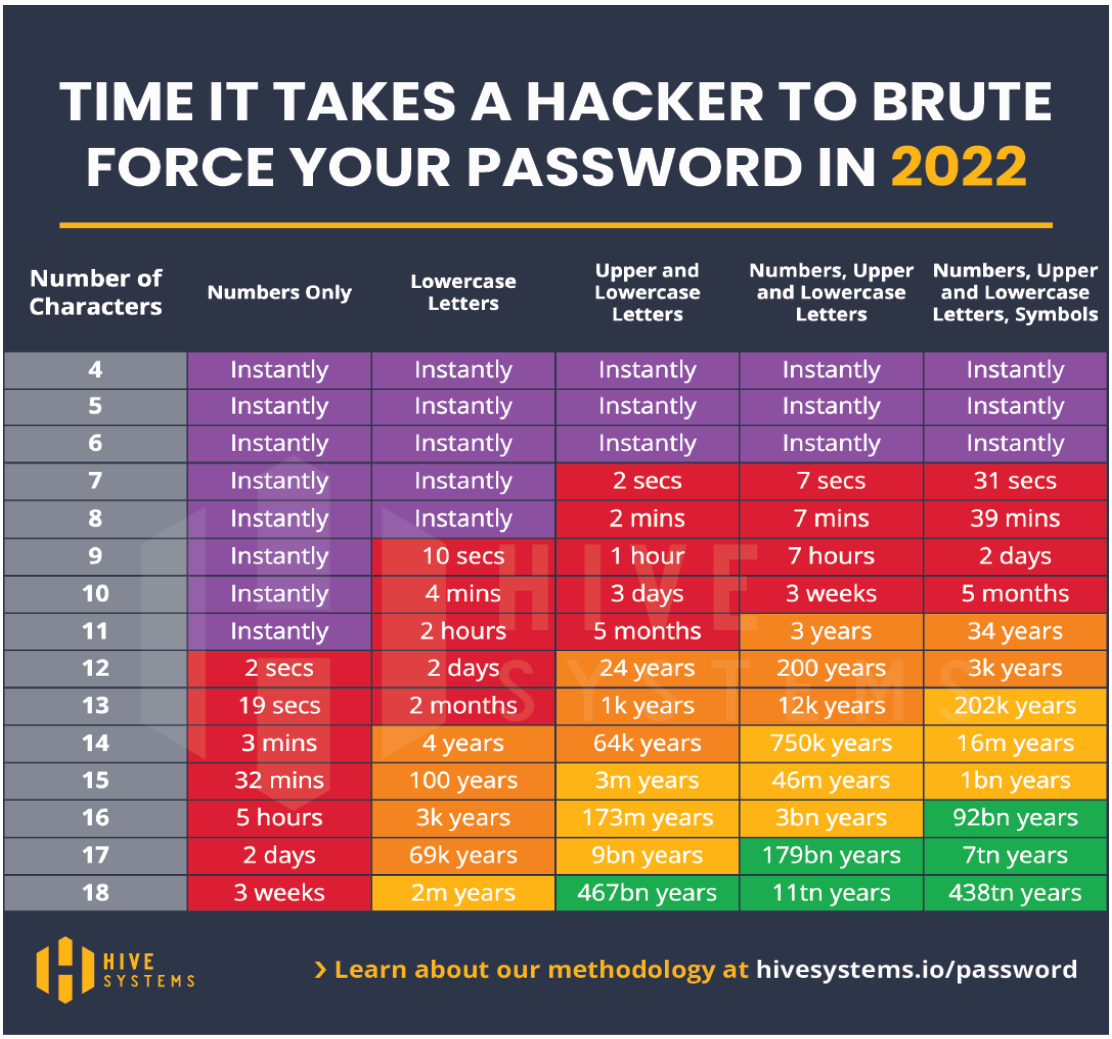
Secure Passwords

A very simple but often overlooked element that can help your security is password security. Often commonly used passwords will be guessed by malicious actors in the hope of gaining access to your accounts. Using simple passwords or having recognizable password patterns can make it simple for cyber-criminals to access a large range of accounts. Once this information is stolen it can be made public or sold for profit on the deep web.

Implementing randomized passwords can make it much more difficult for malicious actors to gain access to a range of accounts. Other steps, such as two-factor authentication, provide extra layers of security that protect the integrity of the account. Here are some suggested Dos and Don'ts for passwords:

- **DO** use a combination of uppercase and lowercase letters, symbols, and numbers.
- **DON'T** use commonly used passwords such as 123456, the word "password," "111111", or a word like, "monkey".
- **DON'T** use a solitary word in any language. Hackers have dictionary- based systems to crack these types of passwords. If you insist on using a word, misspell it as much as possible, or insert numbers for letters.
- **DON'T** use a derivative of your name, the name of a family member, or the name of a pet. In addition to names, do not use phone numbers, addresses, birthdays, or Social Security numbers.
- **DON'T** use the same password across multiple websites. If remembering multiple passwords is an issue, you can use a password manager to securely store your passwords.
- **DO** use abbreviated phrases for passwords. You can choose a phrase such as "I want to go to England." You can convert this phrase to an abbreviation by using the first letters of each word and changing the word "to" to a number "2." This will result in the following basic password phrase: iw2g2e. Make it even more complex by adding punctuation, spaces, or symbols: %iw2g2e!@
- **DON'T** write your passwords down, share them with anyone, or let anyone see you log into devices or websites.
- **DO** change your passwords regularly.
- **DO** log out of websites and devices when you are finished using them.
- **DON'T** answer "yes" when prompted to save your password to a particular computer's browser. Instead, rely on a strong password committed to memory or stored in a dependable password management program.



TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2022

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	2 secs	7 secs	31 secs
8	Instantly	Instantly	2 mins	7 mins	39 mins
9	Instantly	10 secs	1 hour	7 hours	2 days
10	Instantly	4 mins	3 days	3 weeks	5 months
11	Instantly	2 hours	5 months	3 years	34 years
12	2 secs	2 days	24 years	200 years	3k years
13	19 secs	2 months	1k years	12k years	202k years
14	3 mins	4 years	64k years	750k years	16m years
15	32 mins	100 years	3m years	46m years	1bn years
16	5 hours	3k years	173m years	3bn years	92bn years
17	2 days	69k years	9bn years	179bn years	7tn years
18	3 weeks	2m years	467bn years	11tn years	438tn years

HIVE SYSTEMS

› Learn about our methodology at hivesystems.io/password

Physical Security

If you're one of those people who leave their passwords on sticky notes on their desk, you may want to throw them away. Though many attacks are likely to happen through digital mediums, keeping sensitive physical documents secured is vital to the integrity of your company's security system.

Simple awareness of the risks of leaving documents, unattended computers and passwords around the office space or home can reduce the security risk. By implementing a 'clean-desk' policy, the threat of unattended documents being stolen or copied can be significantly reduced.

Password tips and tricks were created by Plumas County IT Dept. Graphic from Hive Systems.