

Forget about passwords: You need a passphrase!

Forget about passwords – it's all about passphrases. Longer, more complex and easy to remember, they will help you be more safe and secure. Our guide shows you how to create a passphrase.

123456. password. 12345678. qwerty. 12345.

All of the above, so easy to remember, so quick to type, so conveniently effortless to manage, represent five of the most common passwords used today. Despite of the fact that more people than ever understand that cybercrime is a growing threat and that data breaches are commonplace, poor security practices are rife. Yet this needn't be the case, especially when it comes to passwords. A little effort can make a huge difference.

The solution? You need to forget about passwords. Simply put, they are easy to crack and not strong enough to offer appropriate security. This is especially true of single word passwords, something like 'strawberries', for example, is asking for trouble. So, what comes instead of passwords? Passphrases. Longer, more complex and easy to remember, they will help you be more safe and secure. On World Password Day (<https://passwordday.org/>), here's a quick guide on how to do this.

Step 1 – Add words to create a phrase

Let's say you like to read. Add some words around it so that it makes sense to you in a meaningful way:

That's a good start, but it could do with being longer. Be more specific:

Step 2 - Add capitals for emphasis

Your passphrase as it currently stands is a lot stronger than the original password. However, it needs more detail. Add capitals, as if you're emphasizing each word (in

Step 3 - Add punctuation for creative flair

Consider this step as a decorative element, as if you're now considering your passphrase visually. To make it easier, add punctuation at the beginning and at the end:

Step 4 - Add spaces to add further complexity

A lot of people are unaware of the fact that you add spaces to your passphrase. This makes it much more complex.

Step 5 - Add block capitals to go one step further

Your passphrase is in good shape. However a 'final topping' will add another layer of security - block capitals:

So there you have it. Five easy steps that takes you from a weak, single word password to a stronger, more complex passphrase.

Some other tips



While we're here, it's also important to remember the following tips for extra password security:

Short passwords are bad. Long passphrases are good

Never reuse an old password

Use two-factor authentication ([/tag/two-factor-authentication/](#)) for added security

Ensure that every account you have has a distinct passphrase

Change your passphrases periodically

Use a reliable password manager

We'd love to hear about some of your password bloopers. What's the worst password you've ever have? The corniest? How often do you forget your passwords? Share your comments below!