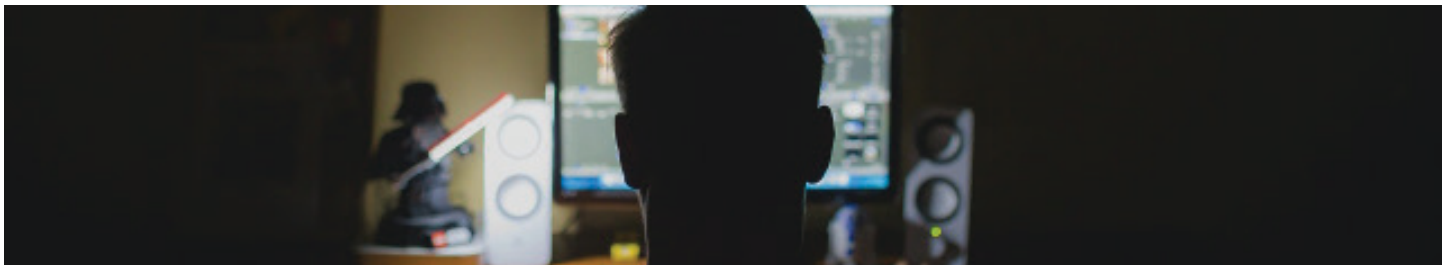
TECHVERA

How to Create (and Remember!) Strong Passwords

Cyber Security

How are passwords hacked?

Many people have the image in their heads of a hacker sitting at a computer, guessing passwords one by one.



This is just not true; in most cases the hacker can simply "set it and forget it", letting his computer program guess millions of different users' passwords every minute until it finds a correct login. **Hackers can guess passwords at the rate of 1 billion guesses a second**, and that number is only growing as computer hardware power increases.

A five-character password will have 10 billion possible combinations; this means a hacker can guess a normal five-character password in only 10 seconds.

Dictionary attacks: Hackers will try to crack passwords with words in a dictionary, and if your password contains words that are found in a dictionary (especially one- or two-word passwords), there is a good chance a hacker could easily guess it.

Mutations: Hackers also "mutate" words to reflect common things people do to try and make their passwords more secure, for example adding an exclamation point at the end or replacing an "O" with a zero. Hackers know all the common mutations people will use, and often try them immediately.

Language and culture: "Hackers are also smart about which words they choose. They don't just choose English words, but include most popular languages (i.e., Spanish, French, German). They also choose words from pop culture, like xbox360 or Britney Spears. If they know who you are, they will find words particular to you. Let's say your name is 'John Smith,' you drive a 'BMW,' you work for 'Microsoft,' and you like to watch 'The Office.' A hacker will Google these terms and create wordlists from the resulting Web pages. Thus, 'Carell325i' seems like a fine 10-character password to defeat hackers, but will get cracked in only a few minutes by a hacker who knows you." (DarkReading.com)

Clearly, you need more than just a few simple tricks to come up with a secure password. Read on to find out how to keep yourself secure!

Common password advice

You're probably familiar with the advice below, and it's still smart to follow these password tips:

- **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." (HowToGeek.com)

The power of the passphrase

As hackers and computers get more advanced, so must our passwords. The common advice above helps, but because it's common knowledge, hackers can also use it against us.

It's time to start rethinking the way you make your passwords. One way to do this is instead of a pass***word***, think pass***phrase***.

When you were in school trying to memorize an ordered list, such as the planets in our solar system, most students were given an easy to remember sentence where the first letters of it corresponded to the first letters in the ordered list (known as a mnemonic device).

So for our solar system example, to remember Mercury, Venus, Earth, Mars, Jupiter, Saturn, Uranus, Neptune, and Pluto, a good memorization sentence would be "**M**y **V**ery **E**mpty **M**onster **J**ust **S**wallowed **U**p **N**ine **P**lanets".

