Strong Password Ideas to Boost Your Security

TLDR

A good password should be long, unique, and easy to remember. Try to use at least 15 characters. One easy way is to join four or more random words. Use a different password for each account. A password manager can store all your passwords, so you only need to remember one main password. This is a simple and safe way to protect your accounts.

Introduction

The best password ideas focus on length, not just symbols. A long and unique password is harder to crack. It also helps protect your email, bank account, and personal photos from unwanted access.

Take Sun$h1n3! as an example. It may look complicated, but our test cracked it in under a second. This shows that adding symbols and numbers does not always make a password safe. A strong password should be hard to guess but easy for you to remember.

Need a password for your new phone or help a parent or child create one? In this blog, you will learn about the simple password ideas for different needs.

Each example includes a strength score tested with zxcvbn, a free password checker by Dropbox. You will also find iPhone passcode tips and common password mistakes to avoid.

What Makes a Good Password?

The longer your password, the harder it is to guess. NIST recommends at least 15 characters for a password used on its own. It allows passwords with 8 characters when you use an extra security step, such as MFA. NIST also says websites should not force users to add symbols or change passwords every few months.

CISA gives similar advice. It recommends passwords with at least 16 characters or 4 to 7 unrelated words. It also suggests using a different password for every account.

Hackers use several ways to guess passwords. Some tools try different letter, number, and symbol combinations. Others start with common words and passwords. They also try familiar swaps, such as using @ instead of a or 3 instead of e. These tricks are easy for password cracking tools to test.

Using the same password on different sites creates another risk. If one account gets hacked, someone may try that password on your other accounts.

A long password made from random words is harder to guess. Use a different one for each account to keep them safe.

5 Password Ideas That Pass a Strength Test

These good password ideas all passed our test. They are also easy to adapt into your own password suggestions. Every time below is a fast offline attack at 10 billion guesses per second. That is a harsh test. A real website slows attackers down far more.

1. Four Random Words

Pick four or more words at random. Do not use a song title or a saying. Join the words with no spaces.

PillowRocketTulipBench scored 4 of 4. It would take about 4 days to crack. Add a fifth word. PillowRocketTulipBenchCactus then takes centuries. Three words fall too fast. CoffeeBridgeAnchor lasts about 1 second. Read our guide on passphrase vs password for more detail.

2. A Long Sentence

Write a sentence only you would write. Remove the spaces. Make it odd. Odd sentences are easy to picture.

GrandmaBakesTenPiesByTheLake has 28 characters. It scored 4 of 4. It would take centuries to crack.

3. A Sentence Turned Into a Longer Acronym

Take the first letter of each word in a sentence. Then add a few full words at the end.

The sentence "I love baking tasty pies with my cousin Dina so does Dad" gives Ilbtpwmcdsd. Add a 2 and the word 'walk home'. The result is Ilbtpwmcdsd2walkhome. It has 20 characters. It scored 4 of 4. It would take about 11 months to crack. A short acronym alone falls far faster. The added words do the real work.

4. Stretch a Password You Already Have

You may need to keep a familiar base. Stretch it with extra words.

PizzaDay99 has 10 characters. It falls in under a second. PizzaDay99WithExtraCheese has 25 characters. It would take about 11 months. Use this idea on one account only. Never use the same base on two sites.

5. A Password Generator

A generator builds a random string. Nobody can guess it. Nobody needs to remember it either.

k7Qm2vXr9LpT4wZsB8 has 18 characters. It scored 4 of 4. It would take about 3 years to crack. Try our password generator. Choose 20 or more characters for key accounts. Save the result in your password manager.

Picking One for a Parent

If you are the family member who handles tech, help your parents choose a password they can remember and type without trouble. Three words may not be enough to keep an account safe.

For example, Google's AI Overview suggested CoffeeBridgeAnchor to a 72 year old, but it was cracked in about a second. Another suggestion, HereComesTheSun1969, was based on a song lyric and took less than an hour to crack.

CISA recommends using 4 to 7 unrelated words. Five words can be a good choice for parents. For example, PillowRocketTulipBenchCactus is much harder to crack. Ask your parent to imagine all five words in one funny scene. If they need help remembering it, write it on paper and keep it somewhere safe at home.

Password Ideas That Look Safe but Are Not

Some popular tips teach weak habits. Four of them are worth dropping. Each one feels clever. Each one fails for the same reason. The trick adds little. Length adds a lot.

