TAKE CONTROL OF YOUR PASSWORDS

THE CHEAT SHEET

In a Nutshell

When a Web site or service asks you to create a password, it's tempting to use something that's easy to remember and type, like `password` or `baseball`, or reuse a password you've used on dozens of other sites. But with hacking and password theft on the rise, that's risky behavior.

A sound password strategy gives you a combination of security (passwords that are sufficiently complex to resist guessing by humans or computers) and ease of use (not having to remember and constantly type many long strings of random gibberish).

Password Threats

- **You:** Don't be oblivious!
- **Guessing:** Common passwords are unsafe.
- **Brute force:** Computers can test passwords by the billions.
- **Theft:** There are many ways to steal or hack passwords.
- **Social Engineering:** Don't get tricked into revealing passwords!

What Not to Do

- Never reuse a password on more than one site!
- Forget simple transformations and substitutions.
- Avoid keyboard patterns and "padding" shorter passwords.

Remember, hackers know all these tricks, too (and many more), and their tools can work around them.

Entropy FTW

For passwords with higher *entropy* (resistance to guessing), use any or all of these techniques:

- Increase password length
- Mix character types (upper- and lowercase letters, digits, and punctuation)
- Select characters randomly

A Sound Strategy

Rely on your brain (and manual effort) only when necessary. Let technology help you with the rest of your password needs. There are just two main parts to a good password strategy.

VIPs: Create a short list of (typically 3 to 6) **V**ery **I**mportant **P**asswords you need frequently and may have to enter without assistance. Examples:

- The master password for your password manager
- The login password for your Mac or PC
- Your Apple ID, Gmail, and Dropbox passwords

Make these passwords strong (high entropy) and memorize them.

Password Managers: Use an app that can ***generate*** long, random passwords, ***store*** them securely, ***sync*** them across all your devices, and ***enter*** them when needed. Examples:

- 1Password
- LastPass
- RoboForm

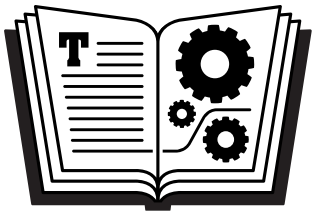
These and many others are available for Mac, Windows, iOS, and Android devices.

Security Questions

When asked to supply the answer to a "security" question (often used for resetting lost passwords), **lie**. It's easy for someone to find out your mother's maiden name or your high school mascot. Just be sure you remember the answer you gave—put it in your password manager for safekeeping.

Other Tips

- Keep your VIPs safe; if someone finds them or watches you enter them, all bets are off. But…
- Make sure a loved one or colleague can access your passwords in an emergency.
- When feasible, enable two-factor authentication (supplementing passwords with another factor, such as sending a security code to your mobile phone).
- Don't forget to update older, weaker passwords!



Buy the book at
takecontrolbooks.com/passwords