Cyber Security Snapshot

Exploring and Assessing Current Topics

MICHIGAN CYBER COMMAND CENTER (MC3)

May 31, 2019
CS-03-2019

Password Security

SplashData released their annual list of the top 100 worst passwords. This list utilized data from 5 million leaked passwords of users. Based on the results of their research, SplashData believes one of the top 25 worst passwords has been used by almost 10% of users. Nearly 3% are estimated to have used the worst password of “123456”. The top two worst passwords of 2018 used were “123456” and “password.”

When guessing passwords, hackers often try common terms from sports, pop culture, and easily guessable words. This is because they know many people use easy-to-remember words as their passwords. Additionally, when trying to guess passwords, hackers know to swap out letters for numbers, as users often take this step. While it does help fulfill some password requirements, it does not make a user’s password more secure. SplashData’s results help to show why many hackers are successful.

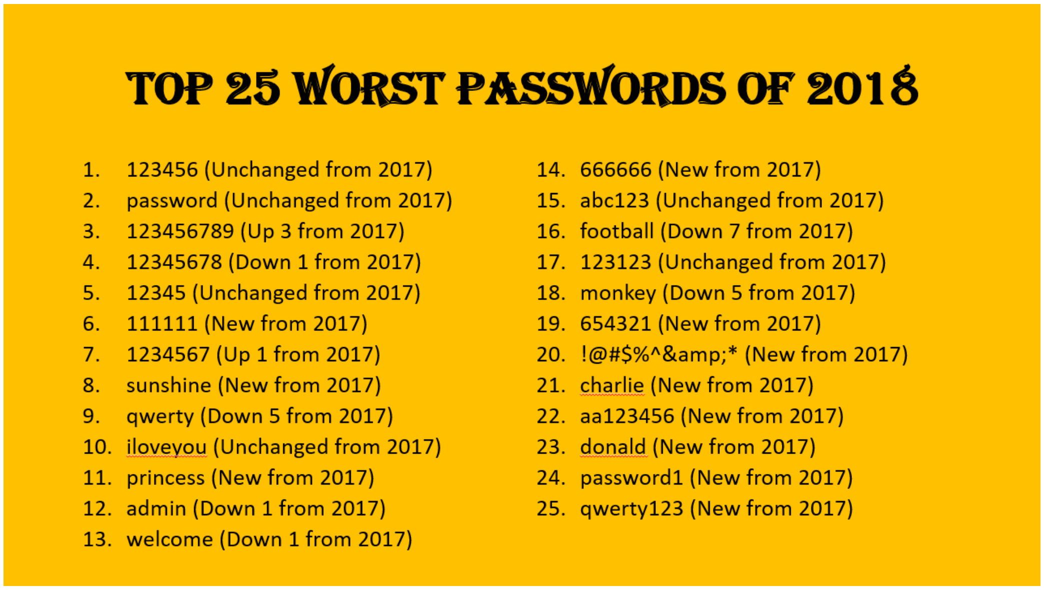
To help remain secure, experts suggest updating passwords frequently. It is not uncommon for organizations to require passwords be reset every 90 days. However, it is less common for individuals to take this step. Continually updating and using strong passwords is an important highly recommended step to help keep accounts secure. At a bare minimum, passwords should be reset upon notification of an unintended disclosure.

Strong passwords should:

- Avoid common phrases
- Be at least 15 characters long (the longer the password, the better)
- Contain special characters, upper case, lower case, and numbers
- Used only once (every account should have a different password)

Strong passwords should not be:

- Shared with others
- Reused (once a password is used, it is never used again)
- Use repetitive or sequential characters (Ex: ggggg. 789jkl)



Top 25 Worst Passwords of 2018

1. 123456 (Unchanged from 2017)
2. password (Unchanged from 2017)
3. 123456789 (Up 3 from 2017)
4. 12345678 (Down 1 from 2017)
5. 12345 (Unchanged from 2017)
6. 111111 (New from 2017)
7. 1234567 (Up 1 from 2017)
8. sunshine (New from 2017)
9. qwerty (Down 5 from 2017)
10. iloveyou (Unchanged from 2017)
11. princess (New from 2017)
12. admin (Down 1 from 2017)
13. welcome (Down 1 from 2017)
14. 666666 (New from 2017)
15. abc123 (Unchanged from 2017)
16. football (Down 7 from 2017)
17. 123123 (Unchanged from 2017)
18. monkey (Down 5 from 2017)
19. 654321 (New from 2017)
20. !@#$%^&amp;* (New from 2017)
21. charlie (New from 2017)
22. aa123456 (New from 2017)
23. donald (New from 2017)
24. password1 (New from 2017)
25. qwerty123 (New from 2017)

