강력한 비밀번호 생성하기

최종 수정일:
2018년 10월 29일

패스워드 매니저를 사용하여 강력한 비밀번호 생성하기

비밀번호 재사용은 아주 나쁜 보안 관행이다. 여러 계정에서 반복해서 사용하는 비밀번호를 공격자가 알게 되는 경우, 공격자는 많은 계정에 접속할 수 있게 된다. 그렇기 때문에 고유하며 강력한 비밀번호를 여러 개 갖는 것이 매우 중요하다.

다행히, 패스워드 매니저(비밀번호 관리자 툴)가 도움이 된다. 패스워드 매니저는 강력한 비밀번호를 생성하고 저장하는 도구로, 사용자는 많은 비밀번호를 외울 필요 없이 다양한 비밀번호를 여러 사이트 및 서비스에서 사용할 수 있다. 패스워드 매니저의 특징은 다음과 같다.

- 개인이 추측하기 어려운 강력한 비밀번호(패스워드)를 생성한다.
- 여러 비밀번호(와 보안 질문에 대한 응답)를 안전하게 저장한다.
- 단일 마스터 비밀번호(또는 패스프레이즈/비밀번호 문장)를 통해 사용자의 모든 비밀번호를 보호한다.

KeePassXC는 무료 오픈소스 기반 패스워드 매니저이다. KeePassXC는 컴퓨터에 설치하거나 또는 웹브라우저에 통합하여 사용할 수 있다. KeePassXC는 기본적으로 변경사항을 자동으로 저장하지 않기 때문에, 비밀번호를 추가하는 과정에서 KeePassXC가 비정상적으로 종료되는 경우, 추가한 비밀번호 전부를 잃을 수도 있다. 이 부분은 설정메뉴에서 변경이 가능하다.

패스워드 매니저가 적절한 도구인지 아닌지 궁금한가? 만약 당신의 공격자가 정부와 같이 강력한 상대라면, 패스워드 매니저는 유용하지 않을 수 있다.

주의사항

- 패스워드 매니저 사용으로 단일한 공격 지점이 만들어진다.
- 패스워드 매니저는 공격자의 명백한 목표가 된다.
- 연구에 의하면 패스워드 매니저에는 여러 취약한 점이 있다.

고급 기법의 디지털 공격이 우려되는 경우, IT 기술에 의존하지 않는 방식으로 비밀번호를 생성하는 전략을 고려할 수 있다. 수동으로 강력한 비밀번호를 만들고 (아래 "주사위를 사용하여 강력한 비밀번호 생성하기"을 참고한다), 이를 적어둔 뒤 안전하게 보관한다.

잠깐, 비밀번호는 머릿속으로 기억하는 것이지, 적어두면 안 되는 거 아닌가요? 사실 비밀번호를 적은 뒤 지갑 같은 곳에 저장하게 되면 적어둔 비밀번호를 잃어버리거나 또는 도난 됐다는 것을 알기 때문에 이는 유용한 전략이다.

주사위를 사용하여 강력한 비밀번호 생성하기

특별히 강력해야 하며 암기가 권장되는 비밀번호가 몇 가지 있다. 예를 들면

- 당신의 기기에 사용되는 비밀번호
- 암호화에 사용되는 비밀번호 (예를 들어 풀 디스크 암호화)

- 패스워드 매니저에 사용되는 마스터 비밀번호 또는 패스프레이즈(비밀번호 문장)
- 이메일 비밀번호

사용자 스스로 비밀번호를 선택할 때 마주하는 어려움 중 하나는 바로 임의적이고 예측하기 어려운 비밀번호를 만드는데 익숙하지 않다는 점이다. 강력하고 기억할 만한 비밀번호를 생성하는 효과적인 방법은 주사위와 단어 목록을 사용하여 임의로 단어를 고르는 것이다. 이를 통해 사용자는 "패스프레이즈"를 생성할 수 있다. "패스프레이즈"는 추가 보안을 위해 더 길어진 비밀번호의 일종이다. 디스크 암호화와 패스워드 매니저에 사용되는 비밀번호는 최소 6단어를 조합한 패스프레이즈 형식을 권장한다.

왜 최소 6단어인가? 패스프레이즈에 사용되는 단어를 고를 때 왜 주사위를 사용하는가? 비밀번호가 길고 임의적일수록, 컴퓨터와 인간이 추측하기 어려워진다. 여기 길고 추측하기 어려운 비밀번호를 선택해야 하는 이유를 설명하는 동영상이 있다.

EFF의 단어 목록을 사용하여 패스프레이즈를 만들어 보자.

컴퓨터 또는 기기가 이미 감염됐거나 스파이웨어가 설치된 경우, 스파이웨어는 당신이 마스터 비밀번호를 입력하는 것을 볼 수 있으며, 패스워드 매니저의 내용을 훔칠 수 있다. 따라서 패스워드 매니저를 사용할 때 컴퓨터 및 다른 기기에 말웨어(악성 소프트웨어)가 감염되지 않도록 관리하는 것이 중요하다.

"보안 질문" 관련 한마디

웹사이트에서 사용자의 신원을 확인하기 위해 사용되는 "보안 질문"에 유의한다. 솔직한 답변은 종종 일반인 또는 인터넷에 공개된 정보인 경우가 많기 때문에, 공격자가 쉽게 알아내고 비밀번호를 완전히 우회할 수 있게 된다.

따라서, 보안질문에 대한 답변을 본인이외에 아무도 모르는 가상의 답변으로 설정하는 것을 권장한다. 예를 들어, 보안 질문이 *"첫 애완동물의 이름은 무엇인가?"인 경우,* 실제 애완동물의 이름 대신 패스워드 매니저로 생성된 임시 비밀번호로 설정이 가능하다. 이처럼 보안질문에 대한 가상의 답변을 패스워드 매니저에 저장할 수 있다.

