



Tech Tips and Tricks

Credential Crimes: Are you committing password misconduct? By Lizzy Cary

If you're like me, you think passwords are the bane of your existence - especially when you are forced to change them so often. Between bank accounts, social media accounts, and email, it probably feels like you must change and remember a new password each week. Plus, you need to come up with something creative that nobody can guess.

Recently, researchers at Virginia Tech gathered 6.1 million anonymized passwords from across the web and had Dashlane, a tech company, analyze them.¹ To their dismay, they found very troubling patterns. Aside from using the same password across numerous accounts, the most common password faux pas that the researchers came across was "password walking." "Password walking" is when a password is created that contains a combination of numbers, letters, and symbols that are adjacent to one another on the keyboard, such as "qwerty" or "12345." Other common themes found were passwords that contained aggressive and/or vulgar language, popular sports teams, or pop culture references. All of these themes leave users vulnerable to hackers who can easily guess their login information. If one (or all) of your passwords is currently "IloveStarWars," you should probably stop reading this and go change that immediately.

Luckily, there are plenty of programs out there that can help us keep track of the numerous, strong passwords that we should have. My personal favorite is LastPass. After importing all your login and password information into your encrypted LastPass "vault," you only have to remember one master password. Every morning, I log into LastPass with my master password. From that point on, LastPass will automatically enter the password for me every time I visit a website that requires me to login. Aside from keeping track of your passwords, LastPass will also generate strong passwords for you. Think your passwords are strong enough the way they are? Take the LastPass security challenge to find out how secure they *really* are. It will analyze the passwords for all your accounts, then take you step-by-step through improving your passwords. There are multiple other great features to LastPass, such as credit monitoring, two-factor authentications, and a mobile app. But, the best part of LastPass is that it is free! Other great password management programs include Dashlane, 1Password, Roboform, and StickyPassword – all with different features. Browse their websites and see which one would work best for you!

¹ Wang, et. al, 2018, *The Next Domino to Fall: Empirical Analysis of User Passwords across Online Services*.

While everyone hates trying to remember multiple passwords, it should bring you some comfort knowing there are numerous programs out there that can do the hard work for you, all while keeping your information safe from hackers. So, the next time you are faced with the annoying task of changing your password, try using a program like LastPass to generate and save a safe, strong password – rather than typing in *Thisreallysucks123*.