Read this Article and then complete the activity

How to Create a Strong Password (and Remember It)

"Be sure to use a strong password" is advice we all constantly see online. Here's how to create a strong password — and, more importantly, how to actually remember it.

Using a password manager helps here, as it can create strong passwords and remember them for you. But, even if you use a password manager, you'll at least need to create and a remember a password for your password manager.

Dealing with Passwords the Easy Way

With the plethora of websites that you probably have accounts for, there's simply no way to easily remember every single password without duplicating them. This is where a password manager comes in — as long as you create a strong master password that you can remember, that's the last password you'll need to deal with.

There are a number of password managers, but Dashlane is probably the best choice for the average person. They have easy to use apps for every single platform, they integrate with every web browser, and it's completely free to use the basic features. If you want to sync your passwords between different devices, you'll need to upgrade to a premium account, but we recommend testing the free version out on your main computer first.

The security dashboard makes it easy to figure out how strong your passwords are

Creating a Strong Password

Strong passwords have four main requirements listed in order of importance:

1) The user can easily remember the password.

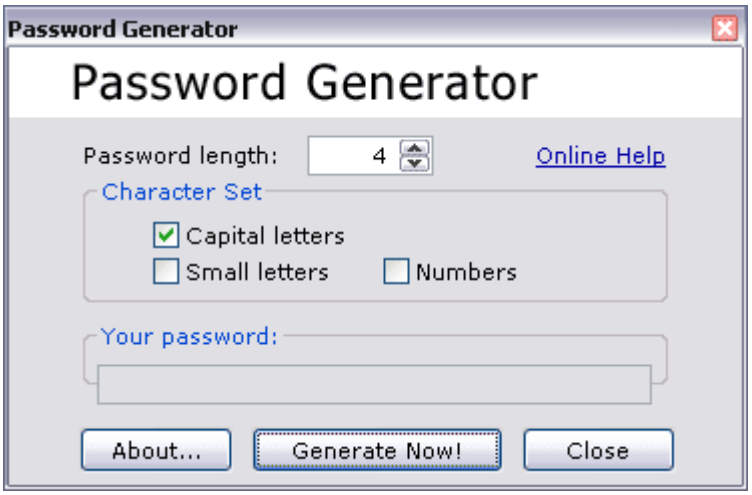
2) It is not trivial for any other person to guess a password.

3) It is not trivial for a program to guess or discover a password.

4) Must be complex, containing numbers, symbols and a mix of upper case and lower case letters.

Based on the list above, the first requirement is probably the most important because you need to be able to remember your password. For example, the password #4ssFrX^-aartPOknx25_70!xAdk<d! is considered a strong password because it satisfies the last three requirements, but it is very difficult to remember. Many organizations require passwords to contain a combination of numbers, symbols, and lower and upper case letters. Passwords that conform to that policy are fine as long as they are easy for the user to remember. Below is a sample password policy set for a typical organization:

- The password must be at least 8-12 characters long
- The password must contain upper- and lower-case letters
- The password must contain a number
- The password must contain a non-alphanumeric character



a. Open a web browser and go to http://passwordsgenerator.net

b. Select the options to conform to password policy set

c. Generate the password. Is the password generated easy to remember?

Using an online password creation tool, create passwords based on random words. Notice that because the words are appended together, they are not seen as dictionary words.

d. Open a web browser and go to http://preshing.com/20110811/xkcd-password-generator/

e. Generate a random word password by clicking Generate Another! at the top portion of the webpage.

f. Is the password generated easy to remember?

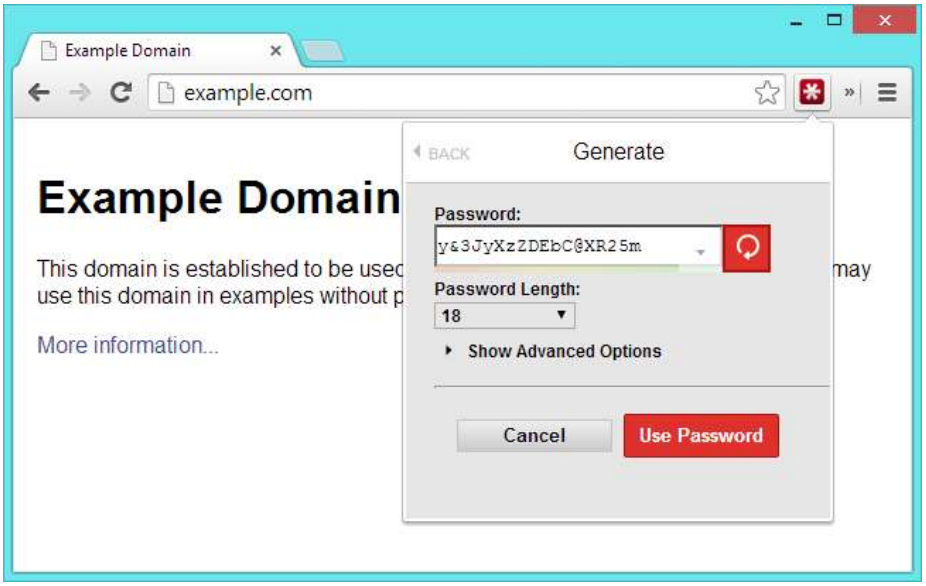
They have a ton of great features like a security dashboard, password changer, and a lot more. If you're serious about security, you'll make sure to use strong passwords everywhere, and the easiest way to manage them is a password manager like Dashlane.

