OUCH! | 2015 년 4월호

컴퓨터 사용자를 위한 월간 정보보호 인식 뉴스레터

OUCH!

**이달 호 주제..**

- 패스워드 문구
- 패스워드 안전하게 사용하기
- 참고자료

# 패스워드

## 배경

패스워드는 이메일, 온라인 뱅킹, 쇼핑 및 스마트폰에 접근하는 등에 거의 매일 사용하는 것이다. 하지만 패스워드는 가장 약한 지점 중 하나이며, 누군가 우리의 패스워드를 알게 되면 그 사람은 우리의 신원을 도용해서, 자금을 이체하거나 개인정보에 접근할 수 있다. 강력한 패스워드는 우리자신을 보호하는데 핵심적인 것이다. 이번 달 뉴스레터에서는 일명 '패스워드 문구'를 이용해서 기억하기 쉬우면서도 강력한 패스워드를 생성하는 방법을 배우게 된다.

**객원 편집자**

가이 브루니는 IPSS의 선임보안컨설턴트이며, SANS 강사 및 ISC 운영자이다. 가이는 SANS GSE자격증을 보유하고 있으며, SANS 사이버 가디언 프로그램을 수료하였다. 가이는 트위터 @GuyBruneau 및 handlers.sans.org/gbruneau에서 활동하고 있다.

## 패스워드 문구

문제는 사이버 범죄자는 패스워드를 공격하거나 추측하기 위해 지능적인 프로그램을 개발하고 있다는 것이다. 그리고 범죄자들은 지속적으로 프로그램을 업그레이드 하고 있다. 이 말은 패스워드가 약하거나 추측하기 쉬우면 쉽게 훔칠 수 있다. 중요한 것은 강력한 패스워드를 이용해서 우리를 보호해야 한다. 패스워드 문자가 길수록 강력하며, 공격자들이 추측하기 힘들다. 하지만 길고, 복잡한 패스워드는 기억하기 어렵다는 점이다. 그래서 대신에 패스워드문구를 사용하도록 권고한다. 이것은 기억하기 쉬운 간단한 문구나 문장이지만, 해킹이 어렵다. 예를 들면 다음과 같다.

한글 패스워드 문구예: 아버지가 어디에 있지?

위 패스워드 문구가 강력한 이유는 길이가12자이며, 중간에 스페이스도 있고, 특수문자도 포함되어 있다(스페이스 및 물음표는 기호이다). 위의 예와 같이 직접 다른 문구를 만들어내거나, @을 포함하거나 'ㅇ(이응)'을 숫자 0으로 교체하는 등으로 해서 새롭게 만들 수 있다. 만약에 웹사이트 또는 프로그램에서 패스워드에서 사용할 수 있는 문자수가 제한되어 있으면, 허용되는 최대한의 문자길이를 사용하는 것이 좋다.

## 패스워드

### 패스워드 안전하게 사용하기

강한 패스워드를 사용하는 것도 중요하지만 패스워드를 이용할 때도 조심해야 한다. 강한 패스워드를 가지고 있다고 하더라도 패스워드를 누군가 훔쳐간다면 소용이 없다.


패스워드 문구를 사용하는 것은 신원과 정보를 보호하기 위한 가장 효과적인 방법 중 하나입니다.

1. 계정마다 서로 다른 패스워드를 사용해야 한다. 예를 들어 네이버, 다음, 페이스북과 같은 개인적인 계정에서 사용하는 패스워드를 업무용 또는 은행 계정의 패스워드로 절대 사용하면 안된다. 이렇게 하면 계정 하나가 해킹되더라도, 다른 계정은 안전하다. 너무 많은 패스워드로 인해 기억하기 어렵다면 패스워드 관리 프로그램을 사용하는 것도 좋은 방법이다. 이 프로그램은 모든 패스워드를 안전하게 저장할 수 있는 것이다. 패스워드 관리 프로그램을 사용하면 컴퓨터의 패스워드와 관리 프로그램 접근 패스워드만 기억하면 된다.

2. 절대로 회사 동료 등에게 다른 사람과 패스워드를 공유하면 안된다. 패스워드는 비밀정보이다. 다른 사람들이 패스워드를 알고 있다면 패스워드는 더 이상 안전하지 않다. 우리가 우연히 다른 사람과 패스워드를 공유했거나 해킹을 당했다고 의심이 되면 즉시 패스워드를 변경해야 한다.

3. 패스워드와 마찬가지로, 일반적인 사용되는 패스워드 문구는 피해야 한다. 예를 들어 “죽마고우”와 같은 유명한 고사성어는 너무 많이 알려져 있기 때문에 좋은 문구는 아니다.

4. 호텔이나 도서관과 같은 공용 컴퓨터에서 업무용 사이트에 로그인하거나 은행 계정에 접근하면 안된다. 이러한 컴퓨터는 누구나 이용할 수 있기 때문에 컴퓨터 키보드 입력 값을 훔치는 악성코드에 감염되어 있을 수도 있다. 회사 업무나 은행 계정은 신뢰된 컴퓨터나 모바일 기기에서 접속하는 것이 안전하다.

5. 웹 사이트 등에서 패스워드를 잊어버리거나 재설정하기 위해 개인적인 사항에 대한 답을 할 때도 주의해야 한다. 문제는 이러한 질문에 대한 답이 인터넷에서 찾을 수 있거나 페이스북 등 SNS 에서 찾을 수 있다. 만약에 개인적인 질문에 대한 답을 제공하고자 한다면 공개된 정보가 아니고 가짜 정보를 이용하는 것이 좋다. 패스워드 관리 프로그램은 이러한 문제를 도와주고 있으며, 추가적인 정보도 저장할 수 있다.

## 패스워드

6. 많은 온라인 계정은 2중 인증 또는 2단계 인증을 제공하고 있다. 로그인하기 위해 패스워드뿐만 아니라 스마트폰으로 보낸 코드를 입력하는 것과 같이 추가적인 정보를 요구한다. 이런 옵션은 패스워드만 사용하는 것보다 안전하다. 가능하다면 이와 같이 강력한 인증 방법을 사용하는 것이 좋다.

7. 모바일 기기에 접속하기 위해서 PIN 번호를 요구한다. PIN 번호는 패스워드이다. 그래서 PIN이 길수록 안전하다. 사실 많은 모바일 기기는 PIN 번호를 패스워드로 변경할 수 있다.

8. 마지막으로 더 이상 사용하지 않는 계정이 있다면, 계정을 삭제하고 비활성화해야 한다.

## 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

| | |
|---|---|
| 2단계 인증: | http://www.securingthehuman.org/ouch/2013#august2013 |
| 패스워드 관리프로그램: | http://www.securingthehuman.org/ouch/2013#october2013 |
| 사회공학 공격: | http://www.securingthehuman.org/ouch/2014#november2014 |
| 공통보안용어: | http://www.securingthehuman.org/resources/security-terms |



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