이중 인증

이중 인증은 다중인증, 2단계인증, 2FA, MFA 등의 다양한 이름으로도 알려져 있습니다. 자세한 내용은 다음의 링크에서 확인해 볼 수 있습니다:
https://eff.org/common2FA.

이는 일반적으로 다음과 같이 정의됩니다.

1) **당신이 아는 것 - 지식기반**
계정이름과 비밀번호가 이에 포함되어 첫번째 요소를 구성합니다.

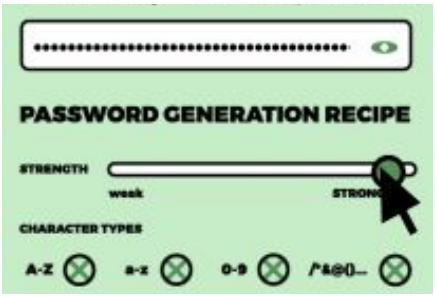
2) **당신이 소유하고 있는 것 - 소유기반**
당신이 휴대하고 다니는 기기를 포함하며, 이중 인증의 두번째 요소를 구성합니다.

다음에서 제안되는 지침들에 따름으로써 계정의 보안을 강화시키시길 바랍니다.

1 지식기반: 강력한 비밀번호를 사용하세요

각각의 계정들을 위한 비밀번호들은 다음과 같은 특성들을 충족해야합니다:

- 무작위적
- 긴 길이
- 고유함



강력한 비밀번호의 생성에 대하여 작성된 EFF(전자프론티어재단)의 가이드를 참조하세요.
https://ssd.eff.org/en/module/creating-strong-passwords

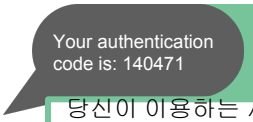
하지만 이렇게 각각의 계정마다 무작위적이고, 길이가 길며, 고유한 비밀번호들을 생성한다면, 어떻게 모두 기억할 수 있을까요?

당신의 위협모델에 따라, 비밀번호 관리 프로그램을 사용할 수도 있습니다.

비밀번호 관리 프로그램의 사용에 대한 EFF의 비디오는 다음의 링크에서 확인할 수 있습니다:
https://ssd.eff.org/en/module/animated-overview-using-password-managers-stay-safe-online

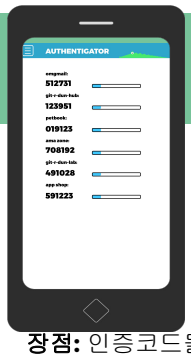
비밀번호 관리 프로그램을 찾고 계신가요?
EFF에서 추천되고 있는 프로그램 및 이의 사용법은 다음의 링크에서 확인할 수 있습니다:
https://ssd.eff.org/en/module/how-use-keepassx

2 소유기반: 당신의 이중 인증 방식을 선택하세요



문자메시지 기반 이중 인증

당신이 이용하는 서비스들이 당신의 휴대전화로 6자리의 숫자가 담긴 문자메시지를 전송합니다. 당신은 이 숫자들을 로그인 시에 입력하게 됩니다. 일부 서비스들은 해당 방식으로만 이중 인증을 제공합니다.
장점 : 편리합니다. 당신이 휴대전화 기기를 변경하더라도, 전화번호가 유지되는 한 로그인에 사용되는 6자리 코드를 전송받을 수 있습니다.
단점: 문자메시지 자체가 안전하지 않습니다. 또한 해외 방문 동안 통신서비스를 이용하지 않을 시, 인증코드를 수신할 수 없습니다. 전화번호가 변경될 때 또한 인증코드를 수신할 수 없게 됩니다. 마지막으로 당신의 휴대전화가 악성코드 및 바이러스에 감염되어 있다면, 공격자가 당신의 인증코드를 읽어볼 수 있습니다.



인증 어플리케이션들

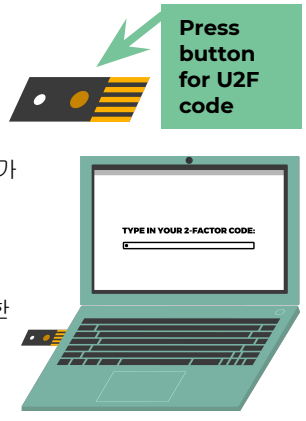
이용하는 서비스가 이중 인증을 위해 생성하여 화면에 표시해주는 6자리 코드를 어플리케이션에 입력합니다. 시간기반 인증 어플리케이션의 경우, 코드가 갱신되기 전에 입력해야 합니다.

