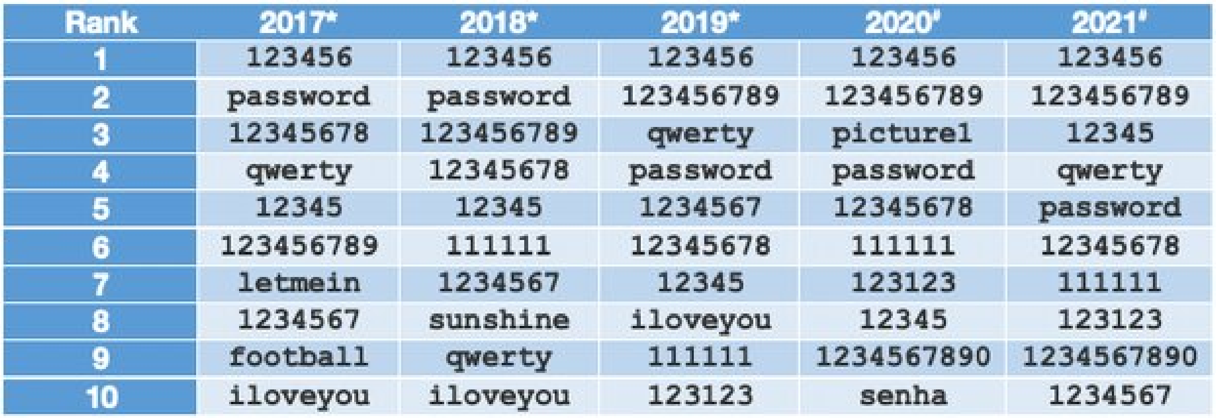
This New Year, why not resolve to ditch your dodgy old passwords?

January 3 2022, by Paul Haskell-Dowland, Lorrie Cranor



Rank	2017*	2018*	2019*	2020#	2021#
1	123456	123456	123456	123456	123456
2	password	password	123456789	123456789	123456789
3	12345678	123456789	qwerty	picture1	12345
4	qwerty	12345678	password	password	qwerty
5	12345	12345	1234567	12345678	password
6	123456789	111111	12345678	111111	12345678
7	letmein	1234567	12345	123123	111111
8	1234567	sunshine	iloveyou	12345	123123
9	football	qwerty	111111	1234567890	1234567890
10	iloveyou	iloveyou	123123	senha	1234567

2017-2019 list of common passwords from SplashData, 2020-2021# from NordPass

Most of the classic New Year resolutions revolve around improving your health and lifestyle. But this year, why not consider cleaning up your passwords too?

We all know the habits to avoid, yet so many of us do them anyway: using predictable passwords, never changing them, or writing them on sticky notes on our monitor. We routinely ignore the recommendations for good passwords in the name of convenience.

Choosing short passwords containing common names or words is likely to lead to trouble. Hackers can often guess a person's passwords simply by using a computer to work through a long list of commonly used words.

The most popular choices have changed very little over time, and include numerical combinations such as "123456" (the most common password for five years in a row), "love," keyboard patterns such as "qwerty" and, perhaps most ludicrously, "password" (or its Portuguese translation, "senha").

Experts have long advised against using words, places or names in passwords, although you can strengthen this type of password by jumbling the components into sequences with a mixture of upper- and lowercase characters, as long as you do it thoroughly.

Complex rules often lead users to choose a word or phrase and then substitute letters with numbers and symbols (such as "Pa33w9rd!"), or add digits to a familiar password ("password12"). But so many people do this that these techniques don't actually make passwords stronger.

It's better to start with a word or two that isn't so common, and make sure you mix things up with symbols and special characters in the middle. For example, "wincing giraffe" could be adapted to "W1nc1ng_!G1raff3"

These secure passwords can be harder to remember, to the extent you might end up having to write them down. That's OK, as long as you keep the note somewhere secure (and definitely not stuck to your monitor).

Reusing passwords is another common error—and one of the biggest. Past data leaks, such as that suffered by LinkedIn in 2012, mean billions of old passwords are now circulating among cyber criminals.

This has given rise to a practice called "credential stuffing"—taking a leaked password from one source and trying it on other sites. If you're still using the same old password for multiple email, social media or financial accounts, you're at risk of being compromised.

Pro tip: Use a password manager

The simplest and most effective route to good password hygiene is to use a password manager. This lets you use unique strong passwords for all your various logins, without having to remember them yourself.

Password managers allow you to store all of your passwords in one place and to "lock" them away with a strong level of protection. This can be a single (strong) password, but can also include face or fingerprint recognition, depending on the device you are using. Although there is some risk associated with storing your passwords in one place, experts consider this much less risky than using the same password for multiple accounts.

The password manager can automatically create strong, randomized passwords for each different service you use. This means your LinkedIn, Gmail and eBay accounts can no longer be accessed by someone who happens to guess the name of your childhood pet dog.

If one password is leaked, you only have to change that one—none of the others are compromised.

There are many password managers to choose from. Some are free (such as Keepass) or "freemium" (offering the option to upgrade for more functionality like Nordpass), while others charge a one-off fee or recurring subscription (such as 1Password). Most allow you to securely sync your passwords across all your devices, and some let you safely share passwords between family members or work groups.

You can also use the password managers built into most web browsers or operating systems (with many phones offering this functionality in the browser or natively). These tend to have fewer features and may pose compatibility issues if you want to access your password from different browsers or platforms.

Password managers take a bit of getting used to, but don't be too daunted. When creating a new account on a website, you let the password manager create a unique (complex) password and store it straight away—there's no need to think of one yourself.

Later, when you want to access that account again, the password manager fills it in automatically. This is either through direct integration with the browser (typically on computers) or through a separate application on your mobile device. Most password managers will automatically "lock" after a period of time, prompting for the master password (or face/finger verification) before allowing access again.

Protect your most important passwords

If you don't like the sound of a password manager, at the very least change your "critical" account passwords so each one is strong and unique. Financial services, email accounts, government services, and work systems should each have a separate, strong password.

Even if you write them down in a book (kept safely locked away) you will significantly reduce your risk in the event of a data breach on any of those platforms.

Remember, however, that some sites provide delegated access to others. Many e-commerce websites, for example, give you the option of logging in with your Facebook, Google or Apple account. This doesn't expose your password to greater risk, because the password itself is not shared.

But if the password is compromised, using it would grant access to those delegated sites. It is usually best to create unique accounts—and use your password manager to keep them safe.

Adopting a better approach to passwords is a simple way to reduce your cyber-security risks. Ideally that means using a password manager, but if you're not quite ready for that yet, at least make 2022 the year you ditch the sticky notes and pets' names.

This article is republished from The Conversation under a Creative Commons license. Read the original article.

Provided by The Conversation

Citation: This New Year, why not resolve to ditch your dodgy old passwords? (2022, January 3) retrieved 9 May 2024 from https://techxplore.com/news/2022-01-year-ditch-dodgy-passwords.html