

# OUCH!

## 이달 호 주제..

- 사전 점검
- 분실/도난 기기
- 와이파이 이용
- 공용 컴퓨터

## 여행중 인터넷 안전하게 이용하기

### 개요

이번 달 뉴스레터에서는 여행 중 인터넷을 안전하게 접속하는 방법 및 준비사항에 대해서 다룬다.

### 사전 점검

가정이나 직장의 네트워크는 안전할 수 있지만, 여행할 때 접속하는 네트워크는 신뢰할 수 없다는 것을 이해해야 한다. 왜냐하면 누가 네트워크에 접속되어 있는 지, 어떤 위협이 있는지 알 수가 없기 때문이다. 일부 간단한 여행 전 조치를 통해 여행 중 데이터를 보호할 수 있다. 여행 출발 1-2 주전에는 다음과 같은 사항을 점검해야 한다.

### 객원 편집자

스티브 암스트롱은 CyberCPR 기술이사이며, SANS 공인강사 및 SANS교육과정 저자이다. 스티브는 트위터 [@Nebulator](#) 및 구글플러스 [+SteveArmstrongSecurity](#) 에서 활동하고 있다.

- 여행할 때 챙겨가는 기기에 필요 없는 데이터가 무엇인지 파악하고, 불필요한 정보는 삭제한다. 이렇게 하면 기기가 분실되거나 도난 되거나 세관에 압수되더라도 영향을 줄일 수 있다. 만약에 업무관련 여행이라면, 회사에서 출장 시 사용할 수 있는 기기가 있는 지 회사에 문의해 볼 수 있다.
- 해외 여행의 경우, 방문 국가의 전기 어댑터가 어떤 종류인지 미리 확인해야 한다. 어댑터가 맞지 않으면 기기를 충전하기 위해 어댑터를 구매해야 한다. 추가로 핸드폰의 경우 모바일 서비스 회사에서 어떤 서비스를 받을 수 있는지 확인이 필요하다. 일부에는 모바일 서비스 회사에서 국제 데이터 사용시 높은 요금을 부과할 수 있으므로, 이 경우 국제 여행시에는 셀룰라 데이터 기능을 꺼두는 것이 좋다.
- 기기에 소프트웨어를 설치해서, 기기를 분실하거나 도난 되었을 때, 원격에서 기기 위치를 추적하고, 원격에서 데이터를 삭제할 수 있도록 한다. 대부분의 모바일 기기들은 이러한 기능이 포함되어 있으므로, 기능을 활성화하기만 하면 된다(기능을 활성화하려면 인터넷 접속이 가능해야 한다.)

### 여행출발 1-2일 전:

- 기기의 운영체제, 애플리케이션 및 안티바이러스 소프트웨어를 최신으로 업데이트하여 최신 버전으로

## 여행중 인터넷 안전하게 이용하기

운영되도록 한다.

- 방화벽과 같이 기기의 보안설정사항을 확인하여 활성화한다.
- 모바일 기기의 경우 강력한 패스워드로 잠금을 설정한다. 이렇게 하면 기기를 분실하거나, 도난되더라도 사람들이 기기에 있는 정보에 접근할 수 없다.
- 기기의 모든 정보를 암호화하여 분실, 도난시 데이터 접근을 차단할 수 있다. 아이폰과 같은 일부 기기는 기기의 패스워드를 설정하면 자동으로 데이터를 암호화한다.
- 모든 기기의 데이터를 백업한다. 이렇게 하면 여행 중 예상하지 못한 일이 발생해도 모든 데이터를 안전한 장소에 저장해 둘 수 있다.



여행 중 안전하게 인터넷을 이용하기 위해서는 떠나기 전에 기기의 안전을 확보하고, 물리적으로 안전하게 유지하고, 항상 소지여부를 파악하고, 모든 온라인 접속 시 암호화해서 사용해야 한다.

### 분실/도난 기기

일단 여행을 시작하면, 기기의 물리적 안전이 중요하다.

예를 들어 사람들이 쉽게 볼 수 있는 자동차 안에 기기를 두면 안 된다. 범죄자들이 자동차 창문을 부수고, 자동차 안에 있는 귀중품을 훔칠 수 있다. 필요하다면 잠금 케이블을 사용해서, 노트북과 같은 것을 두고 내릴 때는 물리적으로 잠금 장치를 하는 것이 좋다. 사람들이 잘 모르는 있는 점은 기기를 분실할 수 있는 위험이 굉장히 높다는 것이다. 버라이즌사에서 10년간 연구한 결과, 사람들은 15회 이상 기기를 분실하거나 도난 당한다는 것이다. 즉 여행 중 공항에서 보안검사대를 통과할 때, 택시나 식당을 떠날 때, 호텔을 체크아웃할 때, 비행기에서 내릴 때는 항상 기기를 잘 챙겼는지 확인해야 한다.

### 와이파이 이용

여행 중에는 호텔이나, 커피숍 또는 공항의 공공 와이파이 AP를 이용하여 인터넷에 접속한다. 공공 와이파이 AP의 문제점은 누가 설치를 했는지, 누가 접속해서 사용하고 있는 지 알 수가 없다는 것이다. 그래서 공공 와이파이에는 안전하지 않다는 것이다. 그래서 기기를 안전하게 하기 위해서는 가능한 조치를 취해야 한다. 추가로 와이파이는 기기와 무선 AP간 무선 주파수를 사용하여 통신을 한다. 그래서 물리적으로 근처에 있는 누구나 통신을 가로채거나 모니터링할 수 있다.

그래서 공공 와이파이를 사용하는 경우, 모든 온라인 접속 활동은 암호화해야 한다. 예를 들어 브라우저를 이용해서 인터넷 사이트에 접속할 때, 방문하는 웹사이트가 암호화하고 있는지 확인해야 한다(URL에 https:// 를 사용하고 잠금 장치 이미지가 있다). 추가로 VPN(가상사설망)이라고 하는 계정을 사용해서 온라인 접속을 암호화할 수 있다. VPN 계정은

## 여행중 인터넷 안전하게 이용하기

회사에서 발급받을 수도 있고, 개인적인 용도로 VPN 계정을 구매할 수 있다. 만약에 믿을 만한 와이파이 AP가 없다면, 스마트폰 테더링을 사용하는 것도 괜찮다(하지만 앞에서 언급했듯이 국제 데이터 통신 요금은 굉장히 비쌀 수 있으므로, 먼저 통신회사에 연락해서 확인을 해보아야 한다.)

### 공용 컴퓨터

호텔 로비, 도서관, 카페 등에 있는 컴퓨터는 사용하지 않는 것이 좋다. 왜냐하면 그러한 컴퓨터를 누가 이용했는지 전혀 모르며, 누가 고의적으로 공용 컴퓨터를 감염시켰을 수도 있다. 가능하다면 자신의 컴퓨터 기기를 사용하고, 믿을 수 있는 것만 사용해야 한다. 만약에 공용 컴퓨터를 사용해야 한다면, 패스워드 입력이 필요한 서비스를 절대로 이용하면 안된다.

### 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

- 패스워드: <http://www.securingthehuman.org/ouch/2013#may2013>
- 2단계 인증: <http://www.securingthehuman.org/ouch/2013#august2013>
- 암호: <http://www.securingthehuman.org/ouch/2014#august2014>
- 태블릿 컴퓨터 보안: <http://www.securingthehuman.org/ouch/2013#december2013>
- 버라이즌 DBIR 2014: <http://www.verizonenterprise.com/DBIR/2014/>

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://plus.google.com/securethehuman.org)