

전 국민대상 월간 정보보호 인식제고 뉴스레터

OUCH!

이달 호 주제..

- 개요
- 프로그램 동작 방법
- 프로그램 선택하기

패스워드 관리프로그램

개요

온라인에서 자신을 보호 보호하고자 할 때 가장 중요한 단계 중 하나는 서로 다른 계정 및 앱에 대해 유일하고, 강력한 패스워드를 사용하는 것입니다. 하지만 대부분의 사람들은 많은 계정을 가지고 있어 모든 패스워드를 기억하는 것이 거의 불가능합니다. 그래서 많은 사람들이 동일한 패스워드를 재사용하고 있습니다. 서로 다른 계정에 동일한 패스워드를 재사용하는 것은 위험합니다. 누군가 패스워드를 알아 내면 동일한 패스워드를 사용하는 다른 계정에 접근할 수 있기 때문입니다. 이에 대한 간단한 해결책은 패스워드 관리프로그램(다른말로 패스워드 금고라고 부름)을 사용하는 것입니다. 이 프로그램은 로그인 인증정보를 안전하게 저장해서, 계정마다 다른 패스워드를 만들 수 있습니다. 패스워드 관리프로그램을 이용하면, 계정마다 다른 패스워드를 기억할 필요 없으며, 패스워드 관리프로그램의 마스터 패스워드만 기억하면 됩니다.

객원 편집자

크리스 크리스티안슨은 20 년의 경험과 수많은 자격증을 가지고 있으며, 캘리포니아에서 활동하는 정보보안 컨설턴트이다. 그는 다양한 컨퍼런스에서 발표했으며 많은 기고를 하였다. 크리스는 트위터 @cchristianson 및 <https://ismellpackets.com>로 연락할 수 있다.

프로그램 동작 방법

패스워드 관리프로그램은 모든 패스워드를 데이터베이스에 저장하며, 디지털 금고같이 동작합니다. 이 프로그램은 금고의 내용을 암호화하고 사용자가 알고있는 마스터 패스워드로 보호합니다. 온라인 은행이나 이메일에 로그인하는 것과 같이 패스워드를 추출 할 때 패스워드 관리프로그램에 마스터 패스워드를 입력하여 금고를 잠금 해제하기만 하면 됩니다. 대부분의 경우 패스워드 관리프로그램이 자동으로 패스워드를 검색하여 안전하게 로그인합니다. 따라서 패스워드를 기억할 필요가 없으므로 수백 가지의 고유하고 강력한 패스워드를 간단히 관리할 수 있습니다.

어떤 패스워드 관리프로그램은 로컬 시스템 또는 스마트폰에 금고를 저장하며, 어떤 패스워드 관리프로그램은 구축한 회사가 관리하는 원격 웹사이트에 금고를 저장합니다. 추가로 대부분의 이 프로그램은 자기가 인가한 다양한 기기에서 금고의 콘텐츠를 자동적으로 동기화할 수 있습니다. 노트북에서 패스워드를 업데이트하면 이 변경사항은 스마트폰, 태블릿 또는 사용하는 다른 컴퓨터와 동기화됩니다. 데이터베이스가 어디에 저장되어 있는 지 상관없이, 사용하고자 하는 시스템 또는 기기의 패스워드 관리 프로그램을 설치하면 됩니다.

패스워드 관리프로그램

먼저 패스워드 관리프로그램을 설치할 때, 수동으로 로그인 ID 및 패스워드를 입력하거나 임포트합니다. 그 후에는 패스워드 프로그램이 새로운 온라인 계정을 등록하고자 할 때, 기존 계정의 패스워드를 업데이트할 때 탐지하여, 자동으로 금고를 동시에 업데이트합니다. 이는 대부분의 패스워드 관리프로그램이 웹 브라우저와 함께 작동하기 때문에 가능합니다. 이러한 통합과정을 통해 웹 사이트에 자동으로 로그인 할 수도 있습니다.

