Memorizing a good email password is easy. Here's how to do it

We all hate remembering passwords. But it's very doable.

By Alaina Yee Senior Editor, PCWorld Feb 14, 2025 7:30 am PST

Image: Pixabay

Using a password manager is a smart move. So is protecting your primary email account with a strong credentials. Combining the two seems like an equally good call, but it's actually dangerous—should you ever lock yourself out of your password manager, you run the risk of losing access to your email account. Also if your password vault is ever compromised, your email account becomes vulnerable to unauthorized access.

I wrote a warning last year about this hazard, and then again earlier this month. Lots of readers took notice. One in particular reached out to me with a very fair question: "You say one should memorize their email password. I use a 16-character random password. Not in 2 years can I memorize that. Any other suggestions?"

Fortunately, a few easy solutions exist for this problem. While not perfect, they're secure and provide an escape hatch for the lock-out issue. We'll start with the absolute simplest—in which you have to memorize absolutely nothing.

Option A: Add a passkey to your account

Unlike passwords, passkeys rely on small amounts of encrypted data to facilitate authentication. Part of the set gets stored on a device you own, while the other part is kept by the service or app you have an account with.

You don't have to memorize anything at all. Even better, passkeys are stronger than passwords as well as being phishing resistant. They're tied to the device they're stored on. The one downside is that if your phone or PC becomes unavailable, you also lose access to any saved passkeys—but you can remedy this by creating more than one passkey on different devices.

By adding a passkey as an additional login method, you can keep your current password setup as-is. You won't gain any extra protection against unauthorized access to your password vault (which is why two-factor authentication is a necessity), but you will have another way to log into your email.

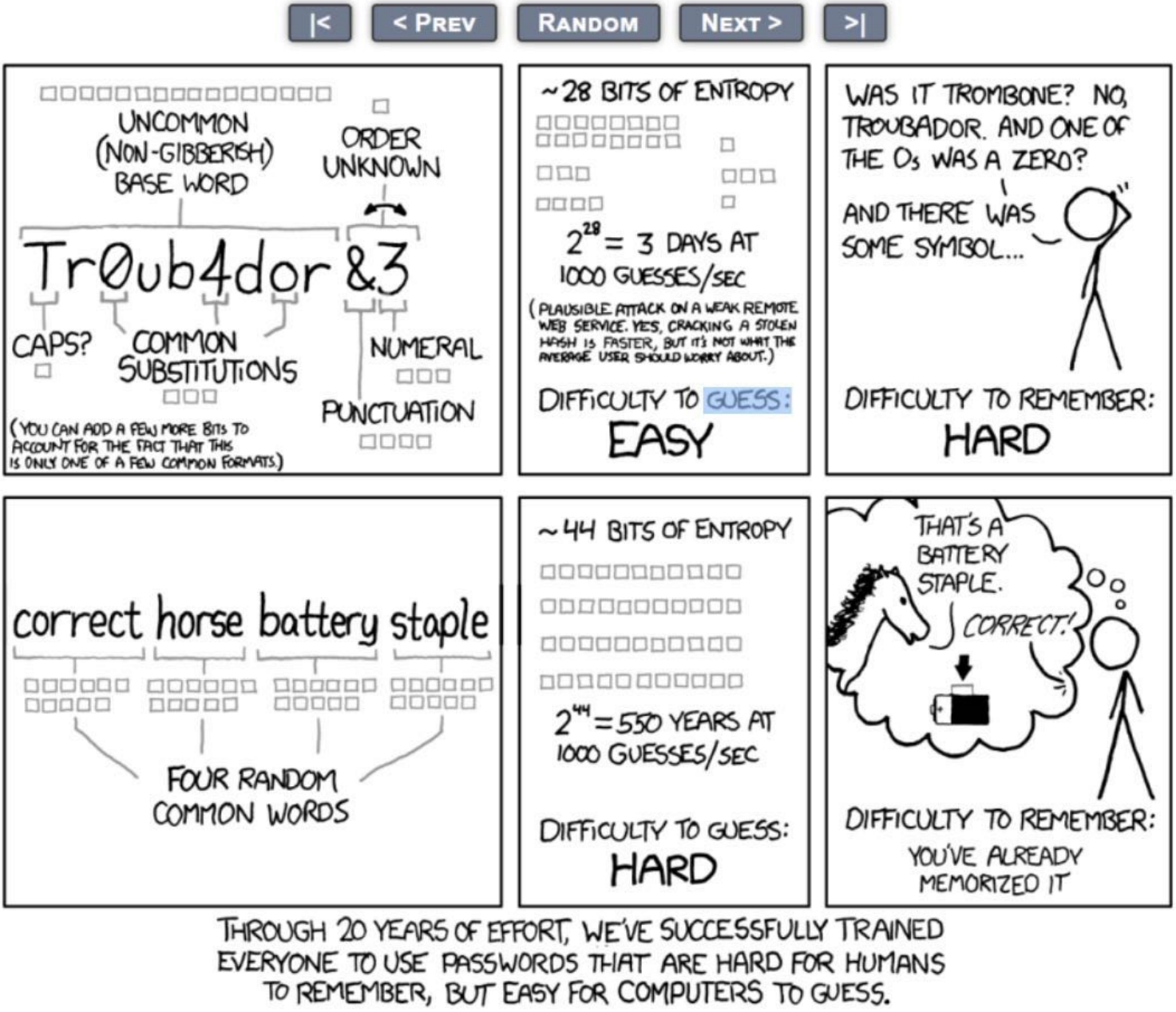
Pros ✅	Cons ❌
• You don't have to change your existing login habits.	• If you lose your device, you lose your passkey. • Your email account is still vulnerable if your password manager is ever compromised (and you don't have 2FA enabled).