Idea	Example	Score	Why it fails
Symbol swaps	Sun$h1n3!	1 of 4, under a second	Swaps sit in every cracking list
Keyboard shifts	jr;;p	1 of 4, under a second	The pattern is short and known
Repeating it	PizzaDay99 typed twice	Guesses only double	The base stays the same

Adding a site code	A tag for each site	Not scored	One leak shows the pattern

The last row needs a closer look. Say your base is the same on every site. Only the site code changes. One leak shows an attacker your pattern. They then guess your other accounts in seconds. You can check if your password was leaked. Do that if you ever used this habit.

Examples of Good Passwords and How They Scored

The table below covers work, Snapchat, Facebook, and Apple ID. It also shows one 8-character and one 15 character example. Times assume a fast offline attack.

Use	Example	Length	Time to crack
8 character	T7#mQ2!x	8	Under a second
15 character	BusLemonFigRain	15	About 4 hours
Work	StaplerOrbitCactusMarble	24	About 6 years
Snapchat	MangoTrainFrogSocksRiver	24	About 12 years
Facebook	WindowKiteBreadOwlMint	22	About 33 years
Apple ID	SoupLanternHorseWindowSpoon	27	About 87 years

Look at the first row. Eight characters fall instantly. NIST allows that length only with MFA. Look at the second row. Fifteen characters meet the NIST minimum. They still fall in hours. Longer is safer.

Need password ideas for work? Pick five random words. Your IT team may set its own rules. Follow them.

Never copy an example. Make your own. You can build one with our password generator.

Passcode Ideas for Your iPhone (and the Most Common Ones to Avoid)

Your passcode unlocks the phone. Face ID does the daily work. The passcode is the backup. Treat it with care.

Choose a random 6 digit code. A custom alphanumeric code is also a good choice. These are the best phone password ideas. A longer code is harder to guess. Your Apple Account password needs separate care. Use five random words there.

To switch to a custom alphanumeric code, open Settings. Tap Face ID and Passcode. Tap Change Passcode. Tap Passcode Options. Choose Custom Alphanumeric Code. Apple lists the latest steps on its Set a passcode guide.

Now look at what to avoid. A 2012 DataGenetics study examined about 3.4 million 4-digit codes. The code 1234 made up 10.7% of them. The top 20 codes made up 26.83%. The top 5 were 1234, 1111, 0000, 1212, and 7777. Those codes were used as a stand-in for PINs. The lesson still holds. People pick the same codes. Attackers try them first.

Skip birthdays too. Skip your address. Skip repeated digits. Our upcoming post on the most common passwords will list more.

Best Password for a Laptop

A passphrase can make your laptop password both strong and easy to remember. Instead of using a random mix of letters and numbers, try combining a few unrelated words, such as TeaGhostRiverLampDrum. It has 21 characters and scores 4 out of 4 for password strength.

You can remember it by saying each word in your head as you type. After a few uses, typing it will feel natural. It is easier to remember than a random string while still offering good protection. Just make sure to create your own combination rather than using this exact example.

Where to Keep Your New Passwords

Nobody can remember 50 random passwords. A password manager fixes that problem. You remember one pass phrase. The manager keeps the rest.

RelyPass is a free offline password manager for iPhone. Your passwords stay on your phone, and they're free to keep there forever. The vault is encrypted with your pass phrase.

Be clear on one point. Lose the pass phrase and nobody can recover the vault. That includes us. Choose a pass phrase you can remember. Write it on paper and keep it at home.

The family plan covers up to 5 people. Each person gets a private, encrypted vault. For more habits, read how to keep your passwords safe.

FAQ

What is a good password to use?

A good password has at least 15 characters. Build it from random words or a long sentence. Use it on one account only. NIST sets 15 characters as the minimum for a password used alone. Never reuse it. Keep it in a password manager so you only remember one.

How do you come up with a good password?

Pick four random words. Join them with no spaces. PillowRocketTulipBench is an example. It scored 4 of 4 in our strength test. It would take about 4 days to crack. A fifth word pushes that to centuries. Never copy an example. Pick your own words from a random source.

What are some good passwords for your phone?

Use a random 6 digit passcode. A custom alphanumeric passcode is also fine. Never use 1234. A 2012 DataGenetics study found 1234 made up 10.7% of the codes it studied. Skip birthdays and repeated digits. Face ID can handle daily unlocks. The passcode then stays a backup you rarely type.

What is the most secure password?

A long random one from a password generator. Store it in a password manager. Then you never need to remember it. Make it 20 or more characters. Use it on one account only. NIST backs length over tricks. Only the manager needs a pass phrase you can recall.