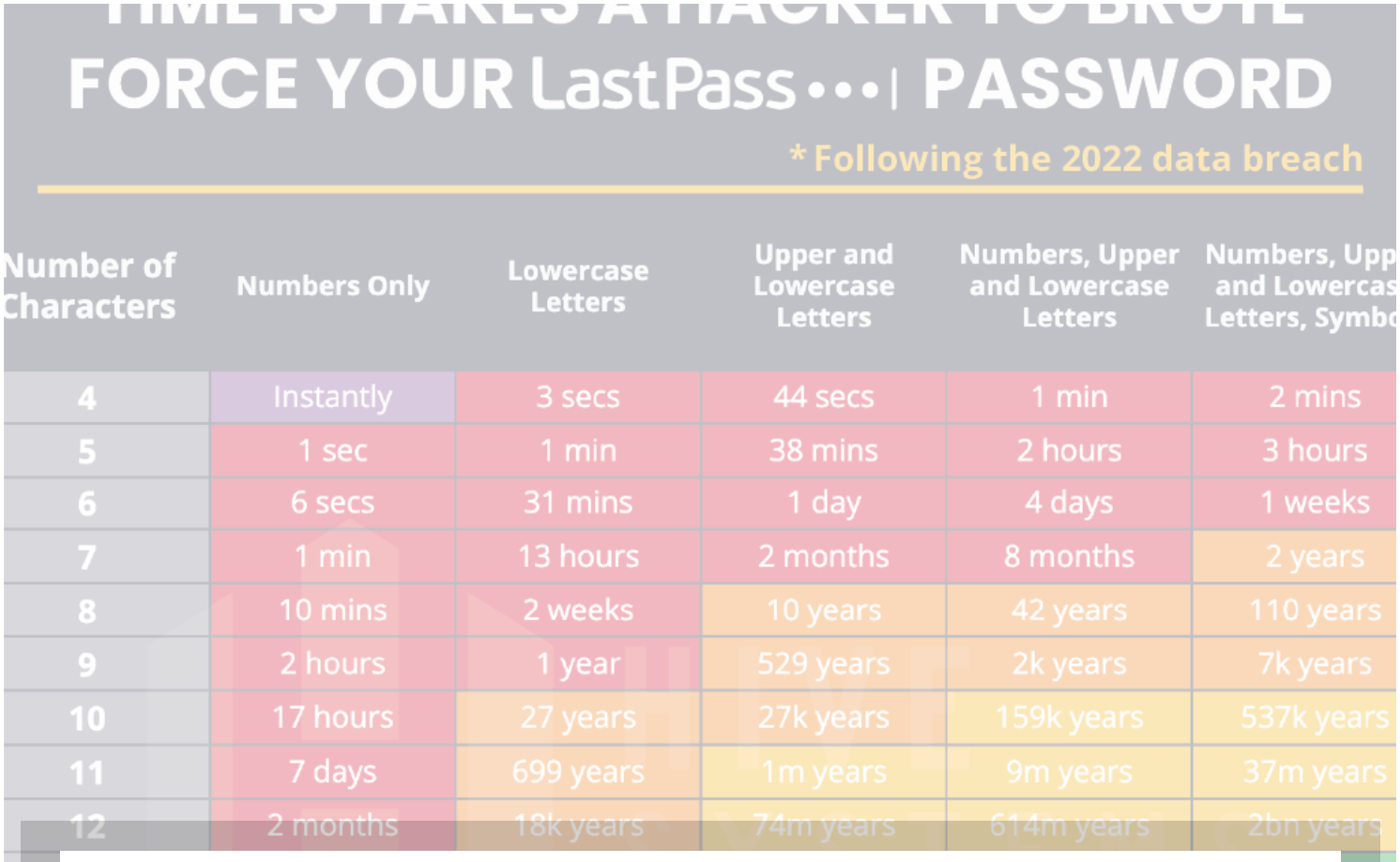

Examining the LastPass Breach Through our Password Table

Infographic | Awareness | Cybersecurity Fundamentals | News | Research

Sep 13 | Written By Corey Neskey

5 min read

Back in November 2022 you may have heard that the password manager company LastPass disclosed a breach in which hackers had stolen password vaults containing data for more than 25 million users. Most people assumed that while not ideal, many of the stolen passwords would never be cracked as they

Follow us – stay ahead.

But not so fast my friend - it's more complex than that. And with the recent string of crypto wallet heists, it appears that some of these passwords may be starting to get cracked. So how is this possible?

Looking for the 2023 Hive Systems Password Table?

SEE IT HERE!

One of the frequent comments we see on our famous Password Table is that it uses an older algorithm to calculate the cracking times (side note: cybersecurity researchers are STILL seeing password breaches that use the MD5 algorithm so unfortunately accurate). In this case though, LastPass very publicly notes they use PBKDF2 with SHA-256. However the number of iterations varies on when and how you used LastPass which can impact the cracking times. That being said, it's not that far-fetched that passwords are being broken - even randomly generated ones created in LastPass.

"I'm a LastPass user. How could we figure out my risk?"

Well let's look at some assumptions first:

- Your password was stolen as part of the 2022 LastPass data breach.
- You did not change the default number of local (usually browser extension) iterations, 5,000

Read more of the ACT

Mar 1, 2024

Let's Talk About Cookies!

Cookies help enhance our browsing experience, but what are the risks? Learn more about how cookies work, what data they collect, and how you can protect your data from misuse.

