OUCH! | 2017 년 2 월호

전 국민대상 월간 정보보호 인식제고 뉴스레터

OUCH!

이달 호 주제..

- 사전 점검
- 분실/도난
- 와이파이 이용
- 공용 컴퓨터

여행 중 인터넷 안전하게 이용하기

개요

우리는 평소 또는 여행 중에도 항상 최고의 기술을 이용하기를 원한다. 이번 달 뉴스레터에서는 여행 중 인터넷을 안전하게 접속하는 방법 및 IT기기를 안전하게 사용하는 방법에 대해서 다룬다.

객원 편집자

마크 윌리엄스는 블루크로스 블루쉴스사의 기업보안 아키텍트입니다. 마크는 또한 SANS 강사 및 ISSA 차타누가 챕터의 의장입니다. 마크는 굉장히 많은 여행을 하였으며, 여행하면서 소지하는 IT 기기로 인해 발생하는 문제에 대해서 잘 알고 있습니다.

사전 점검

가정이나 직장의 네트워크는 안전할 수 있지만, 여행할 때 접속하는 네트워크는 신뢰할 수 없다는 것을 가정해야 한다. 왜냐하면 누가 네트워크에 접속되어 있는 지, 접속해서 사용하는 사람들이 무엇을 하고 있는 지 알 수 없기 때문이다. 여행하기 전에 우리자신과 데이터를 보호할 수 있는 간단한 단계는 다음과 같다.

- 정보를 지키는 가장 안전한 방법은 가지고 있지 않는 것이다. 여행할 때 챙겨가는 기기에 필요 없는 데이터가 무엇인지 파악하고, 불필요한 정보는 삭제한다. 이렇게 하면 기기가 분실되거나 도난 되거나 세관 또는 국경에서 압수되더라도 영향을 줄일 수 있다. 만약에 업무와 관련된 여행이라면, 회사에서 출장 시에만 사용할 수 있는 기기가 있는 지 회사에 문의해 볼 수 있다.
- 모바일 기기 및 노트북 컴퓨터에 강력한 패스워드로 잠금을 설정한다. 이렇게 하면 기기를 분실하거나, 도난 되더라도 사람들이 기기에 있는 정보에 접근할 수 없다. 추가로 모바일 기기 및 노트북 컴퓨터에 디스크 전체 암호기능을 설정하는 것이다. 대부분의 모바일 기기는 스크린 잠금을 하면, 자동적으로 이 기능이 설정된다.
- 기기에 소프트웨어를 설치해서 기기를 분실하거나 도난 되었을 때, 원격에서 기기의 위치를 추적하고, 원격에서 데이터를 삭제할 수 있도록 한다
- 출발하기 전에 IT 기기의 운영체제, 애플리케이션 및 안티바이러스 소프트웨어를 최신으로 업데이트한다. 많은 공격이 오래된 소프트웨어 취약점이 있는 시스템을 노린다.

여행 중 인터넷 안전하게 이용하기

- 모든 기기의 데이터를 백업한다. 이렇게 하면 여행 중 예상하지 못한 일이 발생해도 모든 데이터를 안전한 장소에 저장해 둘 수 있다.
- 해외 여행의 경우, 핸드폰의 경우 모바일 서비스 회사에서 어떤 서비스를 받을 수 있는 지 확인이 필요하다. 일부에는 모바일 서비스 회사에서 국제 데이터 사용시 높은 요금을 부과할 수 있으므로, 이 경우 해외 여행시에는 셀룰라 데이터 기능을 꺼두거나, 해외여행자를 위한 선불 SIM 카드를 구매하는 것이 좋다.

여행 중 안전하게 인터넷을 이용하기 위해서는 떠나기 전에 기기의 안전을 확보하고, 물리적 안전을 유지하고, 모든 온라인 활동에 대해 암호화 기능을 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. 사람들이 잘 모르는 있는 점은 기기를 분실할 수 있는 위험이 굉장히 높다는 것이다. 최근 버라이존사의 연구에 따르면 10년간 연구한 결과, 사람들은 100회 이상 기기를 분실하거나 도난 당한다는 것이다. 여행할 때는 항상 모바일 기기를 잘 챙겼는 지 확인, 재확인해야 한다. 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 와이파이는 두 가지 문제가 있다. 누가 설치를 했는지, 누가 접속해서 사용하고 있는 지 알 수가 없다는 것이다. 그래서 공공 와이파이는 안전하지 않다는 것이다. 그러므로 떠나기 전에 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 모니터링 할 수 있다. 이러한 이유로, 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 회사에서 발급받을 수도 있고, 개인적인 용도로 VPN 계정을 구매할 수 있다. 만약에 믿을 만한 와이파이 AP가 없다면, 스마트폰 테더링을

여행 중 인터넷 안전하게 이용하기

사용하는 것도 괜찮다(하지만 앞에서 언급했듯이 국제 데이터 통신 요금은 굉장히 비쌀 수 있으므로, 먼저 통신회사에 연락해서 확인을 해봐야 한다.)

공용 컴퓨터

호텔 로비, 까페 등에 있는 컴퓨터는 사용해서 민감한 정보에 접근하기 위해 계정에 로그인하지 않는 것이 좋다. 왜냐하면 전에 이 컴퓨터를 누가 이용했는지 전혀 모르며, 누가 고의적으로 공용 컴퓨터를 감염시켰을 수도 있다. 가능하다면 자신의 컴퓨터 기기를 사용하고, 믿을 수 있는 것만 사용해야 한다. 공용 컴퓨터는 날씨 확인 및 뉴스를 본다던가 일반적인 정보를 확인하는 것으로만 사용하는 것이 최선이다. 네이버 등 계정에 로그인을 하는 데 사용한다면, 해커를 초대하는 꼴이 될 수 있다.

자세히 알아 보기

securingthehuman.sans.org/ouch/archives를 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

패스워드:	http://www.securingthehuman.org/ouch/2015 #april2015
백업:	https://securingthehuman.sans.org/ouch/2015#august2015
악성코드:	https://securingthehuman.sans.org/ouch/2016#march2016
암호:	https://securingthehuman.sans.org/ouch/2016#june2016
OUCH 뉴스레터:	https://securingthehuman.sans.org/ouch/archives

편집위원회 : Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis, Cheryl Conley, 번역:진수희(ITL Inc.)