보안 질문의 답변을 설정한 사이트들의 답변을 바꿀 것을 고려해보자. 여러 웹사이트 또는 서비스의 계정에서 동일한 비밀번호 또는 보안 질문 답변을 사용하지 않을 것을 강력히 권장드린다.

다양한 기기에서 비밀번호 동기화하기

패스워드 매니저는 비밀번호 동기화 기능을 통해 여러 기기의 비밀번호에 접근하도록 허용한다. 한 기기에서 비밀번호 데이터베이스 파일을 동기화 한 경우, 나머지 기기에서도 비밀번호 데이터베이스 파일 내용이 업데이트 된다.

종류에 따라, 패스워드 매니저는 사용자의 비밀번호 데이터베이스 파일을 원격 서버에서 암호화된 상태로 저장한다. 패스워드 매니저는 사용자가 필요한 경우 자동으로 암호화를 풀어 비밀번호를 검색한다. 원격 서버에 비밀번호를 저장하고 동기화하는 패스워드 매니저는 편리하지만 공격에는 보다 더 취약하다. 비밀번호 파일이 사용자의 컴퓨터와 원격 서버에 동시에 저장된 경우, 공격자는 비밀번호를 알아내기 위해

사용자의 컴퓨터만 공격할 필요가 없기 때문이다. (하지만 그들은 여전히 사용자가 설정한 패스워드 매니저의 마스터 비밀번호 또는 패스프레이즈를 알아내야 한다.)

이런 상황이 우려된다면, 원격 서버에 비밀번호를 동기화 하는 대신, 비밀번호를 사용자의 기기에만 저장하도록 설정한다.

만약에 대비하여 비밀번호 데이터베이스 파일을 백업한다. 백업을 해 두면 비밀번호 데이터베이스를 기기 고장 등으로 잃어버리거나 또는 기기를 압수당했을 때 유용하다. 백업 생성은 패스워드 매니저 내의 백업 기능을 이용하거나, 백업 파일을 생성하거나, 자주 쓰는 일반 백업 프로그램을 이용해도 된다.

다중 인증과 일회용 비밀번호

강력하고 고유한 비밀번호는 공격자들이 계정에 접속하는 것을 훨씬 어렵게 한다. 이와 더불어 계정을 더욱 보호하기 위해, 이중 인증을 활성화하는 것 또한 권장한다.

일부 서비스는 사용자들이 계정에 접속할 때 두 가지 요소 (비밀번호 이외의 인증방식)를 소지하도록 요구하는 이중 인증 (또한 2FA, 다중 인증 또는 2단계 인증이라고도 한다) 서비스를 제공한다. 두 번째 요소는 모바일 기기에서 구동되는 어플리케이션이 생성한 일회용 코드 또는 숫자일 수 있다.

모바일 기기를 사용하는 이중 인증은 주로 아래 두 가지 방법 중 하나를 사용한다.

- 모바일 기기에 (구글 OTP/Authenticator 또는 Authy등과 같이) 보안 코드를 생성하는 인증 어플리케이션을 활용하여 인증하거나, 또는 (유비키와 같이) 물리적 하드웨어 기기를 연결하여 인증한다;
- 로그인 할 때마다 문자메시지를 통해 추가 보안코드를 받아서 입력해야 하는 서비스

가능하다면 문자 메시지를 통해 보안 코드를 받는 것 대신, 인증 어플리케이션 또는 독립 하드웨어 기기를 사용하여 인증한다. 공격자가 인증 어플리케이션을 우회하여 인증시도를 하기보다, 문자메시지 통신방식의 취약점을 이용하여 보안 코드를 공격자의 핸드폰으로 보내는 것이 보다 더 쉽기 때문이다.

구글과 같은 일부 서비스에서는 일회용 비밀번호 목록을 생성하는 기능이 존재하기도 한다. 이때 사용자는 일회용 비밀번호를 출력하거나 종이에 적어 가지고 다녀야 한다. 생성된 비밀번호는 한 번만 사용할 수 있기 때문에, 비밀번호 사용 이후 스파이웨어에 의해 비밀번호가 도난 당하더라도 공격자는 탈취한 비밀번호를 사용할 수 없게 된다.

개인 또는 기관에서 직접 통신 인프라를 운영하고 있는 경우, 해당 통신 인프라 접속을 위한 이중 인증을 가능하게하는 무료 소프트웨어가 존재한다. 개방형 표준 "시간 기반 일회용 비밀번호" 또는 RFC 6238를 제공하는 소프트웨어를 찾아보길 바란다..

가끔은 비밀번호를 공개해야 할 수도 있다

비밀번호 공개 관련법은 국가마다 다르다. 일부 관할권에선 비밀번호 공개 요구에 대해 법적인 이의 제기가 가능하지만, 다른 관할권에선 정부가 국내법에 따라 비밀번호 공개를 요구할 수 있으며, 심지어는 당신을 비밀번호 또는 키를 알고 있는 혐의로 감금할 수도 있다. 비밀번호를 강제로 얻기 위해 물리적인 위협을 가하는 경우도 있다. 또는 국경을 지날 때 비밀번호 공개 요청 또는 기기 잠금 해제 요청을 거부하는 경우 개인의 이동을 지연시키거나 또는 기기를 압수할 수 있는 상황도 생긴다.

미국에서 또는 미국으로 여행하는 동안 기기 접근에 대한 요청을 대비할 수 있는 미국 국경 통과 가이드를 준비했다. 그 외의 상황에서는, 비밀번호를 강제로 공개해야 하는 상황이 벌어질 경우와, 그로 인한 최악의 결과에 대하여 여행 전에 먼저 고려한 후 대비해보자.