Stronger Password Requirements

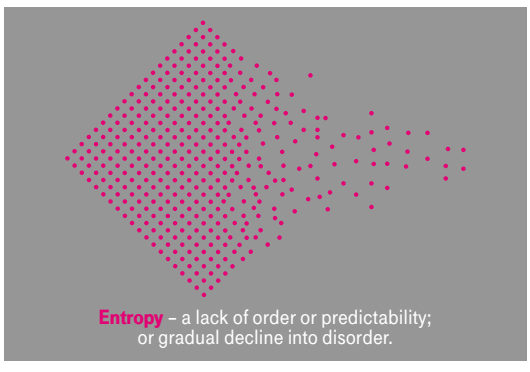
Making Our Stronger Password Requirements Easy

By now, you have likely seen the email and/or the T-Nation article regarding the new stronger password requirements. This Job Aid is designed to equip you with the information you need to create stronger passwords that are secure, and easy to create and remember.

What's Changing

Essentially, nothing is changing regarding the password requirements. What is changing is that this new system will provide an extra layer of protection by detecting and blocking weak passwords and their variants, as well as optionally blocking weak terms that are specific to our organization.

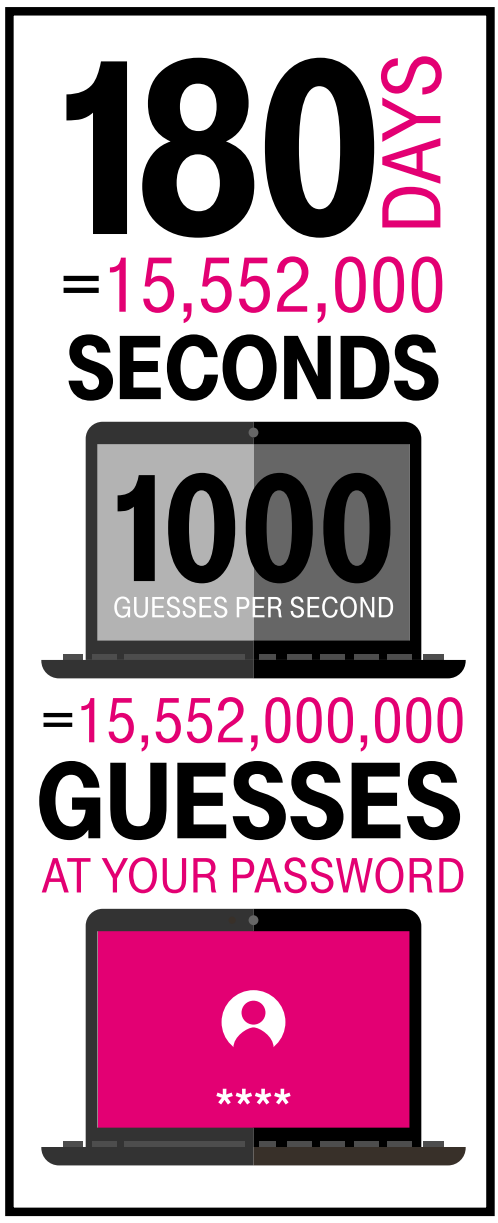
1. You cannot use the same password from the past twenty-four (24) passwords used.
2. These other requirements remain the same:
   - Must be a minimum of eight characters in length
   - Must meet at least three of these requirements:
     - o Contain at least one (1) lowercase letter
     - o Contain at least one (1) uppercase letter
     - o Contain at least one (1) number
     - o Contain at least one (1) symbol
     - o Can not contain any spaces



People vs. Computers

For more than twenty years, we were taught to create passwords that are hard for humans to remember, but easy for computers to guess. We learned to create strong passwords by **using common words** with random numbers or symbols in place of letters (i.e. **cR3at!nG**). These old tricks may fool a human, but they won't deter a computer from eventually figuring out your password. A computer program can and will guess your password—eventually.

The trick is to create a password that a computer won't guess within the 180 days you have before you are asked to create a new password. It's all about Entropy. This is a total mind-shift after years of being taught how "cR3at!nG" passwords with random numbers and symbols in place of letters was the most secure option.



Why Your Attempts to Change Your Password Might Fail Repeatedly

Our new password system will use tools such as banned password lists, fuzzy logic, and algorithms that make it challenging to create an acceptable password—even if you adhere to the requirements listed above. Here are some tips that will help:

DO:

REMEMBER that a successful password must have a minimum of eight (8) characters. Longer passwords are better than short passwords, but not required

Make your password difficult to guess, even by those who know a lot about you

Use the **Acronym Method** —Take an easy-to-remember phrase that means something to you

- Example: "My dog, Spartacus, always chews on his favorite toy!"
- Use the first letter of each word: mdsacohft
- Add capital letters: MdSacohft
- Insert punctuation: MdSacohft!
- Throw in a random number that means something to you (but not birthdays or anniversaries): **MdSacohft!1520**

Why this works:

- It's not a common word, and thus more difficult for a computer to guess
- It's 14 characters long; exponentially more challenging to hack over an eight-character password
- It adheres to the minimum of eight characters requirement
- It's as good as any randomly generated password from a password manager
- I WILL EASILY REMEMBER THIS PASSWORD

DON'T:

DON'T use a Password Manager to store your NT account password. Ever.

DON'T re-use your password for non-work-related purposes

DON'T Use common words that are easily guessed and found in the dictionary.
DON'T Use any T-Mobile common words that are easily guessed: Magenta, AreYouWithUs, HowWePlay, etc.
DON'T Use any regional words that are easily guessed: Seattle, Bellevue, Seahawks, Mariners
DON'T Use your cool "formula" or pattern for your next password. "MyPa$$word2019" changed to "mYpassword2020" won't work anymore. It must be unique from your last 25 passwords.

Here are links to the email and T-Nation article that were published on July 24, 2019
If you are still having issues with your password, please call the Service Desk directly at (877) 878-7326.