The Traditional Password Advice

According to the traditional advice — which is still good — a strong password is:

- **Has 12 Characters, Minimum**: You need to choose a password that's long enough. There's no minimum password length everyone agrees on, but you should generally go for passwords that are a minimum of 12 to 14 characters in length. A longer password would be even better.
- **Includes Numbers, Symbols, Capital Letters, and Lower-Case Letters**: Use a mix of different types of characters to make the password harder to crack.
- **Isn't a Dictionary Word or Combination of Dictionary Words**: Stay away from obvious dictionary words and combinations of dictionary words. Any word on its own is bad. Any combination of a few words, especially if they're obvious, is also bad. For example, "house" is a terrible password. "Red house" is also very bad.
- **Doesn't Rely on Obvious Substitutions**: Don't use common substitutions, either — for example, "H0use" isn't strong just because you've replaced an o with a 0. That's just obvious.

Try to mix it up — for example, "BigHouse$123" fits many of the requirements here. It's 12 characters and includes upper-case letters, lower-case letters, a symbol, and some numbers. But it's fairly obvious — it's a dictionary phrase where each word is capitalized properly. There's only a single symbol, all the numbers are at the end, and they're in an easy order to guess.



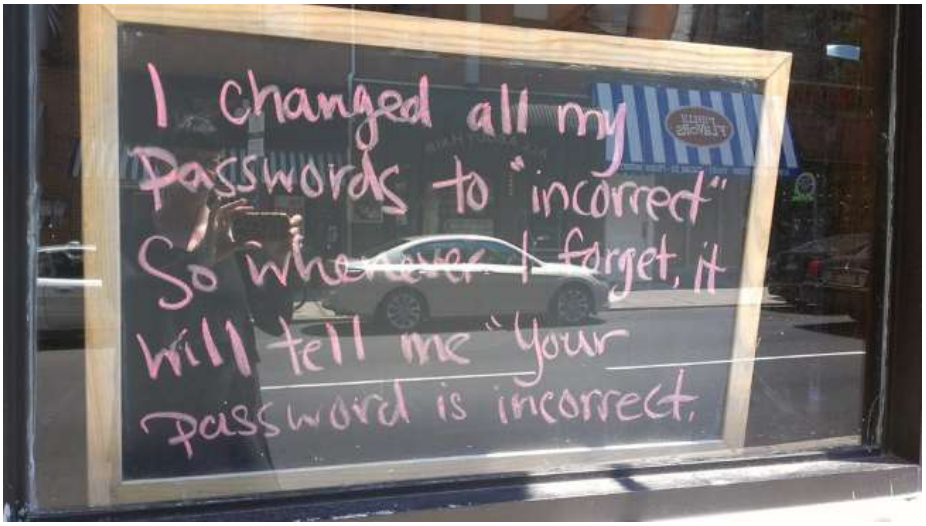
A Trick For Creating Memorable Passwords

With the tips above, it's pretty easy to come up with a password. Just bash your fingers against your keyboard and you can come up with a strong password like 3o(t&gSp&3hZ4#t9. That's a pretty good one — it's 16 characters, includes a mix of many different types of characters, and is hard to guess because it's a series of random characters.

The only problem here is memorizing this password. Assuming you don't have a photographic memory, you'd have to spend time drilling these characters into your brain. There are random password generators that can come up with this type of password for you — they're generally most useful as part of a password manager that will also remember them for you.

You'll need to think about how to come up with a memorable password. You don't want to use something obvious with dictionary characters, so consider using some sort of trick to memorize it.

