

Active Learning: Password Strength

1.

Password Strength

Password	Score	Complexity	Time to crack
123456789	4%	Very weak	Instantly
qwertyuiop	12%	Very weak	Instantly
nascar24	33%	Very weak	Instantly
abrakadabra	7%	Very weak	1 day
rfvfcenhf	10%	Very weak	2 minutes

I believe these tools are pretty accurate for measuring the strength of passwords, at least given these 5 passwords. They are all relatively low complexity, so there is low entropy and as a result the passwords are easy to crack.

2.

Passwords and Time to Crack

Password	Time to crack
A	Instantly
P445w0!	6 minutes
P445w0!744	5 years
P445w0!74499@4	200 million years
P445w0!74499@4!	15 billion years

3. Security.org and passwordmeter.com differ in that security.org reports the theoretical time it would take to crack the password and passwordmeter gives a score based on complexity of the password. For the most part, both websites align with the NIST password guidelines, although security.org does not require a minimum password length. Both websites allow Unicode characters to be used. The characteristics measured by these websites do generally yield a stronger password but are easily tricked into thinking a password is strong just because it possesses certain attributes. This is because they don't actually measure password strength, but rather password entropy. A password could be high entropy according to the websites, but still be insecure if it includes personal information or other guessable traits.

4.

asurve@purdue.edu | pwned?

Good news — no pwnage found!
No breached accounts and no pastes (subscribe to search sensitive breaches)

3 Steps to better security [Start using 1Password.com](#)

- Step 1** Protect yourself using 1Password to generate and save strong passwords for each website.
- Step 2** Enable 2 factor authentication and store the codes inside your 1Password account.
- Step 3** Subscribe to notifications for any other breaches. Then just change that unique password.

Results of Purdue email in haveibeenpwned.com

According to the website, my Purdue email and associated accounts have not been exposed to any breaches. In response to this, I have no urge to further secure my school account as it is already linked with Duo 2FA and is strictly used for trusted sites.

5. Password: 8,909
P455w0rd: 24,839
1234567890: 3,713,205
Q1a1z1: 6,134

Following this test with a few personal passwords of mine, none of them have been included in any breaches documented by haveibeenpwned.

6. Option 2: Google's password checkup plugin works by comparing your saved autofill passwords in password management against a database of breaches and exposed passwords. Whenever you save a password to be autofilled, it tests it and notifies you if a match is found. With this tool they are attempting to solve the problem of Americans using weak passwords, the same password across multiple sites, and aiming to help users know when their credentials have been compromised. Possible problems with using such an extension could be that if Google's password database were to be compromised, every security measure put in place beforehand would have gone to waste and the aim of password checkup would be useless. In addition, losing the master

password to any password management service generally means losing access to every other password stored in your vault.