# Diceware

## “Passphrase”? What’s that?

Computers are now fast enough to quickly guess passwords shorter than ten or so characters. That means short passwords of any kind, even totally random ones like **nQ\m=8*x or !s7e&nUY or gaG5^bG**, may be too weak, especially for settings where an attacker is able to quickly try an unlimited number of guesses.

A “passphrase” is a type of password that is made up of multiple words and is longer than most passwords. Passphrases made of randomly-chosen words can be both easy to remember and hard for someone else to guess, which is what we want out of a passphrase.

Your passphrase is especially suitable when directly used to encrypt information, like for full-disk encryption on your laptop or mobile device. The large number of possibilities makes it much harder for someone to crack even if they get ahold of your device and use encryption-cracking hardware. A passphrase is also useful as a master password for your  password manager application.

Your passphrase should only be used for a single purpose and should not be used for more than one online account. Sometimes password databases or web sites get compromised. If you reuse a passphrase and it ends up being leaked in a data breach or otherwise discovered, it can be used to try to access your other accounts.

## Want to Make a Passphrase? Try EFF’s Wordlists!

EFF has created three wordlists that you can find at **eff.org/dice**. EFF's long list is designed for memorability and passphrase strength. We recommend selecting a minimum of six words from our long wordlist, or when using any other list of this size. The more words you use, the stronger the passphrase. Different wordlists may produce passphrases with different degrees of memorability, but you don't get significantly different passphrase strength by using one wordlist over another, if the lists are the same length.

The creator of our wordlists, Joseph Bonneau, has written a deep dive about passphrase security and the methodology he used to create our EFF wordlists at eff.org/wordlist.

## Generation Method

For most applications, we suggest making a six-word passphrase based upon EFF's long wordlist found at eff.org/dice.

- **Step 1:** Roll five dice all at once. Note the faces that come up.
- **Step 2:** Your results might look like this, reading left to right: 4, 3, 4, 6, 3. Write those numbers.
- **Step 3:** Open EFF's Wordlist (link above) to find the corresponding word next to 43463.
- **Step 4:** You will find the word "panoramic." This is the first word in your passphrase, so write it down.
- **Step 5:** Repeat the above steps five more times to come up with a total of SIX words. When you are done, your passphrase may look something like this: panoramic nectar precut smith banana handclap.
- **Step 6:** Come up with your own mnemonic to remember your phrase. It might be a story, scenario, or sentence that you will remember and can remind you of the words you chose, in order. For example:
- The panoramic view, as I tasted the nectar of a precut granny smith apple and banana, deserved a handclap.
- This passphrase is one of 221073919720733357899776 (or about $2^{77}$) alternatives that could have been chosen by this method. With so many possibilities, this passphrase will be very hard to guess by brute force.

## What Next?

Learn about password managers! These are a great way to avoid the pitfall of reusing passwords and passphrases. You can use the long, random passphrase that you've created today to protect an entire database of login information that your computer can remember so you don't have to. This makes it straightforward to use a different password for every online account, which is good security practice.

For more information on password managers, passphrases, and tips on account security, check out EFF's Surveillance Self-Defense resource at ssd.eff.org.

**The Electronic Frontier Foundation is the leading nonprofit defending digital privacy, free speech, and innovation. https://eff.org**