Tips for Creating a Strong and Unique Password

Please use this document to help you as we transition to our new district password policy that requires a minimum length of 16 characters. The following tips are a compilation taken from the websites listed within this document. Please access these websites for additional tips and information.

Never use personal information: This includes names of family members, pets, birthdays, etc.

Make them random: There are two ways you can do this:

- Use a string of random mixed-case letters, numbers and symbols.
- Create a phrase of 5-7 unrelated words (called a passphrase). You can make this even stronger by getting creative with spelling and/or adding numbers/symbols.

Prioritize password length: Safe passwords are at least 16 characters long and decrease your chances of falling victim to a data breach or cyberattack.

Make them unique: Use a different strong password for each account.

Play with your keyboard:

- The password **1!qazsdrfgbhju8*** is really hard to remember unless you know it makes a 'W' on your keyboard! You can make letters, shapes and more just 'drawing' on the keyboard.

- Use commonly allowed symbols: ! " # $ % & ' ( ) * + , - . / : ; < > = ? [ ] \ ^ _ ` { } ~
- Use "emojis" in your password:

One last thing to keep in mind:

"Hackers regularly use dictionaries, passwords lists that sift through commonly used passwords, context-specific words (like company or service name), previously breached password lists, and hash tables to find patterns…" (NIST Password Guidelines 2024 | AuditBoard)

https://www.cisa.gov/secure-our-world/use-strong-passwords
https://www.webroot.com/us/en/resources/tips-articles/how-do-i-create-a-strong-password
https://us.norton.com/blog/privacy/password-security

Rationale

The increase in length and complexity is based on the NIST Digital Identity Guidelines (see website link below). Password cracking is still a common way for bad actors to infiltrate networks. A longer password is harder to crack (NIST is currently recommending a minimum of 16 characters). Having a longer and stronger password that needs to be reset less frequently, or not at all, decreases the likelihood of a bad actor cracking it. When people are expected to frequently change their password, they are more likely to reuse passwords with slight modifications making them more vulnerable to security breaches. (https://www.auditboard.com/blog/nist-password-guidelines/)