Top 25 most common passwords by year according to SplashData

Rank	2011[4]	2012[5]	2013[6]	2014[7]	2015[8]	2016[3]	2017[9]	2018[10]
1	password	password	123456	123456	123456	123456	123456	123456
2	123456	123456	password	password	password	password	password	password
3	12345678	12345678	12345678	12345	12345678	12345	12345678	123456789
								345678
								345

This Is The World's Most Common Password

February 10, 2017
by SentinelOne

At this point, it's not even funny. In 2016, the world's most common password was "123456." Surprise galore, "123456" was also the most common password in 2015. In 2014, you may be shocked to learn, the most common password was also "123456." That sound you're hearing is the noise a broken record makes.

At this point, maybe let's not focus on the sheer ridiculousness of this statistic. It's overplayed—passwords are obsolete and people choose bad ones when given the choice. Instead, let's look at some background facts. How are these "most common passwords" lists made, anyway? Does using a common password really make you insecure? How secure does using a "secure" password make you, anyway?

How do these "Most Common Password" Lists Even Get Made?

The first thing that you should know is that, while a lot of data gets stolen, not all of that data is valuable. Even lists of passwords aren't necessarily that great. Hackers, as we've often said, are lazy. If you have an email address and a password, you might eventually be able to find someone's address, get their credit card number, and start committing identity theft—but that takes a lot of work. Why's this important?

Due to the rather fungible value of password lists, hacking groups will often post their spoils directly to the internet. This is usually for bragging rights, although it also might be a free sample. Either way, the venue for these postings is usually a site called Pastebin. The public nature of these posts means that companies are able to look for the most common passwords, and therefore assemble these yearly scorecards.

If You Use a Weak Password, Will You Get Hacked?

You're not guaranteed to get hacked if you use one of the most common passwords from 2016—but you'll make it *very* easy for any hacker who tries to target you. Here's how this works:

Normally, when an attacker steals a list of passwords, they'll come out as a list of encrypted phrases, called hashes. By design, hashes are one-way encryption—you're not supposed to be able to use math to turn a hash back into plaintext. The problem, however, is that hashes with the same input always return the same output. In other words, if you take the password "123456" and run it through an MD5 hash generator, you'll always get the output "e10adc3949ba59abbe56e057f20f883e."

If you're a hacker, and you've just stolen a bunch of hashed passwords, you know that the odds are that a bunch of the hashes in there are from people who picked "123456" as their password. If you know that the hashing algorithm was MD5, you can just do CTRL-F for "e10adc3949ba59abbe56e057f20f883e" and steal all those passwords right away. Hackers will usually do this with a whole bunch of the most common passwords, in what's known as a "pre-computed dictionary attack."

Is Your "Secure" Password As Secure As You Think It Is?

A lot of people are now wise to the fact that you shouldn't choose a simple password. There's a huge but coming up, however—the passwords that we generally think of as secure, aren't. Choosing a password with capital letters, numbers, and symbols probably will pose a minor impediment to a hacker who seriously wants your information.

First of all, you've probably chosen a password that looks like this: 11Passw0rd! It's got all of the "secure" elements, but the numbers are at the front, the zero replaces the "O," and the symbol is at the back. It's very common to use those elements in that order, which makes it easy for brute-force password-guessing software to reverse engineer even a relatively complex password—especially since it's based on a word from the dictionary.

Second of all, a lot of websites do password security... poorly. For example, we used MD5 as an example hash. MD5 has been nearly obsolete since about the 1990s, and takes seconds to crack—but a lot of companies use it anyway. There's actually a sizeable contingent of companies which store passwords in plain text. You could be using the most secure password on Earth, and still get burned by malfeasance.

If even "secure" passwords fail the sniff test, how should you protect your data? Establish fail-safes. A strong password on its own is no defense against malware, ransomware, or any of the other numerous ways that attackers can hack your systems. Choose a strong passwords, and choose to educate yourself about the importance of combatting insider threats with this whitepaper on Shadow IT and Security Information.

Like this article? Follow us on LinkedIn, Twitter, YouTube or Facebook to see the content we post.

Read more about Cyber Security

- Popcorn Time: Would You Infect Others To Avoid Paying A Ransom?
- Our Take: SentinelOne's 2022 MITRE ATT&CK Evaluation Results
- Why Your Operating System Isn't Your Cybersecurity Friend
- SentinelOne's Cybersecurity Predictions 2022: What's Next?
- 12 Months of Fighting Cybercrime & Defending Enterprises | SentinelLabs 2021 Review
- 22 Cybersecurity Twitter Accounts You Should Follow in 2022