

컴퓨터 사용자를 위한 월간 정보보호 인식 뉴스레터

# OUCH!

이달 호 주제..

- 개요
- 태블릿 보안설정
- 보안유지방법

## 태블릿 컴퓨터 보안

### 개요

먼저 새로운 태블릿을 가지게 된 것을 축하 드립니다. 태블릿은 온라인 쇼핑, 영화 감상, 게임 등 다양한 활동을 할 수 있는 강력하고 편리한 기술입니다. 태블릿은 우리의 일상생활에서 중요한 역할을 하고 컴퓨터를 대체하고 있기 때문에 우리는 이것을 안전하게 사용하기 위한 몇 가지 단계를 취할 것을 권고합니다.

### 객원 편집자

로리 로젠버그는 정보보호 교육 및 훈련 교재 개발에 많은 경험을 가지고 있다. 지식을 공유하기 위한 새로운 방법을 찾는데 관심이 많다. 트위터 @InfoSecLori 에서 로젠버그에 대한 더 많은 정보를 얻을 수 있다.

### 태블릿 보안설정

태블릿 컴퓨터의 가장 큰 위험은 해커가 아니라, 바로 이용자 자신입니다. 분실할 가능성이 크고, 그렇게 되면 누군가가 태블릿 컴퓨터를 해킹할 수 있습니다. 태블릿을 보호하기 위해 해야 하는 첫 번째는 스크린을 자동 잠금으로 설정하는 것입니다. 이 말은 태블릿을 사용할 때 마다 강력한 패스워드, 패턴인식 또는 지문으로 스크린 잠금을 해제해야 합니다. 이렇게 하면 태블릿을 분실하더라도 다른 사람들이 접근할 수 없으며, 개인정보, 모바일 앱 등을 보호할 수 있습니다. 자동 스크린 잠금을 설정했다면, 새로운 태블릿을 보호할 수 있는 다른 팁이 있습니다.

1. 인터넷으로 태블릿을 원격으로 추적할 수 있는 소프트웨어를 설치하고 활성화 해야 합니다. 태블릿이 분실하더라도 이렇게 하면, 인터넷으로 연결할 수 있으며, 위치를 찾을 수 있으며, 최악의 경우 원격으로 정보를 삭제할 수 있습니다.
2. 기기를 업그레이드하고, 자동 업데이트 설정합니다. 이렇게 하면 최신의 운영체제를 사용할 수 있습니다. 공격자들은 항상 소프트웨어 취약점을 찾고 있으며, 벤더들은 취약점을 수정하기 위해 항상 업데이트를 발표하고 있습니다. 최신의 운영체제 및 모바일 앱을 실행하면 태블릿 해킹이 훨씬 더 어렵게 됩니다.
3. 처음으로 태블릿을 설정할 때 유의하시기 바랍니다. 특히 프라이버시 설정에 유의 바랍니다. 태블릿의 가장 큰 프라이버시 문제는 다른 사람들이 우리의 위치를 추적해서 알 수 있다는 것입니다. 그래서 모든 것에 대해서

## 태블릿 컴퓨터 보안

위치 추적을 비활성화하고, 반드시 필요한 것만 사용바랍니다. 지도 또는 지역의 식당을 찾는 것과 같은 일부 앱은 위치 추적하는 것이 중요하지만, 대부분의 앱은 실시간 위치 정보가 필요하지 않습니다.

4. 대부분의 태블릿 및 앱은 클라우드에 정보를 저장합니다. 이 경우, 데이터가 어디에 저장되는 어떻게 보호되는 지 이해가 필요합니다. 예를 들어 위치정보까지 포함된 개인적인 사진이 전세계 사람들이 볼 수 있도록 공유되는 것은 끔찍한 일입니다. 기본적으로 클라우드에 정보를 공유하는 것은 사용하지 않는 것이 좋으며, 필요한 경우에만 설정할 필요가 있습니다.

5. 태블릿은 앱을 다른 스마트폰이나 노트북 컴퓨터와 동기화합니다. 동기화는 좋은 기능이지만, 어떤 앱을 동기화할 지는 주의가 필요합니다. 만약에 동기화

기능이 설정되어 있다면, 사무실의 브라우저 등에 우리가 방문한 사이트가 그대로 나타나게 됩니다.