Feb 23, 2024

Navigating the Dual Impact of AI in Cybersecurity

Artificial Intelligence (AI) is

encryption key instead of having to deal with your client-side authentication hash nor the server-side authentication hash. Something discovered by Wladimir Palant who has reported several major vulnerabilities in LastPass over the years.

- The LastPass extension used PBKDF2 with SHA-256, set to use 5,000 as the number of iterations (rounds) to turn your master password into your encryption key.
- Your LastPass master password was randomly generated.

If these are all true, then your personal Password Table would look like this:

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	1 sec	1 sec
5	Instantly	1 sec	19 secs	45 secs	1 min
6	Instantly	15 secs	16 mins	46 mins	2 hours
7	Instantly	7 mins	14 hours	2 days	5 days
8	5 secs	3 hours	4 weeks	4 months	11 months
9	49 secs	3 days	4 years	21 years	63 years
10	8 mins	3 months	225 years	1k years	4k years
11	1 hour	6 years	11k years	80k years	307k years
12	14 hours	148 years	607k years	5m years	21m years
13	6 days	3k years	31m years	311m years	1bn years
14	2 months	100k years	1bn years	19bn years	105bn years
15	2 years	2m years	85bn years	1tn years	7tn years
16	16 years	67m years	4tn years	74tn years	516tn years
17	156 years	1bn years	231tn years	4qd years	36qd years
18	1k years	45bn years	12qd years	284qd years	2qn years

Maximum time required to crack PBKDF2 with SHA-256 randomly generated passwords with 5,000 iterations using an RTX 4090 with 12 GPUs

"What if I didn't use a randomly generated password? Just asking for a friend..."

but it's also set to be the newest threat.

Feb 12, 2024

SOC 2 Made Simple

Are you tired of filling out lengthy vendor questionnaires and are looking to pursue an SOC 2 examination report instead? Discover some basic practices to secure your customers' data and pave the way for SOC 2 certification.

above, given the cheap hardware. If your password was part of a breach before or follows common human-made password patterns your table looks more like this:

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	Instantly	Instantly	Instantly
8	Instantly	Instantly	Instantly	Instantly	Instantly
9	Instantly	Instantly	Instantly	Instantly	Instantly
10	Instantly	Instantly	Instantly	Instantly	Instantly
11	Instantly	Instantly	Instantly	Instantly	Instantly
12	Instantly	Instantly	Instantly	Instantly	Instantly
13	Instantly	Instantly	Instantly	Instantly	Instantly
14	Instantly	Instantly	Instantly	Instantly	Instantly
15	Instantly	Instantly	Instantly	Instantly	Instantly
16	Instantly	Instantly	Instantly	Instantly	Instantly
17	Instantly	Instantly	Instantly	Instantly	Instantly
18	Instantly	Instantly	Instantly	Instantly	Instantly

Password Table if your password has been previously stolen, uses simple words, or if you reuse it between websites.

"What if I was super savvy and set the iterations to 600k back before the breach?"

Great cybersecurity awareness! So let's update the assumptions then and the table

- Your password was stolen as part of the 2022 LastPass data breach.
- You did change the default number of local (usually browser extension) iterations, to 600,000 (most people didn't and still haven't).
- The attackers were able to brute force your encryption_key instead of having to deal with

- The LastPass extension used PBKDF2 with SHA-256, set to use 600,000 as the number of iterations (rounds) to turn your master password into your encryption key.
- Your LastPass master password was randomly generated.

If these are all true, then your personal Password Table would look like this:

TIME IS TAKES A HACKER TO BRUTE FORCE YOUR LastPass ••• | PASSWORD

*Following the 2022 data breach

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	3 secs	44 secs	1 min	2 mins
5	1 sec	1 min	38 mins	2 hours	3 hours
6	6 secs	31 mins	1 day	4 days	1 weeks
7	1 min	13 hours	2 months	8 months	2 years
8	10 mins	2 weeks	10 years	42 years	110 years
9	2 hours	1 year	529 years	2k years	7k years
10	17 hours	27 years	27k years	159k years	537k years
11	7 days	699 years	1m years	9m years	37m years
12	2 months	18k years	74m years	614m years	2bn years
13	2 years	472k years	3bn years	38bn years	184bn years
14	19 years	12m years	201bn years	2tn years	12tn years
15	190 years	319m years	10tn years	146tn years	904tn years
16	1k years	8bn years	544tn years	9qd years	63qd years
17	19k years	215bn years	28qd years	562qd years	4qn years
18	190k years	5tn years	1qn years	34qn years	310qn years

HIVE SYSTEMS

Learn more about the math behind this table at hivesystems.io/lastpass

Maximum time required to crack PBKDF2 with SHA-256 randomly generated passwords AFTER you've set it to 600,000 iterations using an RTX 4090 with 12 GPUs

"Well that's not great. What should I do now?"

If you are a LastPass customer (either for you/your family, or your organization), LastPass put out some

Want to learn more about our methodology for creating these Password Tables, our assumptions, limitations, and references? Then check out our full research piece here. Thank you, again @Chick3nman512 for providing benchmarks and explaining the nuances to us.

In the meantime, stay up to date with all of the latest cybersecurity news by subscribing to our ACT Digest or by subscribing to Hive Live to catch all our latest episodes about the world of cybersecurity.

Infographic | Awareness | Cybersecurity Fundamentals | News | Research

Corey Neskey

https://www.hivesystems.com/corey-neskey

Comments (0)

Most Liked

Preview POST COMMENT...