



Digital Foundations

Passwords

Practice using the three methods detailed to build a new more secure password:

- 1 Do you use the same password for more than one thing?
- 2 Does your password mention a number that would be easy to guess like your birthday?
- 3 Does your password use your name?

If so, your password may be **WEAK!**

PASSWORD BASIC RECOMMENDATIONS:

- 1 Include at least one symbol.
- 2 Include at least one UPPERCASE and one lowercase letter.
- 3 Passwords should be at least 7 characters.
- 4 Passwords should be easy to remember (unless using a password manager).
- 5 A password manager is a website/app that helps users save and organize their passwords.
- 6 Passwords should not be a single common word or personal information (birth date, parent's name, etc.).
- 7 Passwords **should not** be shared between websites.

PRACTICE BUILDING YOUR OWN PASSWORD HERE:

On the next page, you will see three other password methods you can use to build secure passwords. We will practice them together next.



BRUCE SCHNEIER'S METHOD

Security expert Bruce Schneier put forth a password method back in 2008 that he still recommends today. It works like this: Take a sentence and turn it into a password.

The sentence can be anything personal and memorable for you. Take the words from the sentence, then abbreviate and combine them in unique ways to form a password. Here are four sample sentences that I put together:

- 1 **WOO!TPwontSB** = Woohoo! The Packers won the Super Bowl!
- 2 **PPupmoarT@O@tgs** = Please pick up more Toasty O's at the grocery store.
- 3 **1tubuupshhh...imj** = I tuck button-up shirts into my jeans.
- 4 **W?ow?imp::ohth3r** = Where oh where is my pear? Oh, there.

[PRACTICE BUILDING YOUR OWN PASSWORD HERE:](#)

COME UP WITH 12 RANDOM WORDS

- 1 You can start with a phrase such as “Even in winter, the dogs party with brooms and neighbor Kit Kats.” Just make sure it is not a simple phrase or a phrase taken from existing literature. You can grab 12 random words, too: “Pantry duck cotton ballcap tissue airplane snore oar Christmas puddle log charisma.”
- 2 When placed into a password checker, the 12-word pass phrase above shows that it will take 238,378,158,171,207 quadragintillion years for a brute force attack to crack.

[CREATE YOUR OWN 12 WORD PHRASE HERE:](#)

THE PAO METHOD

- 1 Memorization techniques and mnemonic devices might help you remember an unbreakable password. At least, that's the theory put forth by Carnegie Mellon University computer scientists who suggest using the Person-Action-Object (PAO) method to create and store your unbreakable passwords.
- 2 PAO gained popularity in Joshua Foer's bestselling book “Moonwalking with Einstein.” The method goes like this: Select an image of an interesting place (Mount Rushmore). Select a photo of a familiar or famous person (Beyonce). Imagine some random action along with a random object (Beyonce driving a Jello mold at Mount Rushmore).
- 3 Once you create and memorize several PAO stories, you can use the stories to generate passwords.
- 4 For example, you can take the first three letters from “driving” and “Jello” to create “driJel.” Do the same for three other stories, combine your made-up words together, and you'll have an 18-character password that'll appear completely random to others yet familiar to you.

[CREATE YOUR OWN PAO METHOD HERE:](#)
