OUCH! | 2015 년 7 월호

컴퓨터 사용자를 위한 월간 정보보호 인식 뉴스레터

OUCH!

이달 호 주제..

- 개요
- 프라이버시
- 보안

소셜 미디어

개요

페이스북, 트위터, 인스타그램, 링트인과 같은 소셜 미디어는 네트워킹 사이트는 강력한 기능을 제공하며, 전 세계의 사람들을 만나고, 상호 교류 할 수 있도록 해줍니다. 그러나, 이런 모든 기능들이 우리들에게뿐만 아니라 가족, 친구 및 회사에게도 상당한 위험이 따릅니다. 본 뉴스레터에서 어떤 위험들이 있고, 위 사이트들을 안전하게 사용하는 방법에 대해서 논의합니다.

객원 편집자

탄야 배컴은 오랫동안 보안 컨설턴트로 활동하고 있다. 탄야는 10년간 SEC502, SEC542, SEC401, MGT414, AUD507 등 많은 SANS 교육과정 저자 및 강사로 활동하고 있다. 탄야의 트위터는 @tbaccam 이다.

프라이버시

소셜 미디어 일반적으로 우려사항은 바로 우리의 개인정보를 보호하는 것입니다. 잠재적인 위험은 다음과 같습니다.

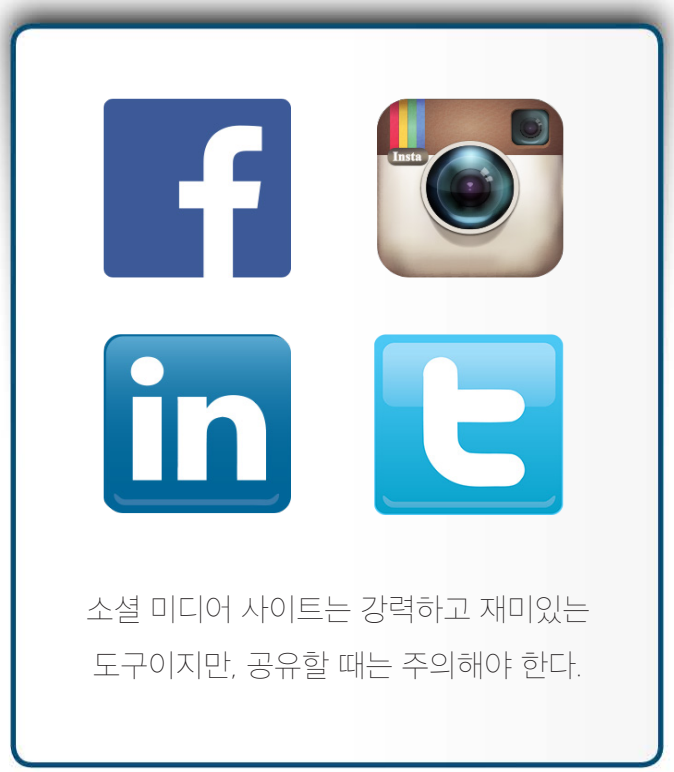
- 미래에 영향을 미침: 많은 기관들이 배경을 알아보는 차원에서 소셜 미디어를 검색합니다. 당혹스럽거나 범죄와 연관있는 게시물이 있다면 아무리 오래된 것이라도 새로운 직업을 구하거나 승진하는데 방해가 될 수 있습니다. 게다가 많은 대학들이 지원 학생들에게도 유사한 방법으로 실시하고 있습니다. 이러한 기관들은 응시 절차 전에 페이지 또는 다양한 사이트에서 저장되어 있는 게시물을 “좋아요” 또는 가입을 했는 지 물어 볼 수 있기 때문에 프라이버시 옵션으로는 보호하지 못할 수 있습니다.
- 자신에 대한 공격: 사이버 범죄자들은 우리의 게시물을 분석하여 우리 자신 또는 회사의 정보에 접근하는데 이용할 수 있습니다. 예를 들어, 웹 사이트에서 수집한 개인정보를 이용해서 “비밀질문”의 답을 추측해서 온라인 패스워드를 재설정하거나, 스피어 피싱과 같은 이메일 공격을 하거나, 우리로 가장하여 회사로 전화할 수 있습니다. 추가로 이러한 공격은 직장 및 집 주소를 알아내어 물리적인 세계에도 침투할 수 있습니다.
- 비고의적으로 회사에 피해를 끼침: 범죄자들 및 경쟁기업들은 회사를 상대로 조직에 대해서 올린 민감한 정보를 사용할 수 있습니다. 우리가 올린 게시물이 의도하지 않게 회사의 평판에 악영향을 끼칠 수 있습니다. 회사에 관한 것을 게시하기 전에는 회사내 소셜 미디어 정책을 반드시 확인하시기 바랍니다. 또한 소셜 미디어 게시물은 모니터링 될 수 있습니다.

가장 좋은 방어책은 게시하는 정보를 제한하는 것입니다. 물론 프라이버시 옵션을 이용하면 일부는 방어가 되지만, 프라이버시 옵션은 복잡하고 우리가 알지 못하는 사이에 자주 변경이 된다는 것을 유의하시기 바랍니다. 우리가 생각하기에는 사적이라고

소셜 미디어

생각하는 것이 다양한 방법으로 공개가 됩니다. 또한 게시물의 프라이버시는 공유한 사람의 수준만큼 안전합니다. 개인정보를 더 많은 사람들과 공유하면 할수록, 정보가 공개될 가능성이 더 높아집니다. 즉 게시한 모든 것은 공개되며, 인터넷에 영원이 남게된다는 것을 가정해야 합니다.

