

Unknown date

Unknown author

Simple Tricks to Remember Insanely Secure

Passwords

One way to ensure that you remember your passwords is to use the same one for every secure site. You know, something simple, like your dog's name. That's one way, sure, but it's not a *good* way. If use the "Fido technique," your password is easy to guess, and you can bet some ne'er-do-well will guess it. Worse, if you use the same password everywhere, then a crook who cracks one site gets access to them all. Really, the only way to use a complex, unique password for every secure site is to install a password manager.

The [best password managers](#) work on all your devices, be they desktops, laptops, smartphones, or tablets. They generate unguessable passwords like *ir23#m#uBJP!4i0k*, remember them for you, and automatically use those saved passwords to log in to your secure sites.

But there's a problem. Almost every password manager relies on a master password to lock up all those saved passwords. The master password must be totally unguessable, because anyone with access to it can unlock all your secure sites. But it also must be totally memorable. If you forget the master password, nobody can help you. On the plus side, this also means a dishonest employee can't break into your password store, and the NSA can't force the company to turn over your data.

So, even if you wisely rely on a password manager, you still have to remember one insanely secure password. How? Here are some techniques to get you started.

Make It Poetic

Everybody has a favorite poem or song that they'll never forget. It might be from Shakespeare, or Pussy Riot, or the Bonzo Dog Doo Dah Band.

Whatever the stanza or verse, you can turn it into a password. Here's how.

Start by writing down the first letter of each syllable, using capital letters for stressed syllables and keeping any punctuation. Let's try this line from *Romeo and Juliet*: "But soft, what light through yonder window breaks?" From that, you'd get *bS,wLtYdWdB?* You could add *A2S2* for Act 2, Scene 2, if that's something you'll never forget. Or *1597* for the year of publication.

If the passage doesn't have a strong meter, you can just take the first letter of each word, using the existing punctuation and capitalization. Starting with the quote "Be yourself; everyone else is already taken. – Oscar Wilde", you could come up with *By;eeiat.-OW*. Adding a memorable number rounds out the password, perhaps *1854* (his birthdate) or *1900* (his death).

Your poetic password will be completely different from these examples, of course. You'll start with your own meaningful song or quotation and convert it to a unique password that nobody else could guess.

Use a Passphrase

Password pundits always advise including all four types of characters: uppercase letters, lowercase letters, digits, and symbols. The reasoning is that by expanding the pool of characters, you vastly expand the time required to crack the password. But sheer length also serves to make cracking harder, and one way to achieve a long, memorable password is to use a passphrase.

Snarky, smart webcomic XKCD took aim at wacky password schemes that suggest starting with a common word, replacing some of the letters with similar-looking numbers, and tacking on a few extra characters. That can leave you wondering. Was it *Troub4dor&3*, or *Troub4dor3&?* Or maybe *Trom3one&3*? A passphrase like [correct horse battery staple](#) is significantly more difficult to crack, due to its length, but also much easier to remember.

Not all password managers permit spaces in the master password. No problem! Just pick a character like the hyphen or equals sign to separate the

Pick words that don't naturally go together, then invent a mnemonic story or image to link them. What would you picture for "butter-proceeds-goof-scream?"

If you have trouble coming up with unrelated words for your passphrase, there are many online passphrase generators, including the aptly named CorrectHorseBatteryStaple.net. You may quite reasonably worry about using a passphrase generated by someone else's algorithm. In that case, you could generate multiple passphrases and clip out the first word from each.

Longer Passwords Are Better Passwords

Long-time PC maven Steve Gibson suggests that the secret to long, strong passwords is padding. If an attacker can't crack your password using a [dictionary attack](#) or other simple means, the only recourse is a brute-force scan of all possible passwords. And every added character makes that attack massively more difficult.

Gibson's website offers a [Search Space Calculator](#) that analyzes any password you enter based on the character types used and the length. The calculator delivers an estimate of how long a brute-force attack would take to crack a given password. It's not a password strength meter, but rather a cracking-time meter, and it's instructive to see how the cracking time goes up when you lengthen the password.

I don't try to watch people enter their passwords, but I've noticed quite a few that, based on hand motions, appear to end in three exclamation points. That's not the padding I'd suggest. First, it requires the shift key. Second, it's too predictable. I wouldn't be surprised if password cracking toolkits already included "!!!" in their dictionaries.

Instead, pick two close-at-hand keys and alternate, adding something like *vcvcvcvc*. Or choose three characters, like *lkjlkjlkjlkj*. Gibson's calculator says that it would take over 45 years for a "massive cracking array" to crack *bS,wLtYdWdB?* (the Romeo and Juliet password from my earlier example). Adding *vcvcvcvc* raises that to more than a quadrillion centuries.

Long, Strong, and Memorable

Once you've invested in a password manager and converted all your logins to use strong, unique passwords, the only password you still have to remember is the one that opens the password manager itself. That master password unlocks everything else, so you really need to spend some time coming up with a master that you can remember easily, but that would be impossible for someone else to guess, or crack.

Work up a password based on a poem, song, or famous quote. Or create a passphrase, linking unrelated words with a memorable image or story. Then add some easy-to-type padding. You'll wind up with a master password that's both memorable and uncrackable.

Viewed using [Just Read](#)