패스워드 관리프로그램의 내용을 보호하기 위해 마스터 패스워드를 강력하고 다른 사람이 추측하기가 매우 어렵게 하는 것이 중요합니다. 실제 가능한 가장 강력한 유형의 패스워드 중 하나를 패스워드로 사용하는 것이 좋습니다. 패스워드 관리프로그램이 2 단계 인증을 지원하면, 마스터 패스워드의 경우 2단계 인증을 사용하시기 바랍니다. 마지막으로 마스터 패스워드를 반드시 기억해야 합니다. 마스터 패스워드를 잊어 버리면 다른 패스워드에 접근할 수 없습니다.

프로그램 선택하기

선택할 수 있는 많은 패스워드 관리프로그램이 있습니다. 참고자료에 패스워드 관리프로그램을 선택할 수 있는 링크가 있습니다. 가장 적합한 프로그램을 선택하기 위해서는 아래 사항을 유의해야 합니다.

- 패스워드 프로그램은 사용하기 간편해야 합니다. 만약에 너무 복잡해서 이해하기 힘들면, 자신의 스타일이나 전문성에 맞는 다른 제품을 찾아보는 것이 좋습니다.
- 사용하고자 하는 곳에 패스워드 관리프로그램이 동작해야 합니다. 모든 기기에 쉽게 패스워드가 동기화될 수 있어야 합니다.
- 잘 알려지고 신뢰할 수 있는 것 사용하시기 바랍니다. 오랫동안 업데이트 되지 않고, 피드백이 없는 것은 주의가 필요합니다. 사이버 범죄자는 우리의 정보를 훔치기 위해 가짜 프로그램을 만들 수 있습니다. 또한 자신의 암호화 솔루션을 개발하였다고 홍보하는 업체에 대해서는 의심해 보시기 바랍니다.
- 마스터 패스워드를 복구할 수 있다고 주장하는 패스워드 관리 프로그램은 사용하지 말기 바랍니다. 이 말은 회사에서 우리의 마스터 패스워드를 알고 있다는 것이며, 이로 인해 위험이 더 증가할 수 있습니다.
- 어떤 프로그램을 선택하던지, 항상 업데이트 및 패치하는 제품을 선택하시기 바랍니다. 그리고 최신 버전으로 프로그램 사용해야 합니다.



패스워드 관리프로그램을 이용하면 다양한 계정의 모든 패스워드를 안전하게 저장할 수 있습니다.

패스워드 관리프로그램

- 패스워드 관리프로그램은 자동으로 강력한 패스워드를 생성할 수 기능과, 선택한 패스워드의 강도를 보여줄 수 있어야 합니다.
- 패스워드 관리프로그램은 비밀 보안 질문에 대한 답, 신용카드 또는 파일 숫자 등 다른 민감 정보를 저장할 때 선택사항을 제공해야 한다.

패스워드 관리프로그램은 모든 패스워드 및 민감 정보를 안전하게 저장할 수 있는 강력한 도구입니다. 하지만 이러한 중요한 정보를 보호하기 때문에 공격자들은 추측하기 어려운 강력한 것이지만, 본인은 쉽게 기억할 수 있는 마스터 패스워드를 사용하기 바랍니다.

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

2017 최고 패스워드 관리프로그램:	https://www.pcmag.com/article2/0,2817,2407168,00.asp
패스워드:	http://www.securingthehuman.org/ouch/2017#april2017
2단계 인증:	https://www.securingthehuman.org/ouch/2015#september2015
Lock Down Your Login:	https://www.lockdownyourlogin.org/
SANS 일일 보안팁:	https://www.sans.org/tip_of_the_day.php

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 로 연락 주시기 바랍니다.

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



securingthehuman.sans.org/blog



[/securethehuman](https://www.facebook.com/securethehuman)



[@securethehuman](https://twitter.com/securethehuman)



[securingthehuman.sans.org/gplus](https://plus.google.com/securethehuman.sans.org)