How an 8 Character Password Could be Cracked in Just a Few Minutes

by Lance Whitney, techrepublic.com, in Security on August 7, 2023

Advances in graphics processing technology and AI have slashed the time needed to crack a password using brute force techniques, says Hive Systems.

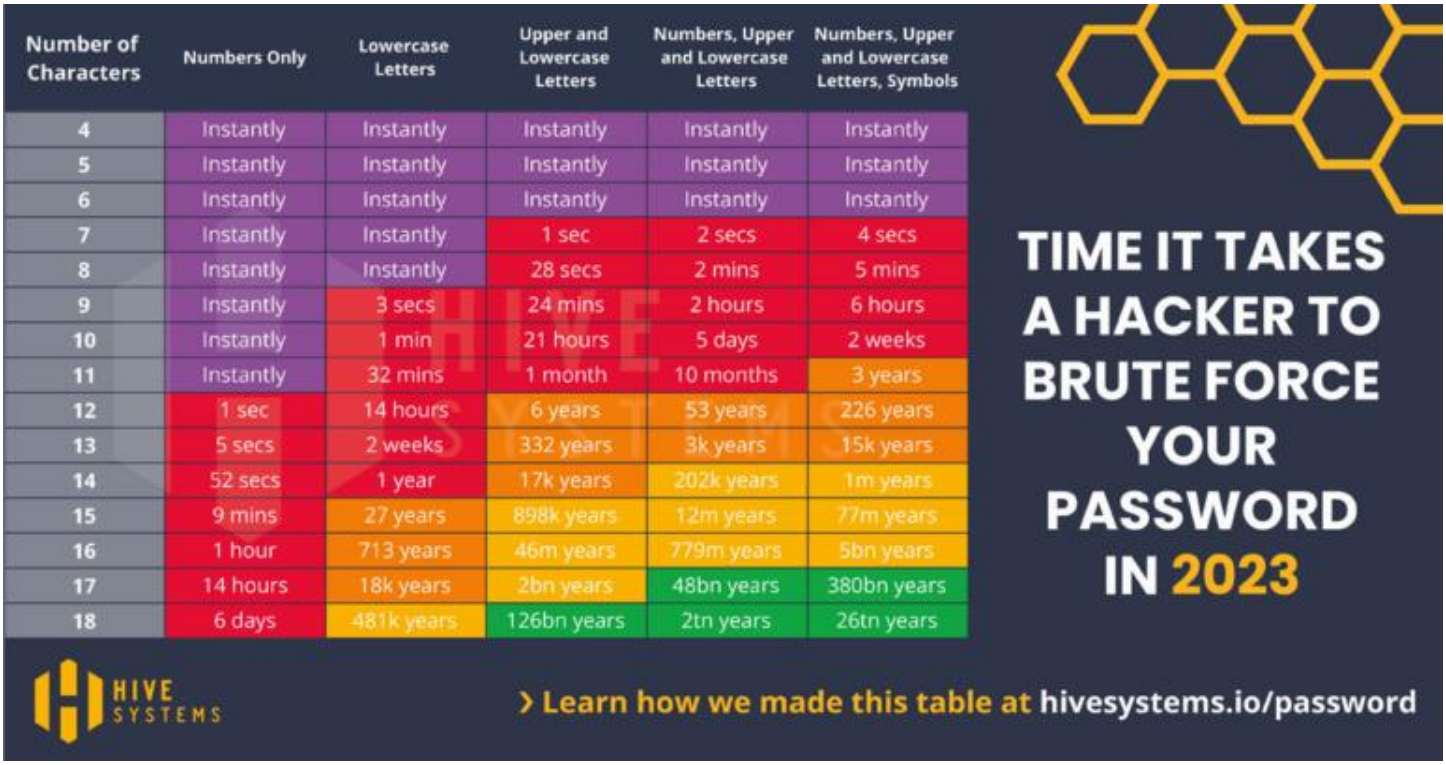
Security experts keep advising us to create strong and complex passwords to protect our online accounts and data from savvy cybercriminals. And "complex" typically means using lowercase and uppercase characters, numbers, and even special symbols. But, complexity by itself can still open your password to cracking if it doesn't contain enough characters, according to research by security firm Hive Systems.

How long does it take to crack a password?

As described in a report from April 2023, Hive found that an 8-character complex password could be cracked in only five minutes if the attacker was to take advantage of the latest graphics processing technology and artificial intelligence. Further, a seven-character complex password could be cracked in 4 seconds, while one with six or fewer characters could be cracked instantly. Shorter passwords with only one or two character types, such as only numbers or lowercase letters, or only numbers and letters, could also be cracked in an instant.

On the plus side, even simpler passwords with a greater number of characters are less vulnerable to cracking in a short amount of time, according to Hive's research. An 18-character password with only numbers would require six days to crack, but one with the same number of characters using lowercase letters would take 481,000 years to crack (**Figure A**). This piece of data shows why passphrases, which use a long string of real but random words, can be more secure than a complex but short password.

Figure A



Hive's report shows that passphrases with a mix of 18 uppercase and lowercase letters, numbers, and symbols are the most difficult to brute force. Image: Hive Systems

What tools do hackers use to crack your passwords?

A hacker aiming to crack complex yet short passwords quickly enough would need the latest and most advanced graphics processing technology. The more powerful the graphics processing unit, the faster it can perform such tasks as mining cryptocurrencies and cracking passwords.
For example, one of the top GPUs around today is Nvidia's GeForce RTX 4090, a product that starts at $1,599. But even less powerful and less expensive GPUs can crack passwords of a small length and low complexity in a relatively short amount of time.
Hackers who don't have the latest and greatest graphics processing on their computers can easily turn to the cloud, according to Hive. By renting computer and graphics hardware through Amazon AWS and other cloud providers, a cybercriminal can tap into multiple virtual instances of a powerful GPU to perform password cracking at a fairly low cost.
Plus, the advances in AI have given hackers another type of tool to crack passwords more quickly and efficiently. An April 2023 report from Home Security Heroes that analyzed 15,600,000 common passwords discovered that by using AI, hackers could crack 81% of them in less than a month, 71% in less than a day, 65% in less than an hour and 51% in less than a minute.

How to protect yourself and your organization from password cracking

Due to the progress in graphics and AI technology, most types of passwords require less time to crack than they did only two years ago. For example, a seven-character password with letters, numbers and symbols would take 7 minutes to crack in 2020 but only 4 seconds in 2023. Given these advances in technology, how can you and your organization better secure your password-protected accounts and data? Here are a few tips.

Use a passphrase instead of a password

A passphrase is a long string of often random words. Passphrases are often more secure than passwords and are usually easier to remember. For example: "sunset-beach-sand" uses words and a dash to separate each word and would take 2 billion years to crack, according to Security.org.

Use a password manager

Since creating and remembering multiple complex and lengthy passwords on your own is impossible, a password manager is your best bet. By using a password manager for yourself or within your organization, you can generate, store and apply strong passwords for websites and online accounts.

Use a strong master password

If you do adopt a password manager, you'll want to protect your stored passwords as effectively as possible. The way to do that is through a strong master password. Create a complex and long password or passphrase you can remember.

Test your passwords

To gauge the strength of a potential password, enter it at a site such as Security.org. The site will tell you how long it would take to crack that password.