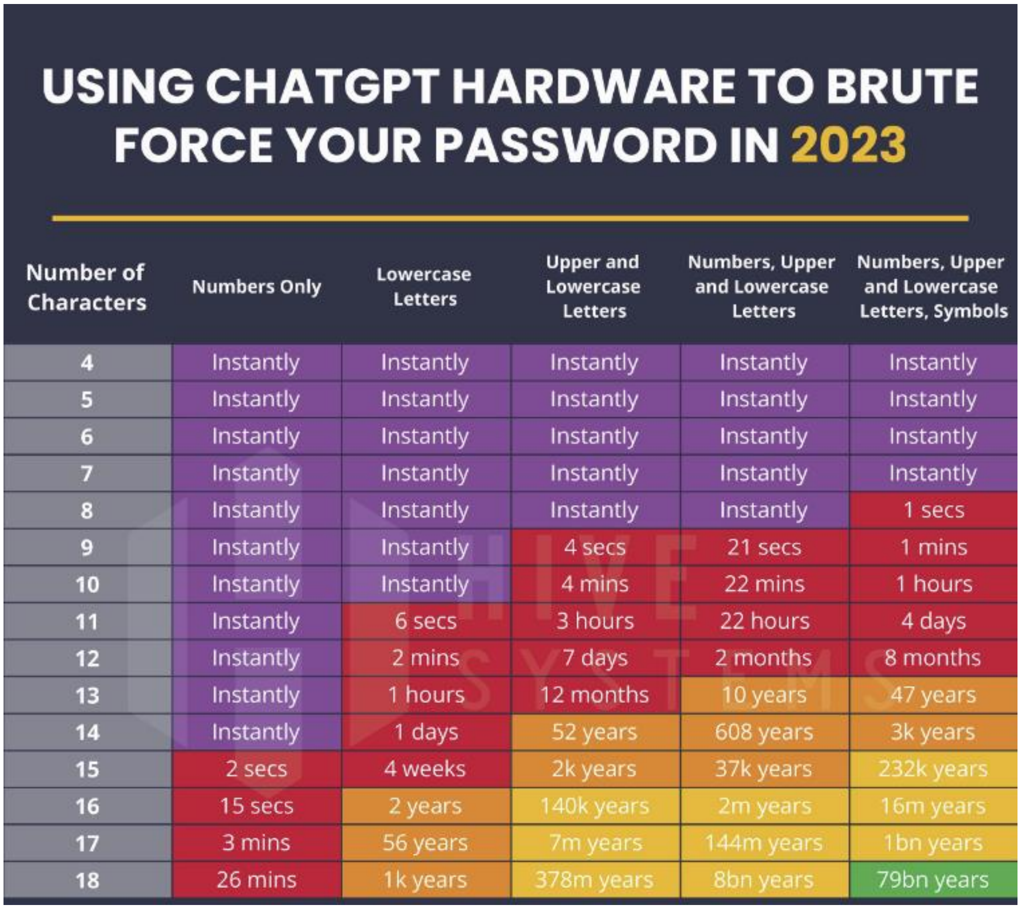
CSH Cold Spring Harbor Laboratory

Cybersecurity Management Office

Password123!

Cybercriminals often resort to guessing passwords, a tactic that remains effective due to common weaknesses in password creation and the infrequent updating of passwords. As we expand multi-factor authentication and other access management controls, attention should be given to passwords that are not in line with the Laboratory's policy. Even if you follow policy, your password may not be strong enough. For instance, if your password is a common phrase or easily guessable sequence like "password123" or "qwerty," it can still be compromised. ***A strong password will have 12 or more characters and can be more of a "passphrase" or a few unrelated words.*** Consider using a memorable phrase "it'saSmallwor1dafterall" or creating your own such as "th1swdBea$trongp@wd!" or "spo0kydistantActions?" (don't use these examples! 😉) to ensure your password is both strong and easy to remember.

How easily can a weak password be cracked by today's hackers? Very easily.



USING CHATGPT HARDWARE 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	Instantly	Instantly	Instantly
8	Instantly	Instantly	Instantly	Instantly	1 secs
9	Instantly	Instantly	4 secs	21 secs	1 mins
10	Instantly	Instantly	4 mins	22 mins	1 hours
11	Instantly	6 secs	3 hours	22 hours	4 days
12	Instantly	2 mins	7 days	2 months	8 months
13	Instantly	1 hours	12 months	10 years	47 years
14	Instantly	1 days	52 years	608 years	3k years
15	2 secs	4 weeks	2k years	37k years	232k years
16	15 secs	2 years	140k years	2m years	16m years
17	3 mins	56 years	7m years	144m years	1bn years
18	26 mins	1k years	378m years	8bn years	79bn years

Increased controls over access to Laboratory data are an emerging requirement of grant agencies. Password auditing helps us meet the new standard and will support our compliance by identifying weak passwords that may be vulnerable to cyber-attacks and brute-force cracking. Per the new requirements, password auditing will continue to be used periodically. Even if you believe your password is strong, the ongoing assessment will help us verify this and reinforce the required defenses. As always, we will work with users whose passwords are flagged as insufficient.

The Cybersecurity Team and Help Desk Team at CSHL are at your service to provide recommendations for stronger passwords in line with policy and the guidance provided in this newsletter.

For assistance with password creation or if you have any questions, don't hesitate to reach out to Cyber@cshl.edu!