Password Protection Standard

User Education –

1. Educate you and your staff on what is and isn't a good password. As IT professionals, most of the time we take for granted what we know. We go on with our busy days believing others already know it and the reality is that most people really don't understand how to properly create passwords and the importance of following simple standards. Users only see the end result and that is gaining access to their accounts. You should schedule 15 minutes every quarter to send out an email, or better yet, hold a small class that covers the importance of good password creation and management.

2. During your talk you should teach the users how to create a strong password and why it is considered a strong password. Teach them the practice of using phrases when possible. "The yellow ball is bouncing" is a considerably stronger password and much easier to remember than a keyboard smash of characters dont45$hTnflyiw0*%.

Below are some items to point out to users about password creation:

- Please do **NOT** use your name, or pet's names or family members
- Please do **NOT** use your Social Security Number, Birth Date, Address, Phone Number, etc.
- Please do **NOT** use any information that would be easily associated to them
- Please do **NOT** use any password on more than one site
- Please use at least 12 characters for a password
- Please use a space if allowed
- And if possible, try and create long phrases

Teach end-users that rather than remembering passwords for every site and or account, to use a password management service like one of the following:

- LastPass – online
- 1Password – online
- DashLane – online
- KeyPass – Local application
- PasswordSafe – Local application

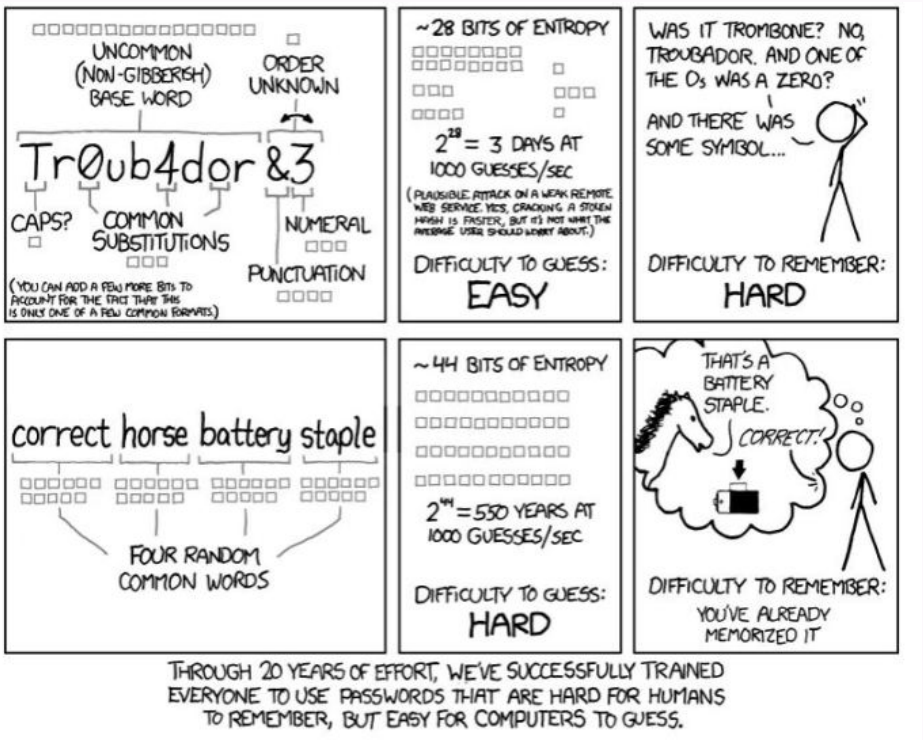
In short, these are all third-party services that allow a user to save all their passwords in one location and secure them with one master password.

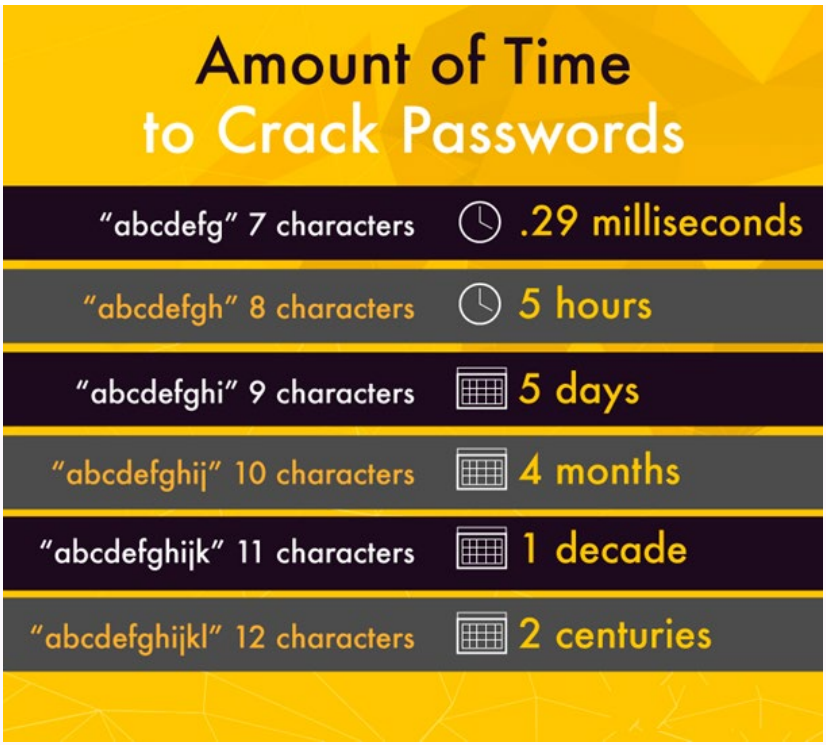
4. If and when possible, run 2FA (Two-Factor Authentication). This will greatly increase the security of the end-user account. Instruct end-users to enable and run 2FA on any of the websites that they use on a normal basis. The website **https://twofactorauth.org/** is a great resource for discovering which websites currently offer 2FA.

Password Management –

1. If you haven't already, now would be an appropriate time to move forward with putting in some password enforcement rules on your User Management platform (EX. Active Directory). Force users to do the following:
    1. Password Length at least 12 Characters long
    2. Uppercase, lowercase, numerical and character requirements
    3. Force Maximum Password Age
        - Set this to 60 or 90 days. This can be shorter if you like but, the shorter the requirement typically the weaker the passwords users create. They don't want to constantly be remembering and changing passwords.
    4. Force Minimum Password Age
        - Set this to 30 days. This will keep users from just resetting their password right back to what it was prior.
    5. Enforce Password Re-use History
        - Set this to a value of 4 or higher. This will force the user to keep cycling their passwords for the entire year.

This **popular xkcd comic** from cartoonist Randall Munroe illustrates the efficacy of a long phrase password vs the dreaded keyboard smash.




Amount of Time
to Crack Passwords
"abcdefg" 7 characters
.29 milliseconds
"abcdefgh" 8 characters
5 hours
"abcdefghi" 9 characters
5 days
"abcdefghij" 10 characters
4 months
"abcdefghijk" 11 characters
1 decade
"abcdefghijkl" 12 characters
2 centuries