SANS SECURITY AWARENESS
ITL TRAINING LEADERS
OUCH! | 2017 년 12월 호
전 국민대상 월간 정보보호 인식제고 뉴스레터

OUCH!

이달 호 주제..

- 패스워드
- 2단계 인증이란?
- 동작방법

온라인 계정 보안강화

개요

이메일, 소셜 미디어 또는 온라인 뱅킹 계좌와 같은 개인정보를 보호하는 핵심요소는 자신의 신원을 증명하는 인증 절차입니다. 잘 알지 못할 수 있지만, 자신이 누구인지 증명할 수 있는 방법은 세 가지가 있습니다. 패스워드와 같이 알고 있는 것, 운전 면허증과 같이 가지고 있는 것, 지문과 같이 신체의 특징을 이용하는 방법입니다. 이 방법 각각에는 장점과 단점이 있습니다. 가장 일반적인 인증 방법은 패스워드입니다. 불행히도, 패스워드 자체를 사용하는 것이 점점 더 안전하지 않은 것으로 판명되고 있습니다. 이번 뉴스레터에서 우리 자신을 보호하는 방법을 알려 주며 패스워드 이외의 다른 것을 사용하여 계정을 안전하게 만들 수 있는 2단계 인증에 대해서 소개합니다.

객원 편집자
티파니 쉬나이크는 국가 사이버보안협회(@staysafeonline) 캠페인 및 이니셔티브의 이사이다. 쉬나이크는 2016년에 백악관, 정부 및 산업계와 협력하여 2단계 인증 에 대한 계정 잠금, STOP.Think. Connect 캠페인을 개발하였다.

패스워드는 더 이상 충분하지 않다

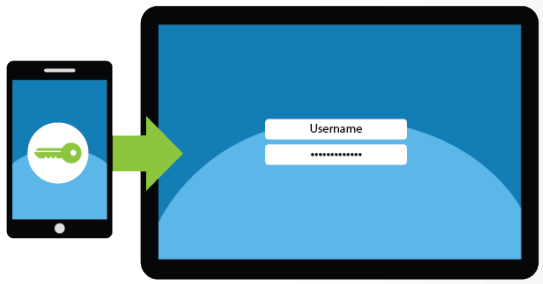
패스워드는 내가 아는 것에 근거하여 자신의 신분을 증명합니다. 그러나 누군가가 나의 패스워드를 추측하거나 접근할 수 있다면, 신분을 가장하여 우리의 모든 정보에 접근할 수 있습니다. 계정을 해킹하는 주요 방법 중 하나가 바로 패스워드를 해킹하는 것입니다. 따라서 다른 사람들이 추측하기 어려운 패스워드문구를 사용하고 모든 계정마다 서로 다른 패스워드를 사용하며 다른 사람과 패스워드를 공유하지 않도록 해야 합니다. 이러한 방법은 효과가 있지만, 패스워드는 더 이상 효과적이지 않습니다. 다행히도 개인정보를 보다 안전하게 유지할 수 있는 간단하고 빠른 방법이 2단계 인증 이라고합니다.

2단계 인증이란

2 단계 인증 (다중 인증 또는 2FA라고도 함)은 패스워드만 사용하는 것보다 훨씬 강력합니다. 이 기술은 신분을 증명하기

온라인 계정 보안강화

위해, 하나가 아니라 두 가지 다른 방법을 요구합니다. ATM이 좋은 사례입니다. 현금 자동 입출금기에서 돈을 인출할 때 실제로 2 단계 인증 방식을 사용하고 있습니다. 현금을 사용하려면 ATM 카드(가지고 있는 것)와 PIN 번호(알고있는 것)의 두 가지가 필요합니다. ATM 카드를 분실하거나 도난당한 경우 다른 사람도 PIN을 알지 못하면 돈을 인출 할 수 없습니다. 도둑이 인출하기 위해서는 ATM 카드와 핀을 모두 가지고 있어야 합니다. 2단계 인증도 이와 동일한 개념을 사용합니다.



가능한 2단계 인증을 사용하여 계정을 안전하게 하십시요. 이 방법이 온라인에서 자신을 보호할 수 있는 최선의 방법입니다.

동작 방법

2단계 인증은 대부분의 주요 은행, 이메일, 소셜 네트워킹 및 기타 사이트에서 광범위하게 사용되고 있습니다. 또한 대부분의 사이트에서 2 단계 인증을 설정하는 방법에 대해서 간단한 단계별 지침을 제공합니다 (자세한 내용은 끝 부분의 참고자료 섹션 참조). 2단계 인증은 다음과 같이 동작합니다. 먼저, 사용자 이름과 패스워드를 사용하여 계정에 로그인합니다. 이것은 2단계 인증 중 첫 번째 단계로서 알고있는 것으로 인증하는 것입니다. 그런 다음 문자로 스마트 폰에 고유 코드를 수신합니다. 그런 다음 해당 코드를 로그인 화면에 입력합니다. 이것은 2단계 인증 중 두 번째 단계입니다. 코드를 수신하려면 휴대 전화가 있어야합니다. 이렇게 하면 온라인 계정은 더 안전하게 됩니다. 사이버 범죄자가 패스워드를 도용하더라도 휴대 전화를 가지고 있지 않으면 계정에 접근할 수 없습니다.

문자 메시지를 통해 고유 코드를 받는 대신 스마트 폰에 특별한 인증 앱을 설치할 수 있습니다. 이 모바일 앱은 로그인 할 때마다 고유한 코드를 생성합니다. 모바일 앱을 사용하면 코드가 앱을 통해 생성되고 문자 메시지를 통해 전송되지 않으므로 훨씬 안전합니다. 또한 고유 코드를 받기 위해 전화 서비스에 연결할 필요가 없으므로 더 편리합니다. 앱에 지속적으로 새로운 코드가 생성되어 계정에 로그인 할 수 있습니다.

온라인 계정 보안강화

처음에는 2단계 인증이 귀찮아 보일 수 있지만, 훨씬 안전하게 개인정보를 보호할 수 있습니다. 계정이 해킹 될 때까지 기다리지 말고 이메일, 은행 또는 소셜 미디어와 같은 주요 계정에서 2 단계 인증을 사용하여 계정을 잠그고, 안전한 상태에서 사용하시기 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

패스워드 문구:	https://securingthehuman.sans.org/ouch/2017#april2017
2단계 인증을 지원하는 사이트:	https://twofactorauth.org
Stop|Think|Connect:	https://www.lockdownyourlogin.org
구글 2단계 인증:	http://www.google.com/landing/2step/

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