가장 좋은 태블릿 보안 방법은 스크린 잠금을 설정하고, 프라이버스 설정을 검토하고, 태블릿을 최신의 상태로 업데이트하는 것입니다.

## 보안 유지 방법

일단 태블릿이 보안조치를 했다면 태블릿의 보안을 유지해야 합니다. 태블릿을 오랫동안 안전하게 유지하는 핵심 단계를 소개합니다.

- 태블릿에 탈옥하거나 해킹하지 마십시오. 이렇게 하면 많은 보안 기능들이 우회되고 무력화 되어 공격에 취약하게 만드는 것입니다.
- 신뢰되는 소스로부터 필요한 앱만 다운로드 하시기 바랍니다. 아이패드의 경우 아이튠즈에서만 다운로드할 수 있습니다. 애플에서 앱들이 공개되기 전에 검증을 합니다. 구글의 경우 구글 플레이에서만 앱을 다운로드하고, 아마존 태블릿은 아마존 앱 스토어에서만 다운로드 하시기 바랍니다. 다른 사이트에서 앱을 다운로드 할 수 있지만, 이러한 앱들은 검증되지 않은 것이며, 악성 코드가 포함되어 있을 수 있습니다. 마지막으로 앱을 다운로드 받는 곳과 상관없이 앱이 더 이상 필요 없거나 사용하지 않는다면, 태블릿에서 삭제하시기 바랍니다.

## 태블릿 컴퓨터 보안

- 새로운 앱을 설치 시에는, 새로운 태블릿을 구성할 때 한 것처럼 프라이버시 옵션을 설정하시기 바랍니다. 앱이 어떤 정보에 접근할 수 있도록 할 지 유의바랍니다. 예를 들어 다운로드한 앱이 정말 모든 연락처에 접근할 필요가 있는가? 만약에 앱의 접근 권한을 변경할 수 있다면, 다른 방법을 찾아보시기 바랍니다. 추가로 주기적으로 접근 권한을 확인이 필요합니다.

태블릿은 실생활에서 유용한 강력한 도구입니다. 위의 보안 단계를 기억하면, 새로운 태블릿을 안전하게 오랫동안 사용할 수 있습니다.

## 자세히 알아 보기

<http://www.securingthehuman.org>를 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](mailto:itl@itlkorea.kr) 로 문의해주시기 바랍니다.

## 참고자료

모바일 앱 안전하게 사용하기:	<a href="https://www.securingthehuman.org/ouch/2015#january2015">https://www.securingthehuman.org/ouch/2015#january2015</a>
패스워드:	<a href="https://www.securingthehuman.org/ouch/2015#april2015">https://www.securingthehuman.org/ouch/2015#april2015</a>
클라우드 안전하게 사용하기:	<a href="https://www.securingthehuman.org/ouch/2014#september2014">https://www.securingthehuman.org/ouch/2014#september2014</a>
모바일 기기 안전하게 폐기하기:	<a href="https://www.securingthehuman.org/ouch/2014#june2014">https://www.securingthehuman.org/ouch/2014#june2014</a>
SANS 일일 보안팁:	<a href="https://www.sans.org/tip_of_the_day.php">https://www.sans.org/tip_of_the_day.php</a>

OUCH!는 SANS Securing The Human 프로그램에 의해 발행되며 [Creative Commons BY-NC-ND 4.0](https://creativecommons.org/licenses/by-nc-nd/4.0/) 라이선스로 배포됩니다 이 문서는 출처를 밝히고, 상업적 목적 또는 수정하지 않는다면 자유롭게 배포할 수 있습니다. 번역 및 추가 문의 사항이 있으시면 [ouch@securingthehuman.org](mailto:ouch@securingthehuman.org) 로 연락 주시기 바랍니다.

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



[securingthehuman.org/blog](http://securingthehuman.org/blog)



[/securethehuman](https://www.facebook.com/securethehuman)



[@securethehuman](https://twitter.com/securethehuman)



[securingthehuman.org/gplus](https://www.securingthehuman.org/gplus)