You can use this same kind of technique to create a strong passphrase. Pick a sentence that you won't forget, for example "**My husband & I met on October 5, 2010.**"

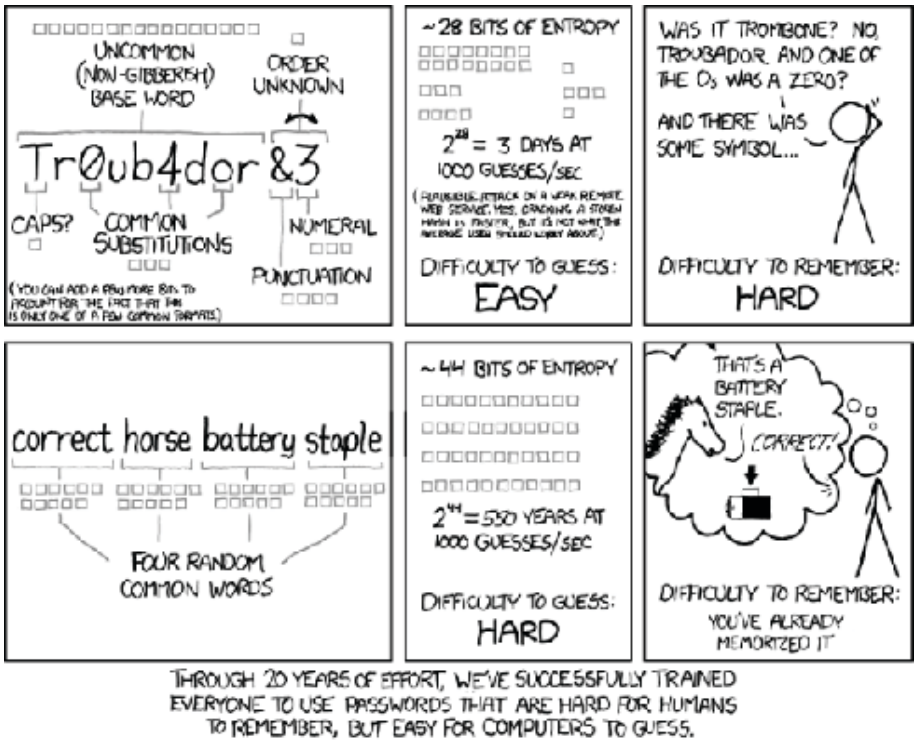
Take the first letters, capitalization and all, symbols, and numbers in that sentence and turn it into your passphrase: "**Mh&ImoO5,2.**"

You can customize your sentence any way you like to make sure it falls within program or website specifications. It is long, completely random, and near impossible to guess plus easy for you to remember! You can even write out and keep the entire sentence near your computer without fear of anyone guessing its true purpose.

Be random

Another password trick that many are turning to is using a string of random words in a nonsensical order. The randomness of the words and their order, and the length of the passphrase are what make this a strong choice.

"For example, 'cat in the hat' would be a terrible combination because it's such a common phrase and the words make 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." (HowToGeek.com)



Comic from xkcd.com

How you choose your words is up to you. You can take a book or dictionary, flip to a random page and stick your finger on a word, then repeat. You can even ask multiple friends or family to give you one word each and mix them together. As long as the words you pick are unrelated to each other, don't make sense together, and are altogether random, you're set! You don't even need to worry about substituting numbers for letters, capitalization, or other mutations with this trick.

Experts using this method suggest at least six words for maximum security.

Password managers

If you don't mind spending a little money, there are plenty of password manager programs that will make using strong passwords much easier.

These apps will create good passwords, remember them for you, store them safely, synchronize them across your computers and mobile devices, and even enter passwords into your login forms so you don't have to type them.

Of course, password managers are also protected by a password, but creating and remembering one long password is much better than dozens of them! Write your master password down if you need to, store it in a SAFE place (not attached to your computer!) and you will be free and clear without having to come up with and memorize tons of different passwords.

Here are some of the more popular password managers:

1Password (1password.com): Nice interface. Also remembers credit-card numbers. Auto-enters passwords in websites. Synchronizes a highly encrypted database of your passwords over either iCloud or Dropbox (or some other homebrew system, if you want). But it's expensive: $49.99 for the Mac or Windows version, plus $17.99 for the iPhone version. Bundles and deals are sometimes available.

LastPass (lastpass.com): Does pretty much everything 1Password does, but it's not as pretty. Has finer-grained security controls, including two-factor authentication (so even if someone learns your password, she can't get into your account unless she has your phone, too) and restrictions by country. A good free version, and a decent deal at $12 a year for mobile access.

Dashlane (dashlane.com): Probably the most beautiful of the password managers. Works across computers and mobile devices. Free on one computer, $29.99 a year for syncing across devices.

Other password managers include Roboform (roboform.com), Norton Identity Safe (identitysafe.norton.com), and SplashID (splashid.com). Try them out, find one you like, and get your passwords secure!