san diego county office of EDUCATION
FUTURE WITHOUT BOUNDARIES℠

INTEGRATED TECHNOLOGY SERVICES

10 Commandments of Password Management

Your first and sometimes only line of defense is your password. However, even the most carefully crafted passwords can be rendered useless if they are not kept secret. This is not such an easy thing to do, especially considering all the clever tricks cyber criminals use. Every other day it seems another organization reports being hacked, resulting in millions of accounts being compromised. Here are 10 ways to create and secure all of your passwords.

1. **Use strong and unique Passwords or Passphrases.**
   Always refer to your organization or District policy. However, the latest best practices identify passwords which should be at least 16 characters, and contain a combination of numbers, symbols, uppercase letters, lowercase letters, and spaces. The password should be free of repetition, dictionary words, usernames, pronouns, IDs, and any other predefined number or letter sequences.
   Password should also be unique for every website or service used. The logic is simple: if you recycle the same password, and a hacker cracks one account, they will be able to access the rest of your accounts.

2. **Devise a password-creating system that is unique to you.**
   There are dozens, hundreds, maybe even thousands of webpages and other resources offering advice on how to craft strong passwords. Of course, these are the first places the people in the business of cracking passwords look for tips. It's not difficult to come up with your own system that combines a variety of methods. creating a system that both allows you to create complex passwords and remember them. For example, create a phrase like "I hope the Padres will win the World Series in 2024!" Then, take the initials of each word and all numbers and symbols to create your password. So, that phrase would result in this: IhtPwwtWSi2024!

3. **Don't write it down. Ever.**
   Either it will be so easy to find that you might as well not use any password at all, or you'll forget where you put it and somebody else will find it and use it to access your accounts.

4. **Disable AutoComplete for user names and passwords.**
   Yes, this feature of Chrome, Firefox, and other browsers can save you time when you're online, but it also allows anyone who gains access to your system to visit all the secured sites in its database, change the passwords, and otherwise act in ways you may not appreciate.

5. **Don't send your password via e-mail or give it out over the phone.**
   Never send sensitive or private data using email as it should not be considered a secure manner to communication. Additionally, your assistant, designee and even your organization's help-desk staff should not know your password. If you are concerned your password has been compromised, change it.

6. **Change your passwords often.**
   Even if you haven't shared it recently (as mentioned above), get into the habit of refreshing stale passwords. The more important the data your password protects, the more often you should update it.

7. **Don’t enter passwords using public Wi-Fi.**
   If you don’t want a hacker to pick up your password, don’t access websites that require you to enter a username or password while using public wireless internet. If you need to access sensitive information remotely, use a Virtual Private Network (VPN) connection.

8. **Clear the cache after using a public computer.**
   If you must use a public computer make sure you wipe out all traces of your use by deleting the browser's personal data.

9. **Enable two-step verification.**
   Any time a service such as Microsoft or Gmail offers "two-step verification," use it. When enabled, signing in will require you to also enter in a code that's sent as a text message to your phone. Meaning, a hacker who isn't in possession of your phone won't be able to sign in, even if they know your password.

10. **Ask for some help to reset your password.** If you've forgotten your password and don't have a password-reset disk handy, contact your account administrator to have your password reset and change the password. When asked for answers to security questions, make sure to provide answers that only you would know and that someone couldn’t easily find out about you by looking on the internet. For example, don’t use your dog’s name as a password reset question if there are pictures of your pooch all over Facebook.