EFF Dice-Generated Passphrases

Create strong passphrases with EFF's new random number generators! This page includes information about passwords, different wordlists, and EFF's suggested method for passphrase generation. Use the directions below with any set of dice.

And now, a message from internationally renowned security technologist, author, and EFF Board Member Bruce Schneier:

Directions

We'll walk you through how to use EFF's Long Wordlist [.txt] to generate a passphrase. For most applications, we suggest making a six-word passphrase.

Step 1: Roll five dice all at once. Note the faces that come up without looking at the wordlist yet. (On our dice, the EFF logo is equivalent to rolling a one.)

Step 2: Your results might look like this reading left to right: 4, 3, 4, 6, 3. Write those numbers down.

Step 3: Open EFF's Long Wordlist [.txt] 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 steps 1-4 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 be able to remember and that can remind you of the particular 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.

Why Use Passphrases?

The word "passphrase" is used to convey the idea that a password, which is a single word, is far too short to protect you and that using a longer phrase is much better. The increased length can allow for a greater number of possibilities overall, even if you use a passphrase made of random words to help you remember it. 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. While the EFF random number generators are not casino-grade dice, we believe that they are sufficiently random for these purposes.

Computers are now fast enough to quickly guess passwords shorter than ten or so characters - and sometimes quite a few more. 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. This is not necessarily true for an online account, where the speed and quantity of guesses will be limited, but it could be true in other cases (for instance, if someone gets ahold of your device and is trying to crack its encryption password).

When to Use 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. Other great uses are the passphrase for an encryption key (like your PGP or SSH key), or, especially, for unlocking a password safe or password manager application.

Your passphrase should only be used for a single purpose, and especially should not be used for more than one online account. Sometimes password databases or websites 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.

Notes on Using the Different Wordlists

EFF's new long list, referenced in the directions above, 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 a significantly different passphrase strength by using one wordlist over another, if the lists are the same length.

When using one of our short wordlists (which contain 1296 words), roll only four dice at once. You can follow our passphrase-generating instructions above, using four dice instead of five. As mentioned elsewhere, passphrases created using one of the short wordlists might be easier to remember and type, but don't provide as much strength per word.

EFF's Long Wordlist [.txt], for use with five dice

EFF's Short Wordlist #1 [.txt], featuring only short words, for use with four dice

EFF's Short Wordlist #2 [.txt], for use with four dice, featuring longer words that may be more memorable.

The creator of our wordlists, Joseph Bonneau, has written a deep dive about passphrase security, and the methodology and criteria he used to create our EFF wordlists. You can also use Arnold G. Reinhold's Diceware word list, the original and still very popular list for using dice to create passphrases.

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. Visit the password manager overview on EFF's Surveillance Self-Defense guide to learn more!

Your passphrase that protects a password vault is now a very important key! Forgetting this passphrase is also a serious risk which could result in permanently losing data, and some people might thus prefer to have the passphrase written down, especially while first trying to memorize it or if they won't be using it every day - but if so, it should be kept in a safe place, not in the same place where the data it protects will be stored. What counts as a safe place for you depends on what you anticipate might happen. It's safer to write on a single thickness of paper on a hard surface to avoid leaving an imprint of the passphrase.