SANS SECURING THE HUMAN | ITL TRAINING LEADERS

OUCH! | 2017 년 4월호

전 국민대상 월간 정보보호 인식제고 뉴스레터

OUCH!

이달 호 주제..

- 패스워드 문구
- 패스워드 안전하게 사용하기
- 참고자료

패스워드

배경

패스워드는 이메일, 온라인 뱅킹, 쇼핑 및 스마트폰에 접근하는 등에서 거의 매일 사용하는 것입니다. 하지만 패스워드는 가장 약한 지점 중 하나이며, 누군가 우리의 패스워드를 알게 되면 그 사람은 우리의 계정에 접근하여, 자금을 이체하거나 이메일을 읽거나 신원을 도용할 수 있습니다. 그래서 강력한 패스워드는 우리자신을 보호하는데 핵심적인 것입니다. 이번 달 뉴스레터에서는 일명 '패스워드 문구'를 이용해서 기억하기 쉬우면서도 강력한 패스워드를 생성하는 방법을 배우게 됩니다.

객원 편집자

미-녹 윈은 SANS 공인강사이며, 시큐어드 IT 솔루션의 CEO 및 수석컨설턴트이다. 그녀는 14 년 이상동안 다양한 산업분야의 전문가들에게 사이버보안 프로그램 개발, 관리해주고 있다. 트위터: @MenopN 링크드인: My-Ngoc "Menop" Nguyen.

패스워드 문구

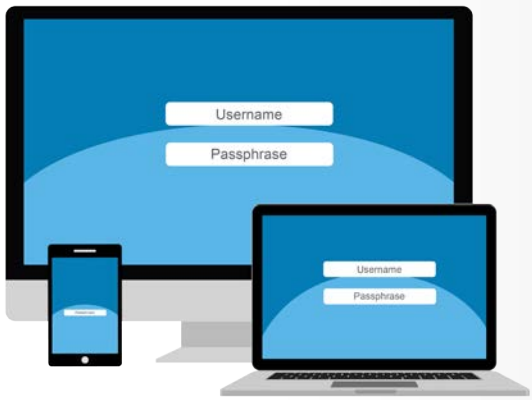
우리들이 매일 부딪히는 문제는 사이버 범죄자는 패스워드를 공격하기 위해 지능적이고 효과적인 방법을 개발하고 있다는 것입니다. 즉 패스워드 강도가 약하면 공격자들이 패스워드를 해킹할 수 있습니다. 중요한 것은 강력한 패스워드를 이용해서 우리를 보호해야 합니다. 패스워드는 복잡할 수록, 공격자들이 추측하기 힘들어 집니다. 하지만 복잡한 패스워드는 기억하기 어렵고 입력하기도 어렵습니다. 그래서 문장이나 긴 문구로 된 패스워드 문구를 사용할 것을 권합니다. 패스워드 문구는 길수록 안전합니다. 이러한 패스워드의 장점은 기억하고 입력하기 쉽지만, 해킹이 어렵습니다. 예를 들면 다음과 같습니다.

한글 패스워드 문구예:
아버지가 어디에 있지?
1:30에 커피한잔

위 패스워드 문구가 강력한 이유는 길뿐만 아니라, 중간에 스페이스도 있고, 특수문자도 포함되어 있습니다(스페이스 및 물음표는 기호이다). 동시에 이 패스워드 문구는 기억하기도 쉽고 입력하기도 쉽습니다. 위의 예와 같이 직접 다른 문구를 만들어내거나, @을 포함하거나 'ㅇ(이응)'을 숫자 0으로 교체하는 등으로 해서 더 강하게 만들 수 있습니다. 만약에 웹사이트

패스워드

또는 프로그램에서 패스워드에서 사용할 수 있는 문자수가 제한되어 있으면, 허용되는 최대한의 문자길이를 사용하는 것이 좋습니다.



패스워드 문구를 사용하면 강력한 패스워드를 만들고 기억할 수 있는 방법입니다.

패스워드 안전하게 사용하기

강한 패스워드를 사용하는 것도 중요하지만 패스워드를 이용할 때도 조심해야 합니다. 강한 패스워드를 가지고 있다고 하더라도 누군가 패스워드를 훔쳐간다면 소용이 없습니다.

