Take These 7 Steps Now to Reach Password Perfection

Galen Garretson Portions courtesy of wired.com

Your passwords are a first line of defense against many internet ills, but few people actually treat them that way. Whether it's leaning on lazy Star Wars references or repeating across all of your accounts—or both—everyone is guilty of multiple password sins. But while they're an imperfect solution to begin with, putting in your best effort will provide an immediate security boost.

Don't think of the following tips as suggestions. Think of them as essentials, as important to your daily life as brushing your teeth or eating your vegetables. (Also, eat morevegetables.)

1. **Use a password manager.** A good password manager, like 1Password or LastPass creates strong, unique passwords for all of your accounts. That means that if one of your passwords does get caught up in a data breach, criminals won't have the keys to the rest of your online services. The best managers sync across desktop and mobile devices and have auto-complete powers. Now, rather than having to memorize dozens of meticulously crafted passwords, you just must remember one master key.
   For a review of password managers by PC Magazine click here.

2. **Go long.** Despite what all those prompts for unique characters and uppercase letters might have you believe, length matters more than complexity. Once you get into the 12-15 character range, it becomes way harder for a hacker to brute force, much less guess, your password. One caveat: Don’t just string together pop culture references or use simple patterns. Mix it up! Live a little! A quick for instance: "g0be@r$" does you way less favors than "chitown banana skinnydip."

3. **Keep 'em separated.** When you do deploy those special characters—which, if you opt against a password manager, lots of input fields will force you to—try not to bunch them all together at the beginning or end. That’s what everyone else does, which means that’s what bad guys are looking for. Instead, space them out throughout your password to make the guesswork extra tricky.

4. **Don’t change a thing.** You know how your corporate IT manager keeps making you change your password every three months? Your corporate IT manager is wrong. The less often you change your password, the less likely you are to forget it, or to fall into patterns—like just changing a number at the end each time—that make them easier to crack.

5. **Single-serve only.** If you’re on the password manager train, you’re already all over this. But if you can’t be bothered, at the very least make sure that you don’t reuse passwords across different accounts. If you do, a retailer breach you have no control over could end up costing your banking password.

See for yourself: Have I Been Pwned? has nearly 5 billion compromised accounts on file—if yours is one of them, there’s a chance your favorite password might already be toast.

6. **Don’t trust your browser.** A convenient shortcut to remembering all those passwords, or getting a paid password manager account, is letting your browser remember them for you. You’ve seen the option yourself. You probably even use it on at least one site. Don’t! The option is convenient, but the underpinning security is often undocumented, and it doesn't require that your password actually be, you know, good. If you need a free and easy option, go with a password manager like Dashlane instead of trusting everything to Chrome.

7. **Add two-factor too.** Hate to say it, but these days not even a password is enough. Many of the services you use today—social networks, banks, Google, and so on—offer an added layer of protection. It can come in the form of a code sent to your phone via SMS, or if you want to step it up, through software solutions like Google Authenticator or hardware like a YubiKey. SMS should be enough for most people; just know that like many entry level security precautions, it's not perfect.

Has your email address and password been released through a breech??
Check these sites to find out:
https://haveibeenpwned.com/
https://breachalarm.com/
https://haveibeencompromised.com/

To test the strength of the passwords you commonly use check these sites:
https://howsecureismypassword.net/
https://thycotic.com/resources/password-strength-checker/
http://www.passwordmeter.com/