나는 어떻게 회원가입 API를 짜야하나요?

: 사용자에게 어떤 ***비밀번호***를 권장해야 할까?

발표 내용이 정리된 글입니다

github.com/joungeun/why/blob/e8ba734a12d2d344e7b6a282d247f0c841b8f4b8/Why%20can%20only%20write%20certain%20special%20characters%20in%20passwords.md

사용자에게 어떤 *비밀번호*를 권장해야 할까?

여러분이 자주 사용하시는 비밀번호 형식은 무엇인가요?

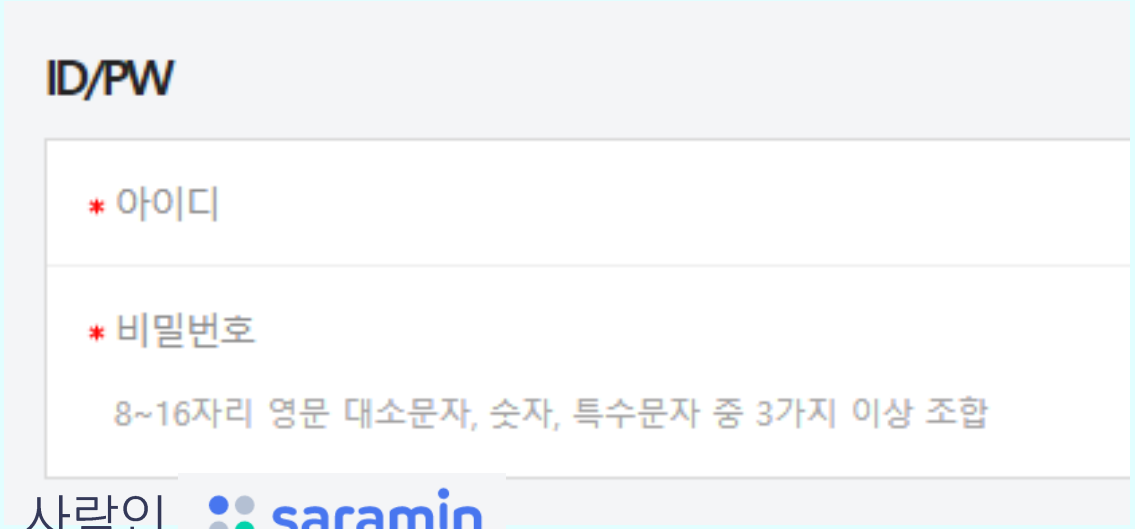
또는 가장 많이 본 비밀번호 형식은 무엇인가요?

사용자에게 어떤 *비밀번호*를 권장해야 할까?

* 8~12자 이내 영문,숫자,특수문자 중 2가지 이상을 조합해야 합니다.
* 사용 불가 특수 문자: ' " + / \ ; : - _ ^ & ( ) < > 제외

내가 짜는 회원가입 API는 좋지 않은 API인가?

사용자에게 어떤 *비밀번호*를 권장해야 할까?



