Complex Passwords

In an ongoing commitment to bolster your digital defenses, let's focus on a powerful tool: complex passwords. Often times, applying a simple but innovative approach – using pass-phrases rather than passwords – can be an easy way to greatly enhance data security.

Pass-phrases are memorable strings of words that offer superior complexity. As displayed by the graphic below, this heightened complexity significantly raises the time needed to crack your password from brute force attacks by a bad actor. This is why we want long, but easy to remember passwords!

A good passphrase should be lengthy, use a mix of upper and lower-case letters, include numbers and special characters, and ideally, be unrelated words or phrases. It should also be easy for you to remember but hard for others to guess. Examples for a good passphrase password could be something like IDrinkCoffee@7:30 or Lose5Poundsin0924!

Remember, make a long password and easy to remember so it isn't necessary to write it down.

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lower Case Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	1 sec	5 secs
7	Instantly	Instantly	25 secs	1 min	6 mins
8	Instantly	5 secs	22 mins	1 hour	8 hours
9	Instantly	2 mins	19 hours	3 days	3 weeks
10	Instantly	58 mins	1 month	7 months	5 years
11	2 secs	1 day	5 years	41 years	400 years
12	25 secs	3 weeks	300 years	2k years	34k years
13	4 mins	1 year	16k years	100k years	2m years
14	41 mins	51 years	800k years	9m years	200m years
15	6 hours	1k years	43m years	600m years	15bn years
16	2 days	34k years	2bn years	37bn years	1tn years
17	4 weeks	800k years	100bn years	2tn years	93tn years
18	9 months	23m years	6tn years	100tn years	7qd years