

How to create a strong yet easy-to-remember password.

Ensuring you use a strong password is a common piece of advice when creating accounts or engaging in any online activity. This article will guide you on how to create a strong password, and more importantly, how to remember it.

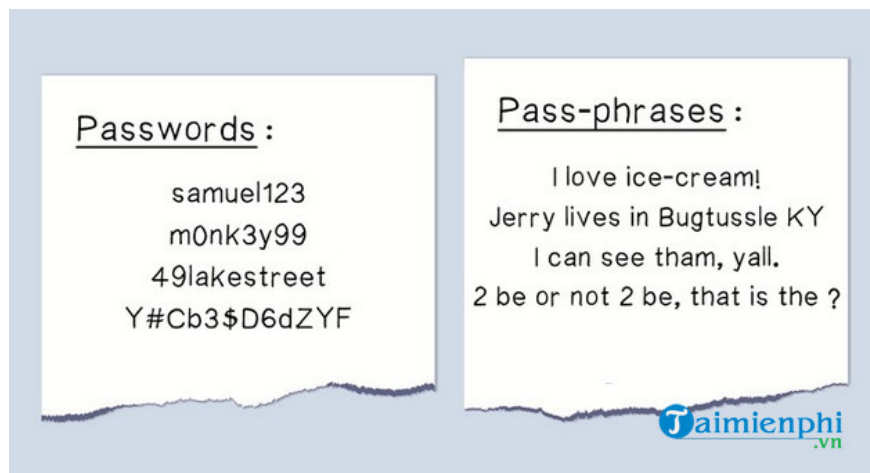
As our lives become increasingly online, maintaining a secure computing environment is crucial. Creating a password isn't enough; it needs to be a **STRONG** password. However, a common misconception is that strong passwords are difficult to remember. So how can you create a strong password that's also easy to remember?



Tips for creating strong, easy-to-remember passwords.

How to create a strong, secure, and easy-to-remember password.

1. Use Passphrase

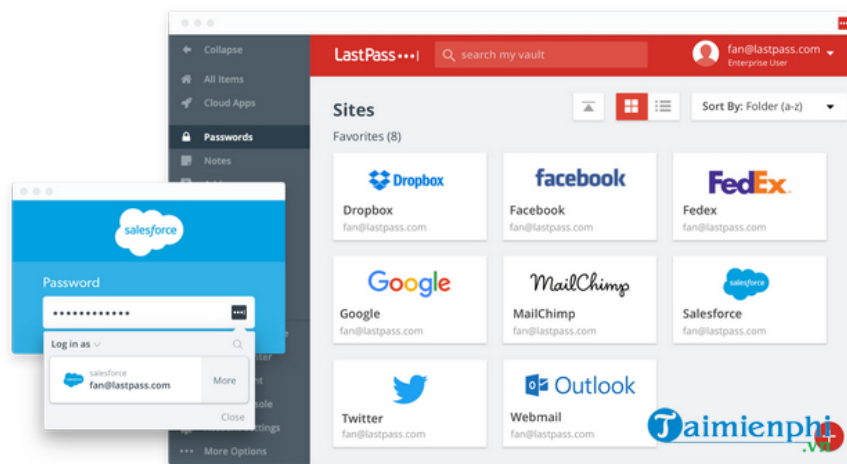


- Access Password [HERE](#)

The great thing about passphrases is that they're long, have many characters, aren't dictionary words, and in some cases, easily include special characters that make it difficult for someone or a computer trying to brute force your password to guess. For example, "my laptop is black and ugly!" is a 28-character password that's easy to remember and almost impossible to guess or hack. Some services like Twitter don't allow passwords with spaces, so you just need to adjust it slightly to suit the platform's requirements.

You should add a numeric character if you don't typically use two-factor authentication for your online accounts.

2. *Trust password management tools.*



Two highly-rated password management software options you can consider are LastPass and **1Password**. Both offer excellent features, not only helping you create long and strong passwords, but also securely storing them online so you can access your passwords on all your devices.

3. *A strong password is a unique password.*

Never use the same password on multiple websites or for multiple accounts. Sharing passwords across websites is like playing Russian Roulette. Just one website hacking can cost you everything, especially if that password is used across all your online accounts. Add an extra layer of security to your online activity by creating unique passwords for each website. That's why you should use a password manager. Each password is unique, and

1Password will warn you if you reuse a password.

4. *Don't use words from the dictionary.*

Password:	putridhouse	Password:	cleanyourdamnhouseboy
Strength:	46%	Strength:	99%
Evaluation:	Medium	Evaluation:	Excellent!
Dictionary attack check		Dictionary attack check	
<p> 'putrid' + 'house' is not a safe word combination. 'house' is a dictionary word.</p>		<p>Your password is: Safe!</p>	
<p>Your password is: Not safe!</p>			

Your name, city name, or your child's name are all great names, but they make terrible passwords. Dictionary words are easy to guess, and there are millions of apps out there that specialize in attacking accounts using dictionary words in every known language. The only exception to this rule is using dictionary words as a passphrase, as mentioned above.

5. *Password maintenance*

Like most valuable assets in life, passwords also need to be maintained. In other words, if you've been using a password for a while, change it periodically.

Above all, a password written on paper and hidden under a computer keyboard doesn't make it secure. So, don't do that. In most cases, if the worst happens and you forget your password, you can almost always reset it using your email address. You can also apply the password creation methods above to change your Wi-Fi password for your home or work modem.

You finished reading the article "**How to create a strong yet easy-to-remember password.**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.