

컴퓨터 사용자를 위한 월간 정보보호 인식 뉴스레터

# OUCH!

이달 호 주제..

- 배경
- 위험
- 아이들 교육

## 사이버안전에 대한 아이들 교육방법

### 배경

최근에는 아이들은 온라인에 접속하고, 다른 사람들과 교류할 수 있는 다양한 방법들이 존재하고 있다. 새로운 소셜 미디어 서비스는 잡초처럼 불쑥 나오고, 수많은 온라인 앱이나 게임이 나타난다. 추가로 많은 학교에서는 인터넷 공유 드라이브와 같은 서비스로 이동하고 있으며, 숙제들이 온라인으로 제출하도록 한다. 아이들은 글자 그대로 “항상 연결”되어 있으면서 자라난다. 이런 것은 장점도 많지만, 위험도 따른다. 이번 달호에서는 아이들이 직면한 세가지 위험을 살펴보고 아이들을 안전하게 할 수 있는 방법을 제시한다.

### 객원 편집자

밥 루디스는 버라이즌에서 보안 데이터 사이언티스이며, 데이터 침해 조사 보고서 저자이다. 밥은 포춘 100대 회사에서 효과적인 보안 인식제고 프로그램을 구축하고 리드하였다. @hrbrmstr 트위터를 팔로우할 수 있다.

### 위험

- 1. 행동:** 온라인 커뮤니티 또는 가상세계에서 교류할 때, 아이들은 실제 세계에서는 절대로 하지 않을 행동을 할 수 있다. 물리적인 존재가 없기 때문에 특히 아이에게는 강력한 익명성의 힘을 느낄 수 있다. 어린이들은 종종 “사이버 왕따”와 같이 다른 친구들을 괴롭히는 유혹에 빠질 수 있다. 거꾸로 우리의 아이들이 다른 아이들의 고의적인 괴롭힘 대상이 될 수 있다.
- 2. 연락:** 어린이들은 메시지, 온라인 커뮤니티 또는 가상세계에서 놀거나 다른 사람들과 거의 항상 연락하고 있다. 물리적인 존재가 없기 때문에 종종 아이들이 상대방이 다른 사람일 수도 있거나, 이기적인 마음을 가지고 있다는 사실을 잊게 된다. 범죄자들이 어린이인 척하면서 디지털 거리를 활보하며, 온갖 기술을 사용해서 잠재적인 범죄 대상과 관계를 구축한다.
- 3. 콘텐츠:** 비디오, 소리, 이미지 또는 텍스트 기반의 온라인 메시지를 캡처하거나 게시하는 것에는 제한이 없다. 아이들은 결과를 생각하지 않고 자신 또는 다른 가족에 대해서 과도하게 공유하고 싶은 유혹이 실제 존재한다. 다른 사람들이

## 사이버안전에 대한 아이들 교육방법

아이들에게 질문을 하거나 링크를 클릭하도록 요구하면, 아이들은 신분 도용 또는 악성코드 감염 위험에 대해서 알지 못한다. 마지막으로 지금 세상은 일단 온라인에 게시되거나 다른 사람과 공유되면 “취소”할 수 없는 세상에 살고 있다. 아이들은 페이스북, 인스타그램, 카카오톡 등의 게시물이 금방 사라지는 것이라고 생각하지만 이 게시물로 인해 나중에 다시 자신들 또는 가족들을 괴롭힐 수 있다는 것을 모를 수 있다.

### 아이들 교육

아이를 보호할 수 있는 방법은 이야기하는 것이다. 부모들은 아이들이 온라인에서 무엇을 하는지 알아야 한다. 그리고 교육을 통해 온라인의 위험과 자신들을 보호하기 위해서는 무엇을 해야 하는 지 알려주어야 한다.