마지막으로 친구들이 우리에 대해서 어떤 정보를 게시하는지도 알아야 합니다. 친구들이 우리에 대해서 개인정보나 민감한 사진을 게시한다면, 내리도록 요청해야 합니다. 친구들이 이것을 거절하면, 소셜 미디어 회사에 연락하여 우리에 관한 게시물을 삭제해 줄 것을 요청하십시요. 동시에 다른 사람에 대한 내용을 게시할 때도 신중하게 하시기 바랍니다.



소셜 미디어 사이트는 강력하고 재미있는 도구이지만, 공유할 때는 주의해야 한다.

보안

프라이버시 문제뿐만 아니라, 소셜 미디어 계정 및 온라인 활동을 보호할 수 있는 단계가 있습니다.

- **로그인**: 강하고 유일한 패스워드로 계정을 보호하고, 다른 사람과 공유하면 안됩니다. 또한 몇몇 소셜 미디어 사이트는 2 중 인증과 같은 강력한 인증 기능을 지원합니다. 가능하면 이러한 좀 더 강한 인증 기능을 사용하시기 바랍니다. 마지막으로 다른 사이트에는 소셜 미디어 계정을 사용하지 말기 바랍니다. 한번 해킹되면, 모든 계정이 취약하게 됩니다.
- **프라이버시 설정**: 만약에 프라버시 설정을 사용하면, 주기적으로 검토하고 시험해야 합니다. 소셜 미디어 사이트는 프라이버시 설정을 자주 변경하며, 실수하기 쉽습니다. 추가로 많은 앱 및 서비스가 게시물의 컨텐츠에 위치정보를 태깅합니다. 물리적인 위치를 노출하고 싶지 않다면 주기적으로 설정사항을 확인해야 합니다.
- **암호**: 소셜 미디어 사이트는 HTTPS 라고 불리는 암호화 기능을 사용해서 사이트와의 연결을 암호화합니다. 트위터 및 구글+ 등 일부 사이트는 기본적으로 암호기능을 제공하며, 일부 사이트는 HTTPS을 직접 설정해야 합니다. 자신이 사용하는 소셜 미디어 계정 설정을 확인하고, 가능하면 항상 HTTPS 기능을 이용하시기 바랍니다.
- **이메일**: 소셜 미디어 사이트에서 온 것으로 보이는 이메일에 있는 링크를 클릭할 때 주의하시기 바랍니다. 이 것은 사이버 범죄자들이 보낸 사기성 공격일 수 있습니다. 이러한 메시지를 대응하는 가장 안전한 방법은 저장된 북마크를 이용해서 직접 웹사이트에 로그인하는 것입니다. 그리고 모든 메시지나 공지내용을 직접 웹사이트를 방문해서 확인하기 바랍니다.
- **악성 링크/사기**: 소셜 미디어 사이트에 게시된 사기성 글이나 의심스러운 링크를 주의해야 합니다. 사이버 범죄자들이 소셜 미디어를 이용해서 공격을 전파하는 것입니다. 친구가 메시지를 게시하였다고 해도 반드시 친구가 하지 않았을 수도 있습니다. 친구의 계정이 해킹되었을 수도 있습니다. 만약에 가족이나 친구가 확인할 수 없는 이상한 메시지를

소셜 미디어

게시하였다면(도둑이 들었다거나, 돈을 보내달라는 등) 전화를 해서 확인하시기 바랍니다.

- **모바일 앱**: 대부분의 소셜 미디어 사이트는 온라인 계정에 접근할 수 있는 모바일 앱을 제공하고 있습니다. 모바일 앱을 다운받을 때는 신뢰받는 사이트에서 다운받고, 스마트폰은 강력한 패스워드가 설정되어 있어야 합니다. 만약에 스마트폰을 분실했을 때, 잠금이 되어 있지않으면, 누구나 스마트폰을 통해 소셜 미디어 사이트에 접근할 수 있고, 우리 계정으로 게시할 수 있습니다.

소셜 미디어 사이트는 전 세계 사람들과 교류 할 수 만들 어 주는 굉장한 것입니다. 만약 여러분이 위의 설명을 인지하고 따른다면, 더욱 안전하게 온라인 경험을 즐길 수 있습니다. 소셜 미디어 사이트를 좀더 안전하게 사용하는 방법 및 불법적인 활동을 신고하는 것 등에 관해서는 사용하는 소셜 미디어 사이트의 보안 가이드 페이지를 확인해 보시기 바랍니다.

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

패스워드:	http://www.securingthehuman.org/ouch/2015#april2015
2단계 인증:	http://www.securingthehuman.org/ouch/2013#august2013
모바일 앱 안전하게 사용하기:	http://www.securingthehuman.org/ouch/2015#january2015
사이버안전에 대해 아이들 교육방법:	http://www.securingthehuman.org/ouch/2015#june2015
페이스북 보안:	https://www.facebook.com/safety

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