1. 계정마다 서로 다른 패스워드 사용. 예를 들어 네이버, 다음, 페이스북과 같은 개인적인 계정에서 사용하는 패스워드를 업무용 또는 은행 계정의 패스워드로 절대 사용하면 안됩니다. 계정마다 다른 패스워드를 사용하면 계정 하나가 해킹되더라도, 다른 계정은 안전합니다. 너무 많은 패스워드로 인해 기억하기 어렵다면 패스워드 관리 프로그램을 사용하는 것도 좋은 방법입니다. 이 프로그램은 모든 패스워드를 안전하게 저장할 수 있는 것입니다. 패스워드 관리 프로그램을 사용하면 컴퓨터의 패스워드와 관리 프로그램 접근 패스워드만 기억하면 됩니다.
2. 절대로 회사 동료 등 다른 사람과 패스워드 공유 금지. 패스워드는 비밀정보입니다. 다른 사람들이 패스워드를 알고 있다면 패스워드는 더 이상 안전하지 않습니다. 우리가 우연히 다른 사람과 패스워드를 공유했거나 해킹되었거나 도난되었다고 의심이 되면 즉시 패스워드를 변경해야 합니다. 유일한 예외는 긴급상황을 대비해 가족들에게는 개인적인 패스워드를 공유할 수 있습니다. 이 때 공유할 수 있는 방법은 중요 패스워드를 기록해서, 안전한 장소에 저장하고 가족 등 신뢰하는 사람들에게 저장한 위치를 공유하는 것입니다. 이 방법을 사용하면 우리에게 긴급사항이 발생해서 도움이 필요하면, 가족들이 중요 계정에 접근할 수 있습니다.
3. 공용 컴퓨터 사용금지. 호텔이나 인터넷 카페와 같은 공용 컴퓨터에서 계정에 로그인 하면 안됩니다. 이러한 컴퓨터는 누구나 이용할 수 있기 때문에 컴퓨터 키보드 입력 값을 훔치는 악성코드에 감염되어 있을 수도 있습니다. 신뢰할 수 있는 컴퓨터나 모바일 기기에서만 계정에 로그인 해야 합니다.
4. 웹 사이트 등에서 개인적인 질문에 대한 답변 주의. 이러한 질문은 패스워드를 잊었거나 재설정할 때 사용됩니다. 문제는 이러한 질문에 대한 답이 인터넷에서 찾을 수 있거나 페이스북 등 SNS 에서 찾을 수 있다는 것입니다. 만약에 개인적인 질문에 대한 답을 제공하고자 한다면 공개된 정보가 아니고 가짜 정보를 이용하는 것이 좋습니다. 보안 질문에 대한 답을

패스워드

기억하지 못한다면요? 영화 주인공과 같은 주제를 선정해서 이 주인공에 대한 답을 만들면 됩니다. 다른 방법은 패스워드 관리프로그램을 사용하면 대부분의 프로그램에서 패스워드와 추가적인 정보도 안전하게 저장할 수 있습니다.

5. 많은 온라인 계정은 2중 인증 또는 2단계 인증을 제공하고 있습니다. 로그인하기 위해 패스워드뿐만 아니라 스마트폰으로 보낸 코드를 입력하는 것과 같이 추가적인 정보를 요구합니다. 이 방법은 패스워드만 사용하는 것보다 안전합니다. 가능하다면 이와 같이 강력한 인증 방법을 사용하는 것이 좋습니다.
6. 모바일 기기에 접속하기 위해서 PIN 번호를 요구합니다. PIN 번호는 패스워드입니다. 그래서 PIN이 길수록 안전합니다. 사실 많은 모바일 기기는 PIN 번호를 긴 패스워드나 지문 등의 생체인증으로 변경할 수 있는 기능이 있습니다.
7. 마지막으로 더 이상 사용하지 않는 계정이 있다면, 계정을 삭제하고 비활성화해야 합니다.

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 관리프로그램:	https://securingthehuman.sans.org/ouch/2015#october2015
2단계 인증:	https://securingthehuman.sans.org/ouch/2015#september2015
로그인 보안강화:	https://lockdownyourlogin.com
SANS SEC301 - 보안 기초 교육과정:	https://sans.org/sec301

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