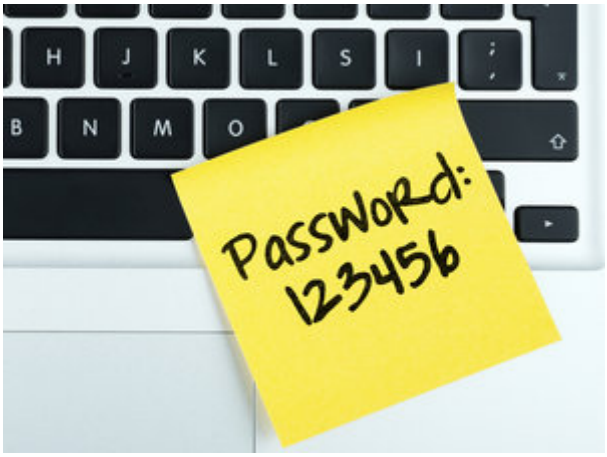
Common Sense Password Practices



With all the online hacks and security breaches going on these days, I would like to share a few pointers on what goes into a good strong password.

- Complexity: In general I recommend a password that is at least 8 characters, contains a number, an uppercase letter, and a special character such as ! or @ if allowed. Although common words and names are easy to remember, you want to avoid these and go with a sequence of characters that are more random and obscure. If you insist on using common words and names for memorability, try replacing letters in the word or name with numbers or special symbols. For example, you could take the word list and turn it into 1i$t.

- Uniqueness: Use a different password for each account you create, that way if one of your accounts ever becomes compromised the hacker will only have access to that one account.

- Use two-factor authentication: Two-factor authentication adds another layer of security to an account by requiring something you have (your cellphone

etc.) in addition to something you know (your password). Many sites offer this feature now and can be configured for example to require that you enter a code sent to your cellphone when signing in on a new or different computer. This way, if your password gets compromised, the hacker still will not be able to sign in as you on their computer (unless they have possession of your cellphone too!). For convenience sake, you can choose not to require two-factor authentication on your own personal computer(s) going forward after the initial verification.

- Use a password manager: If keeping track of a unique password for every online account is too daunting as task, consider using an online password manager that keeps all your login credentials in a secure encrypted vault that is accessible with a master password. Although making all of your passwords accessible by one master password defeats the uniqueness principle above, some password management services have gone to great lengths to make this method as safe as possible while providing the convenience of only needing to remember one master password. One such password manager that is highly regarded by security experts is LastPass, which supports two-factor authentication.
- Periodically change your password: As passwords can become lost or stolen over time, it is good to periodically change them. Stanford University recommends that passwords be changed every six months or so for good measure.

~Ted Eiler