일 앱을 현재 상태를 유지하기 위해 반드시 업데이트해야 한다. 사이버 범죄자들은 앱의 취약점을 지속적으로 찾고 있다. 범죄자들은 이러한 취약점을 공격하기 위해 익스플로잇을 개발한다. 앱을 만든 개발자들은 이러한 취약점을 패치하기 위해 업데이트를 발표하여 기기를 보호한다. 자주 업데이트 사항을 확인하고 설치할수록 안전하게 사용할 수 있다. 대부분의 운영체제는 모바일 앱을 자동적으로 업데이트할 수 있도록 설정할 수 있다. 자동 업데이트할 수 있도록 설정하는 것이 좋다. 만약에 이 방법을 사용할 수 없다면 적어도 2주에 1회는 모바일 앱의 업데이트를 확인해야 한다. 하지만 모바일 앱이 업데이트될 때, 앱이 요구하는 접근 권한도 함께 확인해야 한다.

자세히 알아 보기

http://www.securingthehuman.org를 방문해서 OUCH! 뉴스레터를 읽어 보시고, 월간 OUCH! 정보보호지식 뉴스레터를 구독하십시오. 그리고 SANS 정보보호지식 솔루션에 대해서 좀 더 알아보시기 바랍니다.

한글판

본 문서는 한국의 ITL(http://www.itlkorea.kr)에서 번역하였습니다. ITL 은 미국 SANS 연구소의 한국 파트너로서 IT 거버넌스 및 IT 보안 분야의 최신의 지식과, 양질의 교육과 세미나를 진행하는 교육기관입니다. 추가적인 사항은 itl@itlkorea.kr 로 문의해주시기 바랍니다.

참고자료

사회공학:	http://www.securingthehuman.org/ouch/2014#november2014
모바일 기기 폐기하기:	http://www.securingthehuman.org/ouch/2014#june2014
태블릿 컴퓨터 보안:	http://www.securingthehuman.org/ouch/2013#december2013
공통 보안 용어:	http://www.securingthehuman.org/resources/security-terms
SEC575: 모바일 기기 보안 과정:	http://www.sans.org/sec575

편집위원회 : Bill Wyman, Walt Scrivens, Phil Hoffman, Lance Spitzner, 번역: 진수희(ITL Inc.)