- 1. 가정에서의 안전:** 가변적이기는 하지만, 가정은 안전한 온라인 행동을 시작할 수 있는 곳이다. 어린이가 더 어릴 때 얘기할수록 더 좋다. 정기적인 대화를 통해 온라인 안전 문제에 대해서 얘기하고, 실제로 발생한 부정적인 사건을 보여준다. 만약에 여러분의 아이들이 무엇을 하는지 모르고 있다면, 물어보아야 한다. 전혀 모르는 척하면서 아이들에게 최신의 기술이 무엇인지 어떻게 사용하는 것인지 보여달라고 요청할 수 있다. 예를 들어 만약에 아이들이 카카오톡을 하고 있다면, 어떻게 사용하는 지 보여달라고 요청하고, 계정을 하나 만들어 달라고 하여 아이들을 팔로우하면서 보면 된다. 이제 아이들이 무엇을 하는 지 관찰하는 것을 배웠기 때문에 아이들이 더 쉽게 얘기할 수 있다. 추가로 모든 온라인 활동은 가정의 거실에서만 하도록 하고 시간을 정해서 사용하도록 해야 한다. 집의 컴퓨터를 거실에 두어 아이들이 위험한 행동을 하지 않도록 한다. 모바일 기기의 경우 거실에 충전소를 두어, 밤에 자로 갈 때는 모바일 기기를 충전하도록 규칙을 정할 수 있다.
- 2. 타인과의 안전:** 어린이들이 집 밖에 있을 때 더 위험해 질 수 있다. 이 경우 아이들한테 어디에 가든 사이버 규칙을 적용하도록 안내해야 한다. 만약에 아이들이 모바일 기기를 가지고 있는 경우 사용 패턴(시간 및 사용량)을 확인하여 집 밖에서는 규칙을 어기는 지도 확인해야 한다. 모든 규칙을 지키게 할 수는 없으나, 모바일 기기가 탈선하고자 할 때 부모의 관심어린 충고가 기억나게 된다.



온라인에서 아이들을 보호할 수 있는 방법은 위험에 대해서 교육하고, 부모들이 아이에게 얘기하는 것뿐만 아니라, 아이들도 부모에게 얘기하는 것입니다.

## 사이버안전에 대한 아이들 교육방법

3. **주위의 도움:** 사이버 세계에서 우리는 혼자가 아니다. 위대한 행위를 감시하기 위해 다른 부모들, 친척, 교사, 친구들과 함께 노력해야 한다. 동네 커뮤니티에서 아이들을 도와주도록 하고, 아이들이 위험한 길로 가는 것을 보는 경우 동네 커뮤니티에서 긍정적인 상호작용을 주도하도록 해야 한다.

마지막으로 아이들이 실수를 하는 경우, 즉시 훈계하는 것보다 자신이 한 실수로부터 배울 수 있는 경험으로 처리해야 한다. 항상 “왜”를 설명하고 아이들이 아직 보지 못할 수 있는 위험으로부터 부모는 보호하려고 한다는 점을 알려주어야 한다. 그리고 아이들이 온라인에서 불편한 일을 겪으면, 스크린 샷으로 저장해서 언제든지 부모에게 얘기할 수 있도록 해야 한다. 아이들이 부적절한 것을 했을 때 부모에게 얘기하는 것이 쉽지 않을 수 있다. 실제 세계에서 자유롭게, 활발하게 의사소통하는 것이 오늘날 디지털 세상에서 아이들을 안전하게 만들 수 있는 가장 좋은 방법이다.

### 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

- 사이버 스마트: <http://www.cybersmart.gov.au/Parents.aspx>  
온가드 온라인: <http://www.onguardonline.gov/topics/protect-kids-online>  
Stay Safe Online: <https://www.staysafeonline.org/stay-safe-online/for-parents/raising-digital-citizens>  
어린이 보호 패널: <http://www.rsaconference.com/media/into-the-woods-protecting-our-youth-from-the-wolves-of-cyberspace>

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/securingthehuman.org)