1985 called. They want their passwords back!

Sat, 10/01/2022 - 11:11

|

Rob Tompkins, CISSP, Lead Cybersecurity Engineer, Tulane IT Information Security Team

View PDF

Passwords, love them or hate them, are here for a while.

We deal with them in almost every facet of our lives, and they just keep getting longer. I am not going to disagree that it's annoying, but I am here to convince you that it’s important. Putting it mildly, bad passwords are bad for business (A lesson learned from the 2019 SolarWinds incident).

Most organizations require an eight to nine-character minimum password. **However, those credit card companies you give your account information to only require seven-character passwords, and today that takes just 31 seconds to crack!**

But why on earth would you still use passwords with only seven characters? Those companies must follow a standard called PCI DSS, which STILL recommends a minimum seven-character password. If this illustrates anything, it is that the minimum is not enough.

So, I dug further into password requirements thinking there must be a strong recommendation from one of today’s industry leaders…right? NO!

The recommendation was originally suggested in the 1985 Department of Defense Password Management Guideline…seriously!

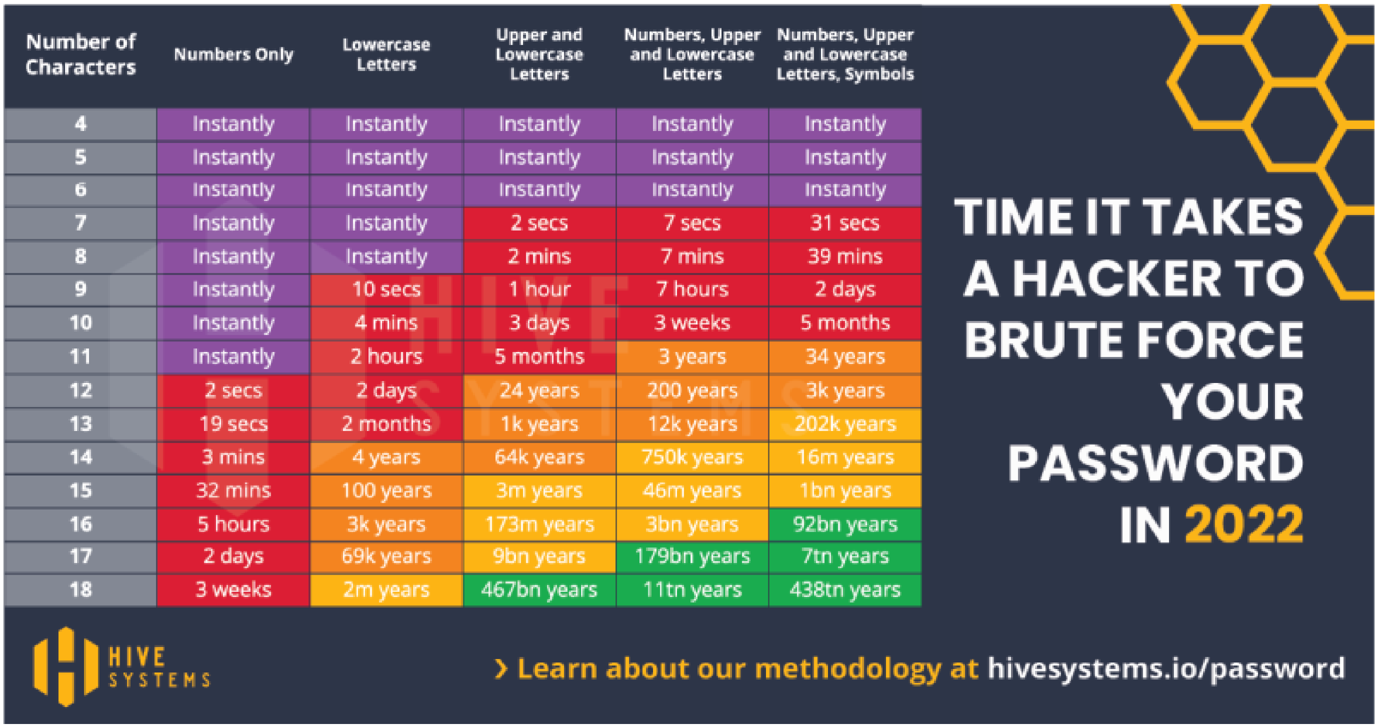
Acoustic coupler modem with analogue phone for 300 baud dial-up internet

Back in the 80s, an eight-character password with letters and numbers could withstand six months of attack over a 300-baud modem, but that’s when we used ridiculously slow modems and connections. Today's network speed is infinitely better…yet our security is not.

That, my friend, is a problem.

Because computer technology advances so quickly, the time it takes to crack a password is constantly getting shorter. **Now an eight-character password can be cracked in 39 minutes** according to HiveSystems' 2022 infographic Are Your Passwords in the Green.

My recommendation? Use the longest password you can just to avoid being cracked!



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

SolarWinds 2019 Password Hack

Earlier, I mentioned SolarWinds, a very popular IT management platform with customers in many different industries. They were attacked in 2019 and an estimated 18,000 of their customer’s organizations were compromised. You're probably wondering, "how does a well-known IT software development company get compromised?"

Well, a security researcher discovered a weak default password (solarwinds123) for their file transfer protocol (FTP) server, and warned the company that "any hacker could upload malicious [code]" and distribute it to their customers. The New York Times reported the company did not employ a chief information security officer and that employee passwords had been posted on GitHub in 2019.

Here's a brief overview from Wikipedia:

"*APT29, aka Cozy Bear, working for the Russian Foreign Intelligence Service (SVR), was reported to be behind the 2020 attack. Victims of this attack include the cybersecurity firm FireEye, the US Treasury Department, the US Department of*

Commerce's National Telecommunications and Information Administration, as well as the US Department of Homeland Security. Prominent international SolarWinds customers investigating whether they were impacted include the North Atlantic Treaty Organization (NATO), the European Parliament, UK Government Communications Headquarters, the UK Ministry of Defence, the UK National Health Service (NHS), the UK Home Office, and AstraZeneca. FireEye reported the hackers inserted 'malicious code into legitimate software updates for the Orion software that allow an attacker remote access into the victim's environment' and that they have found 'indications of compromise dating back to the spring of 2020...''

What's the biggest lesson learned from this major breach? Don't use simple passwords like "solarwinds123"!

QUICK PASSWORD TIPS

- Create long passwords or passphrases
  preferably 12+ characters
- Use a unique password for every online account
- Find a password manager that meets your needs
- Never share your passwords with anyone

WORK SAFE,
PLAY SMART

As I said earlier, bad passwords are bad for business. The best are long random passphrases. Most of the time you can use spaces and write out a sentence with punctuation–something like "Every1 needs long passwords!" This 28-character passphrase with a combo of capitalization, letters, numbers, and symbols is easy to remember and would take trillions of years to crack (at least based on today's technology).

Aside from using passphrases here are some additional recommendations:

- **Longer is better.** Passwords or passphrases should be 12 characters or more, no matter the site’s requirements – e.g., “Every1needslongpasswords!”
- **Create a unique password for each account.** One stolen password can be leveraged to gain access to every single account. Using one password also increases your chances of becoming a victim of identity theft.

- **Use a password manager.** Instead of a notebook, sticky notes, or web browser, find a trustworthy password manager, so you only need to remember ONE password.
- **Passwords are personal.** Treat your passwords like your toothbrush. Don’t share them with anyone!

Passwords aren’t going anywhere, but we can’t stay stuck in the 1980s.

Let’s charge into the future with better security practices and help keep the Tulane community safe!