MANN GROUP CYBERSECURITY

How to Create A Strong Password You Can Remember

Passwords have been a source of frustration for information security professionals and users alike since the inception of business computing. At heart is the conflict between humans' capability to remember passwords, and ensuring hackers can't compromise accounts by guessing, credential harvesting or brute-force attack of those user passwords.

A strong password provides improved protection from hacking, but can increase risk if the user cannot remember it. Obtaining frequent password resets hurts productivity, annoys users and adds risk in itself, but users are also likely to use risky behaviors such as writing the password on a post-it under their keyboard.

Despite widely held beliefs in the industry, strong passwords don't need to be changed very often. NIST guidance has greatly backed off the recommended forced password reset frequency. Without password management utilities, a strong password that can be remembered is far better than a very strong and refreshed one that cannot be recalled from memory by anyone except Rainman.

A good way to create a memorable password that is also strong is to use a combination of rules that are easy to remember. Here's how to do it using what I call the "Apples to Apples" approach. Most people can remember 3-5 of these passwords with some practice.

Kids can use this approach as well; teenagers can be allowed to be creative with their "secret" password and codes. Instilling good cyber hygiene behaviors such as these will help kids remain safe online through their lifetime. With increased schoolwork being conducted online, this is especially important.

Apply these policies to create and protect your password:

1. Create a list of 5 crazy object words that pique your funny bone. Create another list of wacky one or two-word descriptors. You can be PG rated using Apples to Apples game cards as a guide, or MA rated using something naughtier like the Cards Against Humanity game cards. *Do not use your family, friends, pets or things that can be associated with you on social media*. Combine one object word and one descriptor (for example: fileted magicarp)
2. Create a simple algorithm for applying upper and lower-case that ensures usage of both cases. An example is to begin each word with a capital and also the following letter. Make this simple so that you can remember it. You should now have a funny word combination with some upper and lower-case letters.
3. Create a simple algorithm for applying numbers that ensures at least one number is added. You can replace a specific letter with a number (for example zero-O) and also append or prefix your word combination with a specific number. Make this simple to remember and apply.
4. Create a simple algorithm that ensures at least one special character is used, replacing certain letters with special characters and adding at least one other somewhere. Replacing "@" for "e" or "a", or replacing "S" with $ are commonly used examples. Try to be a little more creative but make it simple to remember.
5. After applying these steps you should now have an easy to remember, 12-20 character password based on a memorable phrase that uses both cases, numbers and special characters.

6. Use this password on your most important account. Depending on circumstances this could be your home router administrator account or your operating account (Windows or Apple ID).
7. Rinse and repeat for other important accounts such as home banking and social media. Never use the same word combination, but always apply the same algorithms for each password. This provides unique passwords that have some consistent logic behind them, thereby making them far easier to remember.
8. I don't discourage usage of account and password lists, if done with security in mind. My analysis indicates it is better to have a secure list on paper somewhere safe than resetting forgotten passwords repeatedly.
    a. Write down your password word combinations only, in lower case and matched to their accounts. Put the list someplace safe (not on your monitor or under your keyboard). This is your fallback if you forget which word combinations apply to which accounts, but it does not contain your actual passwords. You can use a hint list instead for more security if you are confident the hint will work for you.
    b. Write down your algorithms (that you've used consistently on all accounts) and put your "secret code" someplace very safe and not near your word combination list. You want to have these rules memorized, but this is your final backup if you forget. Separating lists physically ensures that even if one list is compromised, your password cannot be determined easily.
    c. If either of these lists is believed to be compromised, reset all passwords and start over.
9. If you need more passwords than you can remember in your head, you should use password management tools, which can handle the larger numbers and use more complex algorithms. Use a strong and memorable password for your management tool.

Mann Group Cybersecurity provides cybersecurity risk assessments and recommendations to small businesses and public entities in Southern Washington at a low cost.

Learn more at www.manngroupit.com and listen to our Cyberspace Cavern podcast at https://podcast.manngroupit.com