Option B: Switch to a passphrase

Popularized by web comic xkcd, this variation on passwords mashes together unrelated words to create the necessary combination of randomness and uniqueness.

Combining multiple words in this way is simpler to remember than a random-generated password, especially if you can make up a story (or use another memory trick) to help with recall. And passphrases rely on the randomness of the word combination for their strength, so you don't have to add special characters or numbers. In fact, you shouldn't unless they're also random insertions—which are harder to remember.

Editor's Note: This space is intentionally left blank to be able to present the following graphic (hopefully) in a more 'readable' size.



The comic that popularized passphrases.

xkcd

For a truly effective passphrase, you can use a password manager's generator, either in the app or through online tools. (Don't have a password manager yet? We have recommendations, if you need one.) Aim for at least four words, with six words (or even more) as a beefier starting point. The longer a password or passphrase, the stronger it is.

(As a rough point of reference: If replacing a 16-character random password that contains capitalization, numbers, and special characters, a six-word passphrase provides roughly similar strength. A password's advantage is that it can fit more entropy into shorter lengths, relative to passphrases.)

Explore frequently asked questions

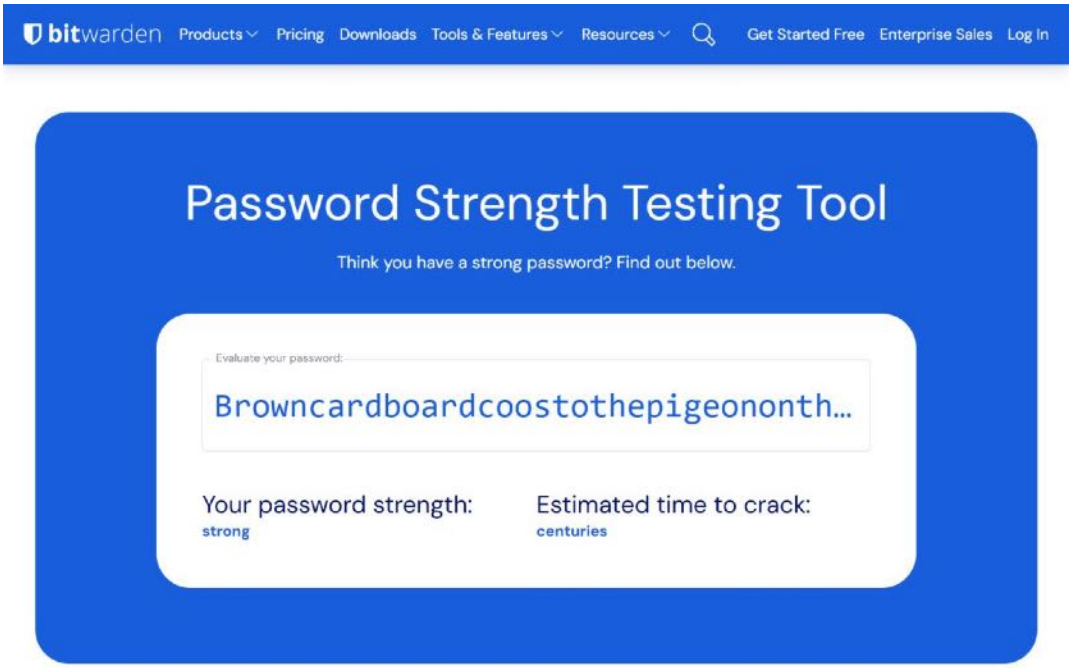
Pros ✅	Cons ❌
• Keeps your email login info private. • Much easier to remember than a truly random password with numbers, capitalization, and special characters.	• Still requires memorization. • Not as strong as a random password if you have character limits (e.g., password cannot be longer than 16 characters.) • If ever stored improperly by your email service, a leaked passphrase can be potentially easier to crack (which is problematic unless you have 2FA enabled as an extra layer of defense).