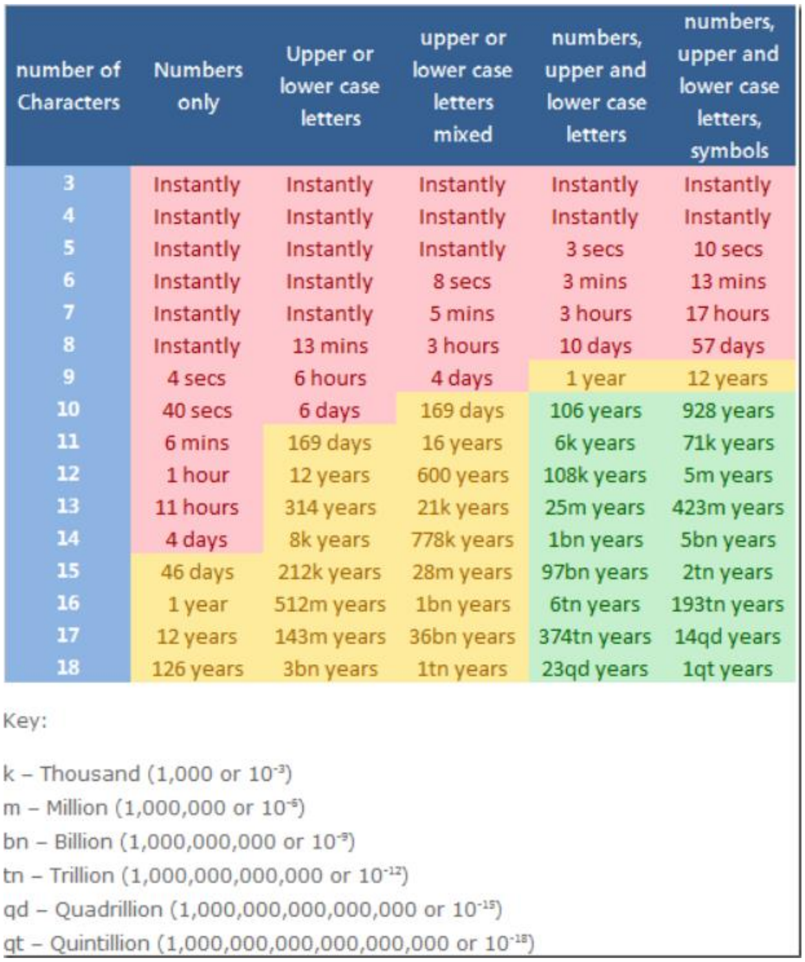
*This document is the property of the Michigan Cyber Command Center (MC3) and is prepared for the limited purpose of information sharing. This information is designated **UNCLASSIFIED**. Information found within this document can be shared without restriction. This document must not be reclassified in any way, in whole or in part. Violation of this restriction will be cause for removal from MC3 distribution lists.*

To help remember passwords, users could consider using password managers. Passwords can also be written down if they are secured in a private place only accessible to the user. Writing passwords down and utilizing password managers can be extremely helpful when managing numerous unique passwords.

To help improve password strength, security experts recommend utilizing passphrases. These are similar to passwords but are a sequence of words or other texts connected together to increase the password's length. This increased length makes it more difficult for hackers to guess.

If possible, users should utilize two factor authentication (also known as multifactor authentication). This type of authentication adds an extra layer of security as it requires a username, password, and a unique item only known to them. Often, this unique item comes in the form of a one-time security code is sent to the user via email, text message, or phone call.

Any additional questions or concerns can be sent to the Michigan Cyber Command Center (MC3) at mc3@michigan.gov or at 1-877-MI-CYBER



number of Characters	Numbers only	Upper or lower case letters	upper or lower case letters mixed	numbers, upper and lower case letters	numbers, upper and lower case letters, symbols
3	Instantly	Instantly	Instantly	Instantly	Instantly
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	3 secs	10 secs
6	Instantly	Instantly	8 secs	3 mins	13 mins
7	Instantly	Instantly	5 mins	3 hours	17 hours
8	Instantly	13 mins	3 hours	10 days	57 days
9	4 secs	6 hours	4 days	1 year	12 years
10	40 secs	6 days	169 days	106 years	928 years
11	6 mins	169 days	16 years	6k years	71k years
12	1 hour	12 years	600 years	108k years	5m years
13	11 hours	314 years	21k years	25m years	423m years
14	4 days	8k years	778k years	1bn years	5bn years
15	46 days	212k years	28m years	97bn years	2tn years
16	1 year	512m years	1bn years	6tn years	193tn years
17	12 years	143m years	36bn years	374tn years	14qd years
18	126 years	3bn years	1tn years	23qd years	1qt years

Key:

k – Thousand (1,000 or 10^{-3})
m – Million (1,000,000 or 10^{-6})
bn – Billion (1,000,000,000 or 10^{-9})
tn – Trillion (1,000,000,000,000 or 10^{-12})
qd – Quadrillion (1,000,000,000,000,000 or 10^{-15})
qt – Quintillion (1,000,000,000,000,000,000 or 10^{-18})

Time required to crack (i.e. guess) passwords is based on length, complexity, and computing power used.

This document is the property of the Michigan Cyber Command Center (MC3) and is prepared for the limited purpose of information sharing. This information is designated ***UNCLASSIFIED.*** *Information found within this document can be shared without restriction. This document must not be reclassified in any way, in whole or in part. Violation of this restriction will be cause for removal from MC3 distribution lists.*