사람인 saramin

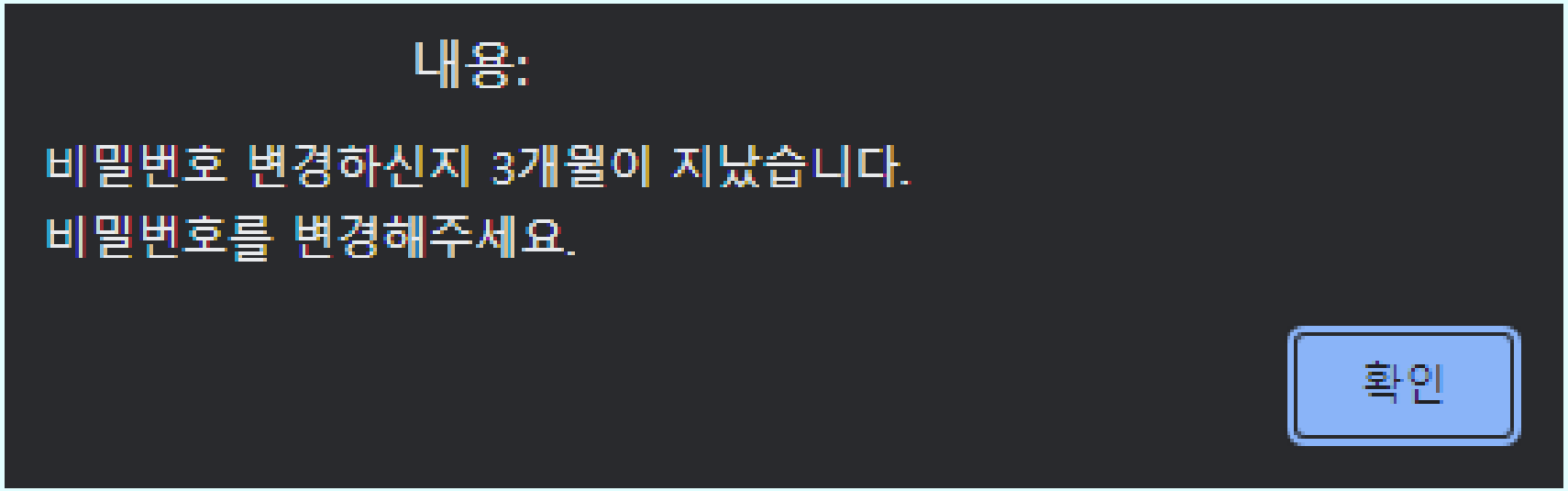
대문자, 소문자 숫자, 특수문자 등을 조합

8자리 이상

쿠팡 coupang

사용자에게 어떤 *비밀번호*를 권장해야 할까?

NIST (미국 국립표준 기술 연구소)



90일 주기로 비밀번호를 변경하라

사용자에게 어떤 *비밀번호*를 권장해야 할까?

빌 버 (Bill Burr)
특징: 비밀번호에 특수문자 쓰게 함

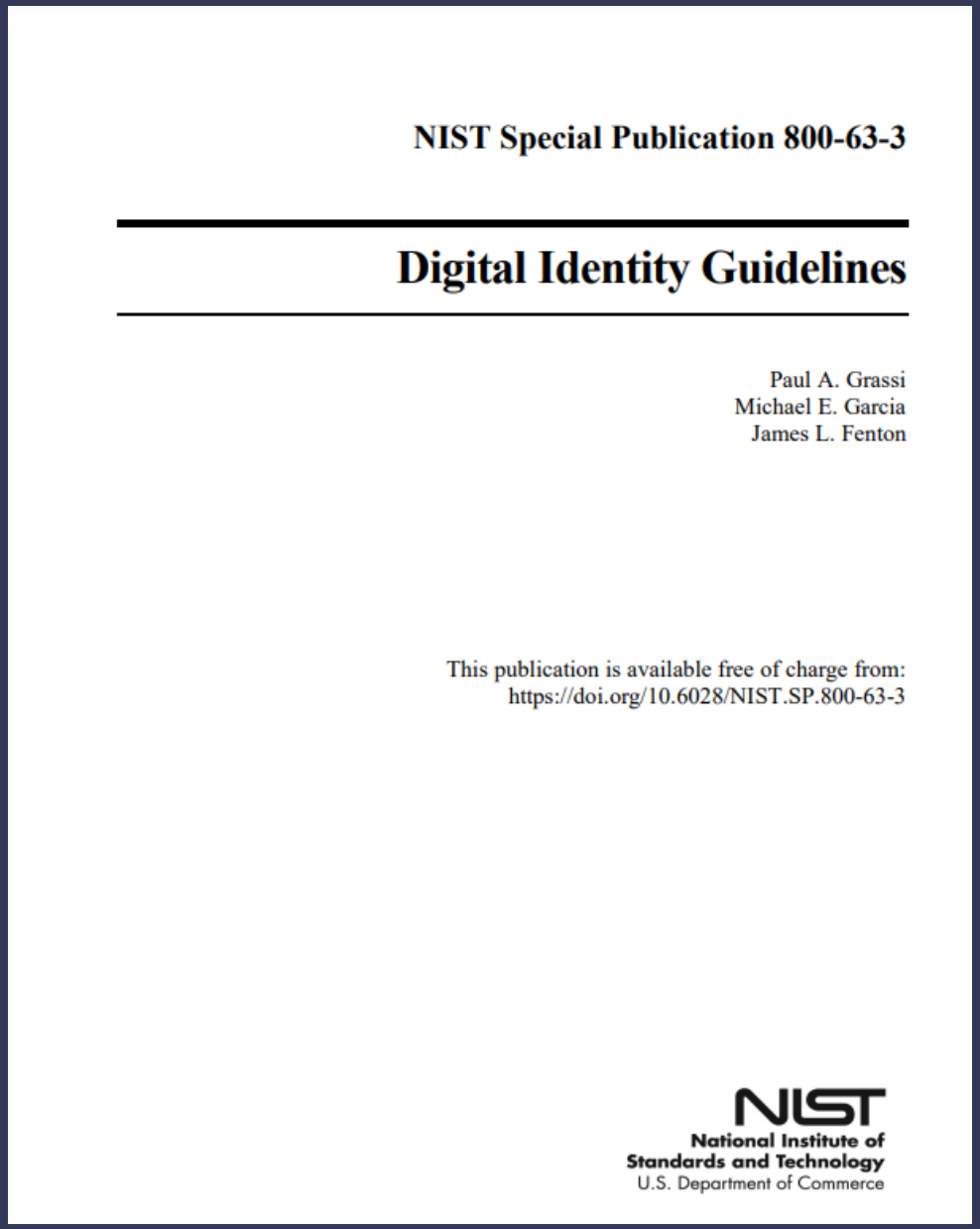
후회돼요

사용자에게 어떤 *비밀번호*를 권장해야 할까?

