Sandfly Security®

How to Make a Strong Password

2025-05-14

Despite predictions for 30+ years that passwords are going away, passwords are still a part of our life and likely will be for some time. Yet, passwords get compromised frequently. Often the compromise is a result of stolen hashed password lists from a vendor or online service. Once the hashes are obtained, attackers run brute force attacks and compromise the accounts.

In theory, hashes protect your password if they are stolen. The hash masks your password from view vs. simply reading what it is directly if left unencrypted. For example:

Password: **sandflysecurity**
Hash: **$1$979ohiHO$ZSURNC9iw7Oq/HTTfHz0n1**

However, password hashes have come and gone over the years. Newer hashes are designed to protect against modern attacks. Yet, older hashes are weak and can be attacked at billions of hashes a second making brute force attacks very likely to succeed.

As a user, you don't have control over what hashes a service may be using, or what future hardware may make current hashes vulnerable. However, you can do one thing that is **guaranteed** to make brute force much harder if your password hash gets stolen:

Use a really long password.

By long, we mean a minimum of 15 characters, and preferably use a passphrase which can be seven or more words. A longer passphrase is not only easier to remember, but is tremendously stronger than shorter passwords even of random characters.

Roll Dice for a Strong Password

Making a strong password is as simple as rolling some dice and using Diceware. Diceware uses a set of five dice and list of words to allow you to roll a randomly generated passphrase that is secure. Not only this, but these passphrases are memorable and extremely strong once you get over a short length. Here's what you need:

Step 1: Get the EFF Diceware list: https://www.eff.org/dice
Step 2: Get a set of five dice (retired casino dice you can find online are great).
Step 3: Roll the dice and look up the word in the EFF list by the number you rolled.
Step 4: Repeat until you have the password length you desire (minimum 7).

For very critical applications like your password manager, disk encryption, crypto wallets, etc. you would want to use the longer end of the chart below. We'd suggest staying above seven words for the foreseeable future.

Wordlist length: 7776 (EFF Diceware Wordlist)
Entropy bits per word: 12.92 vs. English 4.7 bits per letter

Words	# Combinations	Entropy	Rating
1	7,776	12.92 bits	Bad
2	60,466,176	25.85 bits	Bad
3	470,184,984,576	38.77 bits	Bad
4	3,656,158,440,062,976	51.70 bits	Bad
5	28,429,979,228,573,992,576	64.62 bits	Bad
6	221,073,919,720,733,357,299,776	77.55 bits	Borderline
7	1,719,070,692,009,463,347,353,548,416	90.47 bits	Good
8	13,367,494,538,843,734,067,838,845,976,576	103.4 bits	Awesome
9	103,945,371,260,556,250,000,000,000,000,000	116.32 bits	Awesome
10	808,281,277,464,764,060,643,139,600,990,272	129.25 bits	Awesome
11+	Very Big!	142+ bits	Phenomenal

Eight Characters vs. Eight Words

It may sound strange, but these two passwords below are the same length. It's just that Diceware's alphabet is 7,776 characters long and standard English is only 26. Each new Diceware "letter" (word) tremendously expands the complexity vs. a single English letter.

English eight character: **applepie**
Diceware eight word: **blob cinch quirky mayflower candy defrost garden cardiac**

But look at the difference:

English letter combinations: 208,827,064,576
Time to break at one billion attempts a second: 208 second (3.5 minutes)

Diceware combinations: 13,367,494,538,843,734,067,838,845,976,576
Time to break at one billion attempts a second: 421 trillion years.

Do I Have to Use Dice?

There are online generators for Diceware, and many password vaults now support this format, but we recommend you use physical dice where the password is really important. Computer random number generators have had problems in the past so you can never be sure they are really random, plus there have been bugs in password generators that made predictable passwords in other ways. Physical dice ensure you are getting truly random numbers and you never have to worry about them being hacked.

Make a Password Long to Make it Strong

You can't control what password hash a developer or application may use, but you can make your password much more resistant to breaking even with a weak hash by simply using a very long passphrase. Use Diceware where it counts and know you won't be a victim of brute force attacks.

References

Diceware Homepage

https://theworld.com/~reinhold/diceware.html

EFF Diceware List

https://www.eff.org/dice