Option C: Use a memorable password

For most people, this option won't count as easy—so memorable is a very relative term here.

Compared to the other methods above, this one requires a much higher level of memorization. But depending on how your brain works, you may find this easier than recalling a group of unrelated words. It can also be a necessary evil when passkeys aren't supported and a passphrase's effectiveness is blunted by character limits.

The general thought here is to create your own randomness by leaning on a sentence or long phrase only you know (and no one can guess), and then adding capitalization, numbers, and special characters. Avoid drawing wholesale from songs, movies, catchphrases, novels, and the like for your source material—someone could guess at your password if you use sections verbatim or even pull pieces from a popular quote.



You can use tools like Bitwarden's password strength tool to get a rough idea of how strong your homebrew password is.

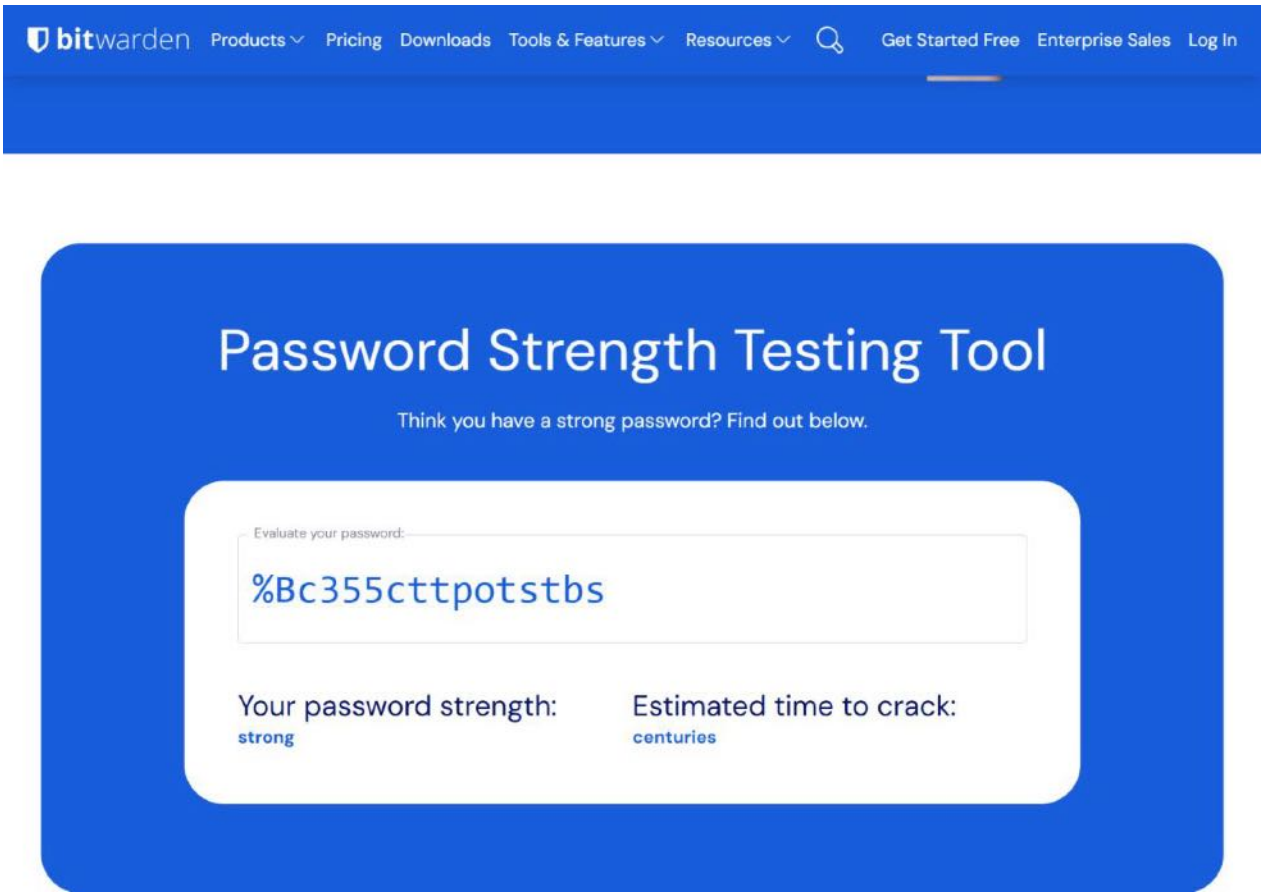
Bitwarden

A rough example of this method is constructing a nonsensical sentence based on mundane things already in your memory, but would never mention in combination to anyone else. Example: Your commute often takes you by big piles of cardboard, a bunch of talkative pigeons always hang out at your bus stop, and the word "slurry" appears in your head a lot. (Humor me on that last one.)

From here, you could use just the sentence "*Brown cardboard coos to the pigeon on the slurry*" as your own passphrase. You could also slap in a number and a special character, picking them and their position based on other things in your memory, if you like complexity. (Goes against the point of this article, but who am I to keep you from your fun?)

For this example, I'll choose a building number on the corner near my favorite ice cream store, and the % sign because I like how it looks. Then I'll stick the special character at the start because I know it's a less common spot, and the number after the second word, because this fictional email account is the second email address I ever created.