For example, maybe you can find it easy to remember a sentence like "The first house **I** ever lived in was 613 Fake Street. Rent was $400 per month." You can then turn that into a password by using the first digits of each word, so your password would become **TfhIeliw613FS.Rw$4pm.** This is a strong password at 21 digits. Sure, a true random password might include a few more numbers and symbols and upper-case letters scrambled around, but it's not bad at all. You just need to remember two simple sentences, so it's easy to remember.



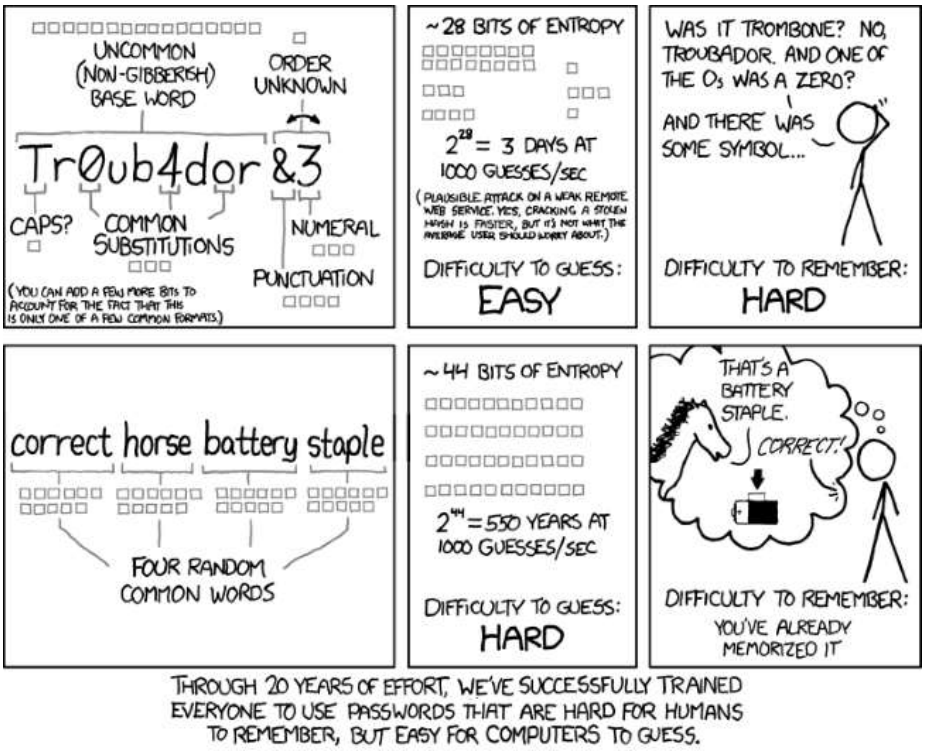
The Passphrase / Diceware Method

The traditional advice isn't the only good advice for coming up with a password XKCD did a great comic about this many years ago that's still widely linked to today. Throwing all the usual advice out, the comic advises choosing four random words and stringing them together to create a passphrase — a password that involves multiple words. The randomness of the word choice and length of the passphrase makes it strong.

The most important thing to remember here is that the words need to be random. For example, "cat in the hat" would be a terrible combination because it's such a common phrase and the word makes sense together. "my beautiful red house" would also be bad because the words make grammatical and logical sense together. But, something like "correct horse battery staple" or "seashell glaring molasses invisible" is random. The words don't make sense together and aren't in grammatically correct order, which is good. It should also be much easier to remember than a traditional random password.

People aren't good at coming up with sufficiently random combinations of words, so there's a tool you can use here. The Diceware website provides a numbered list of words. You roll traditional six-sided dice and the numbers that come up choose the words you should use. This is a great way to choose a passphrase because it ensures you use a random combination of words — you may even end up using words that aren't a normal part of your vocabulary. But, because we're just choosing from a list of words, it should be fairly easy to remember.

Diceware's creators now recommend using at least six words because of advances in technology that make password-cracking easier, so keep that in mind when creating this sort of password.



Comic from XKCD

It's not all about password strength. For example, if you re-use the password at multiple locations, it may be leaked and people may use that leaked password to access your other accounts.

Using unique passwords, avoiding phishing sites, and keeping your computer safe from password-capturing malware is also important. Yes, you should choose a strong password — but you need to do more than that. Using stronger passwords won't keep you secure from all the threats out there, but it's a good first step.

Image Credit: Lulu Hoeller on Flickr

JOIN THE DISCUSSION (13 REPLIES)

Chris Hoffman is a technology writer and all-around computer geek. He's as at home using the Linux terminal as he is digging into the Windows registry. Connect with him on Google+.

- Published 05/29/15

MORE ARTICLES YOU MIGHT LIKE