2003년 가이드라인이
오히려 보안에
취약할 수 있다는 사실!!

ㅇㅈ!!!!!!!

사용자에게 어떤 *비밀번호*를 권장해야 할까?



NIST Special Publication 800-63-3

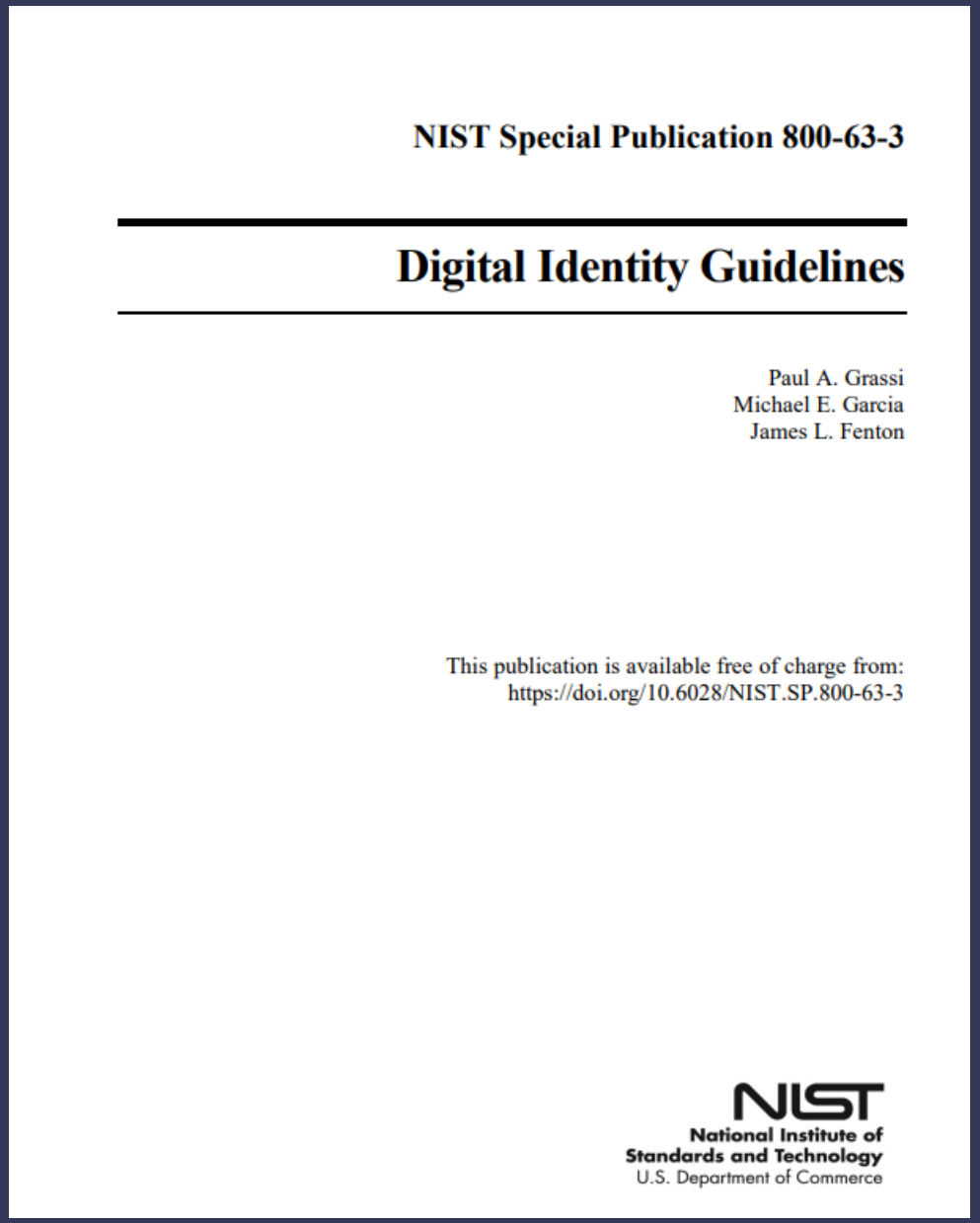
Digital Identity Guidelines

Paul A. Grassi
Michael E. Garcia
James L. Fenton

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-63-3

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

사용자에게 어떤 *비밀번호*를 권장해야 할까?