`%Browncardboard355coostothepigeononntheslurry`



This password is only 16 characters long, but it's reasonably secure. (Again, these kind of evaluation tools are only rough estimators.)

Bitwarden

For shorter passwords, you can use just the first character of each word (or last, or third, or etc). That's not usually necessary nowadays, since major email providers let you create a password as long as you want. But let's say I'm using this method for a bank account (rather than email), where I'm limited to just 16 characters.

As mentioned above, a passphrase won't be as strong with just 16 characters, and few banks offer passkey support. If I snag the first character from each word of this made-up sentence, I get:

`%Bc355cttpots`

A little short, and thus notably less secure, so I'll also add some spice and three more characters from "*this bank sucks*"

`%Bc355cttpotstbs`

And at long last, I have a strong password I should be able to remember… provided I type it enough times repeatedly so it sticks. We should all riot until passkeys are ubiquitous.

Pros ✅	Cons ❌
• Depending on how constructed, can be easier for some minds to recall. • The only best strong option if an account doesn't support passkeys and also blunts the effectiveness of a passphrase by limiting passwords to a short number of characters (e.g., 16 max).	• Creating the password can be complex (or downright convoluted), and then you still have to remember it. (Trust me, I get why people store their email account login info in their password managers.)

Author: Alaina Yee, Senior Editor, PCWorld

A 14-year veteran of technology and video games journalism, Alaina Yee covers a variety of topics for PCWorld. Since joining the team in 2016, she's written about CPUs, Windows, PC building, Chrome, Raspberry Pi, and much more—while also serving as PCWorld's resident bargain hunter (#slickdeals). Currently her focus is on security, helping people understand how best to protect themselves online. Her work has previously appeared in PC Gamer, IGN, Maximum PC, and Official Xbox Magazine.