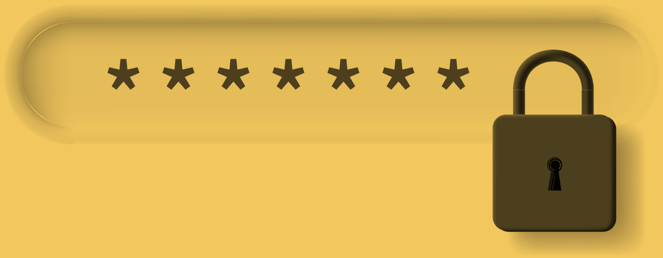
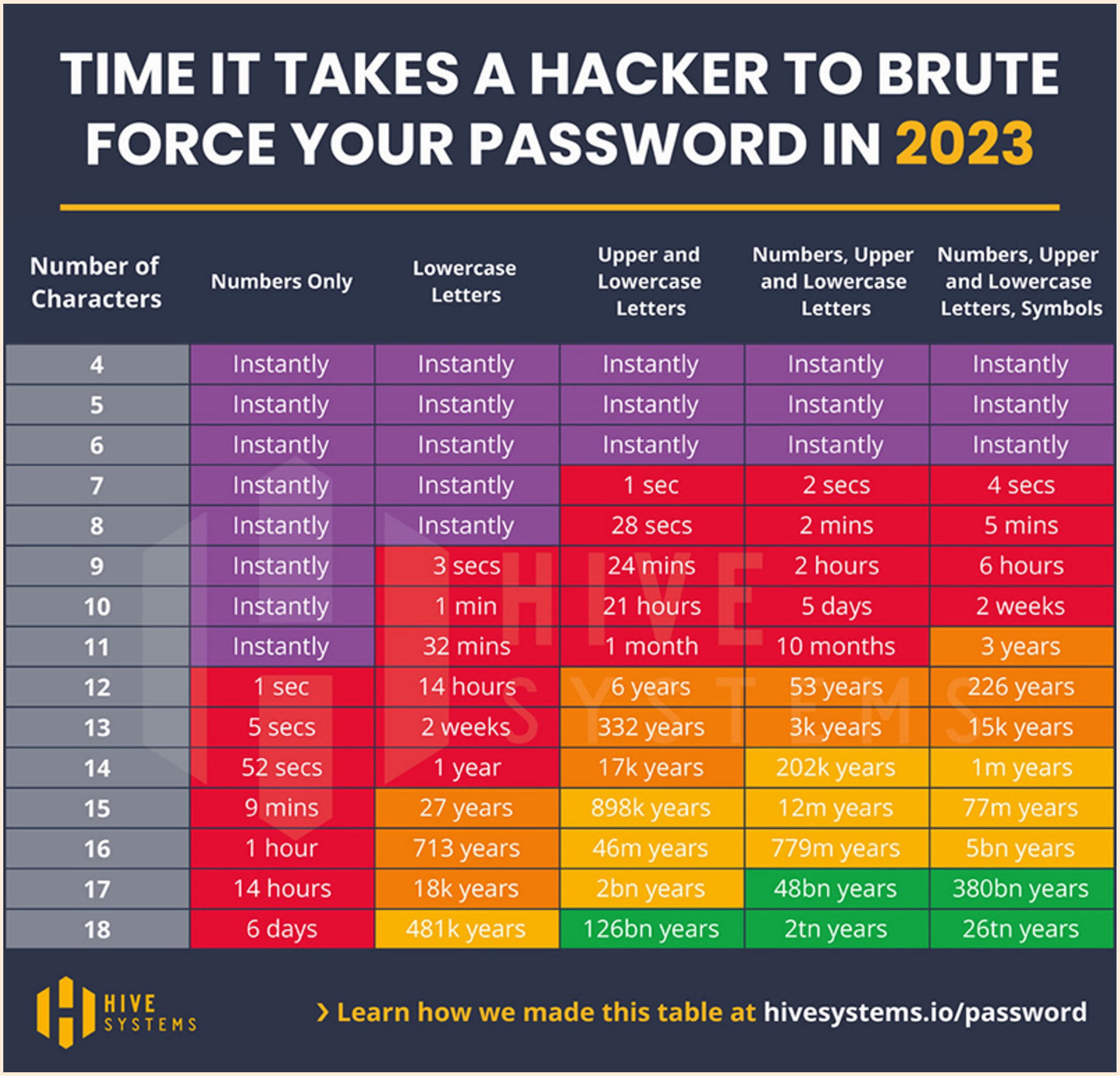
PASSWORDS



Did you know that in 2018 it would take 4 hours using a brute force[1] attack to crack an eight character password? Did you know that in 2023, it only takes a few minutes?



TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2023

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	1 sec	2 secs	4 secs
8	Instantly	Instantly	28 secs	2 mins	5 mins
9	Instantly	3 secs	24 mins	2 hours	6 hours
10	Instantly	1 min	21 hours	5 days	2 weeks
11	Instantly	32 mins	1 month	10 months	3 years
12	1 sec	14 hours	6 years	53 years	226 years
13	5 secs	2 weeks	332 years	3k years	15k years
14	52 secs	1 year	17k years	202k years	1m years
15	9 mins	27 years	898k years	12m years	77m years
16	1 hour	713 years	46m years	779m years	5bn years
17	14 hours	18k years	2bn years	48bn years	380bn years
18	6 days	481k years	126bn years	2tn years	26tn years

HIVE SYSTEMS

› Learn how we made this table at hivesystems.io/password

[1] A brute-force attack is one where a threat actor attempts as many password or passphrase combinations as possible until the correct one is found

PASSWORDS

So, when generating your own password, you should:

1 Focus on the password’s length as opposed to its intricacy. NIST recommends that User-generated passwords should be at least 12 characters.

2 Avoid passwords with consecutive characters (e.g., ‘1234’).

3 Avoid passwords with recurring characters (e.g.,’ rrrrr’).

4 Visit “breached password tracking websites,” such as “Have I Been Pwned” or “BreachAlarm” to check if your password has been exposed during a data security incident.

5 And, of course, create unique passwords for all accounts.

Certainly, with the seemingly infinite number of passwords individuals have these days, creating, let alone, using unique passwords for each account can be daunting. That is when a password generator may be helpful.

But, when relying on a password generator, you should:

1 Use a password manager. Because these passwords are not user-generated, they can be hard to remember. A password manager allows you to easily store such a password inside a password manager vault.

2 Use a password manager that allows you to “paste” the password generated password into the password manager. Pasting allows you to more easily input the password into a password manager, and hence makes it less likely you will write the password on a piece of paper.

3 Avoid password managers that allow recovery of the master password. Allowing recovery of the master password can lead to the compromise of the entire password vault.

Please visit our website for more practical cybersecurity tips to help you stay safe.