NIST Special Publication 800-63-3

Digital Identity Guidelines

Paul A. Grassi
Michael E. Garcia
James L. Fenton

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-63-3

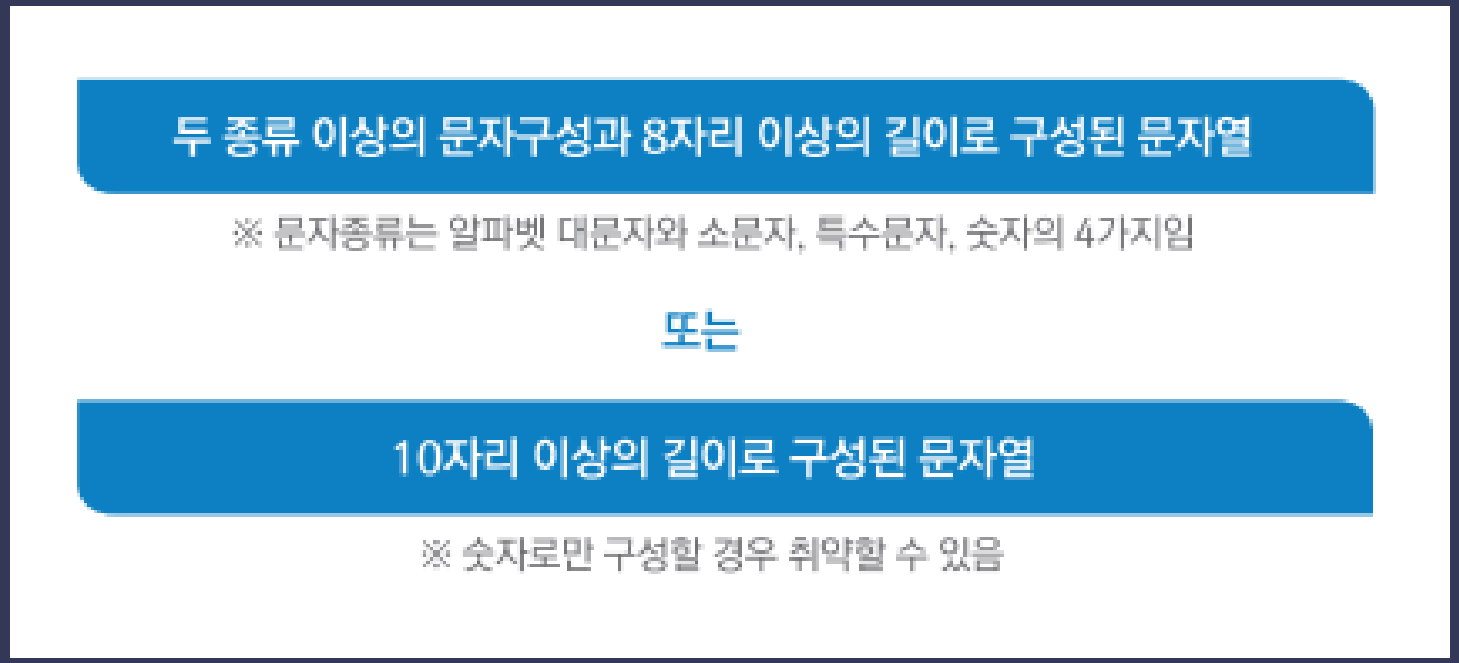
NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

검증자는 패스워드에 대해 구성 규칙을 요구해서는 안 된다.
(생성 규칙의 복잡성 높이지 마.)

검증자는 패스워드를 임의로 변경하라고 요구해선 안 된다.
(주기적 변경 요구 금지.)

사용자에게 어떤 *비밀번호*를 권장해야 할까?

KISA(한국 인터넷 진흥원)에서도…



결론

Monkey1! < monkeyspringbootmouseschool

(MonkeySpringBootMouseSchool)

사용자에게 어떤 *비밀번호*를 권장해야 할까?

결론

글자수 제한

블랙리스트 사용

근데 특수문자 제한은 좋지 않다는 말을 드리고 싶습니다
제가 찾아보면서 느끼는 건데, 특수문자 제한은 사용자에게 보안에 대한 의문을 불러일으킵니다

2020.06.22 09:13

사이트도 올해 새로 수주를 해서 개편을 했는데 황당하게도 비밀번호에 &를 못넣더라구요.
긴게 개편 전에는 & 넣는게 가능해서 원래 비밀번호에 &가 있었던 저는 그대로 잘쓰고 있
인정보 수정 부분(수정 전에 기존 비밀번호를 입력하는 부분)에서 자꾸 에러가 나서 전화해
있으면 안된다고...
어보니 보안 강화라는 황당한 답변을 받았네요. 정녕 올해 만든 사이트가 맞는건지...

를 낮추는 행위이니 '보안 약화' 인데 말이죠. 보안 강화란 도

문자가 제한되면 경우의 수가 줄어들어서 더 보안에 취약해지
화랍니다. 뭐 딱히 전문성 있는 답변을 기대한건 아니지만...