장점: 인증코드들이 당신의 휴대전화 또는 태블릿 기기 내에 보관되며, 통신사가 확인 할 수 없습니다. 어플리케이션의 정보는 암호화를 통해 보호됩니다.
단점: 이 방식 역시 휴대기기가 악성코드 또는 바이러스에 감염되어 있다면 공격자는 손쉽게 인증코드를 탈취할 수 있습니다. 또한 백업코드를 보관하지 않은 상태에서, 휴대기기를 분실하게 되면 계정 또한 분실하게 됩니다.

U2F & 하드웨어 토큰들

USB포트에 하드웨어 토큰을 삽입 후, 서비스가 이중 인증을 위해 요청할 시 하드웨어의 버튼을 누릅니다.

장점: 인증코드가 하드웨어 토큰에 보관됩니다. 계정의 보안을 걱정하는 분들에게 가장 추천되는 방법입니다. 당신의 휴대기기에 보관되지 않기 때문에, 공격자가 휴대기기의 악성코드 또는 바이러스를 통해 인증코드를 탈취할 우려가 없습니다.
단점: 하드웨어 토큰을 구매하여 휴대해야 합니다.(Yubikey가 가장 대중적인 상품으로 알려져 있습니다) 토큰을 항상 챙기는 일은 다소 불편할 수 있습니다. 또한 하드웨어 토큰을 분실할 시, 계정에 다시 로그인할수 없게 될 수 있습니다.



이중 인증의 활성화를 시작하세요!

이중 인증의 활성화 전:

☐ 당신의 휴대기기 또는 하드웨어 토큰을 타인과 공유해서 사용하는 것에 대해 다시 한번 고려해 보시기 바랍니다. 공유하는 상대방들이 당신의 이중 인증코드에 접근할 수 있게 됩니다.

☐ 다음의 사이트를 방문하여 당신이 이용하는 서비스들의 계정에 이중 인증을 활성화 하는 방법을 확인하세요.
https://eff.org/12days2FA

☐ 다음의 사이트를 방문하여 당신이 이용하는 서비스들 중 어떤 서비스가 이중 인증 방식을 제공하는지 확인하세요.
https://twofactorauth.org/

☐ 이중 인증을 제공하는 서비스들을 하단의 표에 적어보세요.

이중 인증을 제공하며 내가 이용하는 서비스들:

서비스명?	제공되는 이중 인증 방식?	활성화 완료?

계정의 보안상태를 모니터링하기위해 추가적으로 당신이 할수 있는 것들:

☐ 당신이 이용하는 계정들에서 가능하다면 로그인 기록 저장기능을 활성화하세요.

☐ 정기적으로 확인하는 이메일에 각종 계정들의 로그인 알림이 전달되도록 하십시오.

☐ 문자메시지 기반 이중 인증코드를 더욱 더 보호하기 위해, 통신사에 연락하여 당신의 통신사 계정의 환경설정 변경을 위해 요청되는 비밀번호를 생성하세요.

백업 플랜을 준비하세요:

☐ 휴대기기 또는 하드웨어 토큰의 분실에 대비한 백업 플랜을 고민해본 후 아래에 작성해보세요:

_____.

☐ 여행중에도 이중 인증이 활성화 되어있는 서비스들을 사용하기 위한 백업플랜을 고민해 본 후 아래에 작성해보세요:

_____.

☐ 백업코드들을 하단의 공간 또는 다른 종이에 받아적어 놓으세요.

☐ 물리적으로 안전한 공간에 이 코드들을 보관하세요.

만약 당신이 여행중이거나, 휴대기기 또는 하드웨어 토큰을 분실했을 시 _____ 서비스를 위한 백업코드는:

이 코드들은 일회용입니다. 분실되지 않을 안전한 장소에 보관하세요.

_____ _____ _____

_____ _____ _____

_____ _____ _____