컴퓨터 사용자를 위한 월간 정보보호 인식 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 각각의 계정에 대해 유일하고, 강력한 패스워드를 사용하는 것이다. 하지만 대부분의 사람들은 많은 계정을 가지고 있어 모든 패스워드를 기억하는 것이 거의 불가능하다. 간단한 해결책은 패스워드 관리프로그램(다른말로 패스워드 금고라고 부름)을 사용하는 것이다. 이 프로그램은 로그인 인증정보를 안전하게 저장하는 것이다. 또한 이를 이용해서 웹사이트, 모바일 앱 및 다른 애플리케이션에 로그인할 수 있다.

객원 편집자

레니 젤트서는 NCR 에서 고객 IT 운영 보안업무하며, SANS 연구소에서 보안 전문가 교육을 한다. 레니는 @lennyzeltser 트위터에서 활동하며, zeltser.com에서 보안기술문서를 발간하고 있다.

프로그램 동작 방법

패스워드 관리프로그램은 디지털 금고같이 동작한다. 이 프로그램은 사용자 ID, 패스워드 등 민감 정보를 안전하게 저장할 수 있다. 웹 사이트에서 로그인 계정을 요구하면, 이 프로그램은 자동으로 패스워드를 찾아서 웹사이트에 안전하게 로그인할 수 있다. 이 프로그램은 수 백개의 유일하고, 강력한 패스워드를 만들어주고, 만들어진 패스워드를 기억할 필요가 없다.

패스워드 관리프로그램은 데이터베이스에서 상세정보를 저장하며, 이곳을 금고라고 한다. 이 프로그램은 금고의 콘텐츠를 암호화하고, 자기만 알고 있는 마스터 패스워드로 보호한다. 온라인 뱅크 또는 이메일 계정에 로그인하기 위해 인증정보가 필요하면 금고를 열기 위해 패스워드 관리프로그램의 마스터 패스워드를 입력하기만 하면 된다. 어떤 패스워드 관리프로그램은 로컬 시스템 또는 스마트폰에 금고를 저장하며, 어떤 패스워드 관리프로그램을 구축한 회사가 관리하는 원격 웹사이트에 금고를 저장한다. 추가로 대부분의 이 프로그램은 자기가 인가한 다양한 기기에서 금고의 콘텐츠를 자동적으로 동기화할 수 있다. 노트북에서 패스워드를 업데이트하면 이 변경사항은 스마트폰, 태블릿 또는 사용하는 다른 컴퓨터와 동기화된다. 데이터베이스가 어디에 저장되어 있는 지 상관없이, 사용하고자 하는 시스템 또는 기기의 패스워드 관리 프로그램을 설치해야 한다.

패스워드 관리프로그램

먼저 패스워드 관리프로그램을 설치할 때, 수동으로 로그인 ID 및 패스워드를 입력해야 한다. 그 후에는 패스워드 프로그램이 새로운 온라인 계정을 등록하고자 할 때, 기존 계정의 패스워드를 업데이트할 때 탐지하여, 자동으로 금고를 동시에 업데이트한다. 이러한 통합과정을 통해 자동적으로 웹사이트에 로그인할 수 있도록 한다.

패스워드 관리프로그램을 이용하면 다양한 계정의 모든 패스워드를 안전하게 저장할 수 있습니다

패스워드 관리프로그램은 민감 데이터를 안전하게 저장하도록 설계되었다. 하지만 금고의 콘텐츠를 보호하는데 사용하는 마스터 패스워드는 다른 사람들이 추측할 수 없는 어려운 것이어야 한다. 마스터 패스워드를 가장 강력한 패스워드 형태의 문구로 만들 것을 권고한다. 만약에 패스워드 관리프로그램에서 마스터 패스워드에 2단계 인증을 지원한다면 이 기능을 사용하기 바란다. 마지막으로 마스터 패스워드를 다른 시스템이나 계정의 패스워드를 사용하시면 안된다. 이렇게 하면 해커들이 금고에 접근하고자 하더라도, 패스워드 추측이 불가능하다. 마지막으로 마스터 패스워드를 반드시 기억해야 한다. 만약에 이것을 잊어버리면, 다른 패스워드에 접근할 수 없게 된다.

프로그램 선택하기

아래는 사용자들이 선택할 수 있는 무료, 오픈 소스 및 상용 패스워드 관리프로그램이 존재한다. 가장 적합한 프로그램을 선택하기 위해서는 아래 사항을 유의해야 한다

- 패스워드 프로그램이 사용하고자 하는 금고에 접근할 때 모든 시스템 및 모바일 기기에서 동작할 수 있는 지 확인. 이러한 프로그램은 모든 기기에 금고의 콘텐츠를 쉽게 동기화 시켜준다.
- 잘 알려지고 신뢰할 수 있는 것 사용. 오랫동안 업데이트 되지 않고, 피드백이 없는 것은 주의가 필요하다. 가짜 안티바이러스 소프트웨어처럼, 사이버 범죄자들은 정보를 훔치기 위해 가짜 프로그램을 만들 수 있다.
- 간단히 사용할 수 있어야 함. 만약에 너무 복잡해서 이해하기 힘들면, 자신의 스타일이나 전문성에 맞는 다른 제품을 찾아보는 것이 좋다.
- 항상 업데이트 및 패치하고, 최신 버전으로 프로그램 사용
- 패스워드 관리프로그램은 다양한 계정에 대해서 강력한 패스워드를 쉽게 선택할 수 있어야 함. 또한 자동으로 강력한 패스우드를 생성할 수 기능과, 선택한 패스워드의 강도를 보여줄 수 있어야 한다.

패스워드 관리프로그램

- 패스워드 관리프로그램은 비밀 보안 질문에 대한 답, 신용카드 또는 파일 숫자 등 다른 민감 정보를 저장하는 선택사항을 제공해야 한다.
- 산업계 표준 기술을 이용하여 암호화하지 않고, 사설 또는 알려지지 않는 암호기술을 사용하고 있는 지 주의가 필요함. 사설 또는 알려지지 않는 암호제품을 광고하는 프로그램은 주의해야 한다
- 마스터 패스워드를 복구할 수 있다고 주장하는 패스워드 관리 프로그램은 사용 자제. 이 말은 회사에서 우리의 마스터 패스워드를 알고 있다는 것이며, 이로인해 위험이 증가할 수 있다.

패스워드 관리프로그램은 모든 패스워드 및 민감 정보를 안전하게 저장할 수 있는 강력한 도구이다. 하지만 중요한 정보를 보호하기 때문에 공격자들이 추측하기 어려운 강력하지만, 쉽게 기억할 수 있는 마스터 패스워드를 사용하기 바란다.

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:	https://www.securingthehuman.org/ouch/2015#september2015
탑 5 패스워드 관리프로그램:	http://lifehacker.com/5529133/five-best-password-managers
SANS 일일 보안팁:	http://www.sans.org/tip_of_the_day.php

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