Allidm.com

Discovering Identity and Access Management Solutions

Strong Password

http://www.allidm.com/blog

Disclaimer and Acknowledgments

The contents here are created as a own personal endeavor and thus does not reflect any official stance of any Identity and Access Management Vendor on any particular technology

Introduction

- The secret to strong passwords is to not choose a password, but to build a password.

- Follow best practices
  - At least
    - 8 Characters
    - Include 1 Symbol
      - (e.g. @#$%)
    - Include 1 number
      - (e.g. 123456)
    - Include 1 lowercase
      - (e.g. abcdefgh)
    - Include 1 uppercase
      - (e.g. ABCDEFGH)

Password Entropy

- Password entropy is a measurement of how unpredictable a password is.

- Password entropy predicts how difficult a given password would be to crack through guessing, brute force cracking, dictionary attacks or other common methods.

Password Generation

- Users can generate the password in the following ways
  - Manually
    - Follow best practices
  - Automatically
    - Using Web App
    - Using Mobile App

Manual Generation

- Three Word Approach
  - This approach consist to use more than one Word to generate a password
  - Select three or more words that are not related, but have something in common.
    - Synonyms
    - Homonyms
    - Antonyms
    - Words that rhyme
    - Words wiht the same prefix

Bruce Schneier’s method

- Take a sentence and turn it into a password.
- The sentence can be anything personal and memorable for you.
- Take the words from the sentence, then abbreviate and combine them in unique ways to form a password.
- Sample
  - Ltime@go-inag~faaa! = Long time ago in a galaxy not far away at all.
  - Wow...doestcst = Wow, does that couch smell terrible.
  - WIw7,mstmsritt... = When I was seven, my sister threw my stuffed rabbit in the toilet.

The PAO Method

- Memorization techniques and mnemonic devices might help you remember an unbreakable password.
- Select an image of an interesting place. Select a photo of a familiar or famous person. Imagine some random action along with a random object.

PAO – How it works?

- Select a an image of an interesting place (for example, a baseball field) as well as a photo of a familiar or famous person (say, Bill Gates). You would then imagine some random action along with a random object to create a PAO story, says Jeremiah Blocki, the lead researcher. Blocki proposes, “Bill Gates swallowing a bike on the baseball field.”

- After you create and memorize stories for several different image pairs, you would use those stories generate unique passwords.
  - You might take the first three letters from “swallow” and “bike” so that you associate the image pair of Gates and a baseball field with “swabik”.
  -
- Do the same for three other stories, combine your made-up words together, and you’ll have an 18-character password that’ll appear completely random to others yet familiar to you.

Automated Generation

- Web Site
  - http://passwordsgenerator.net/
  - https://xkpasswd.net/s/
  - http://password-checker.online-domain-tools.com/

JUST DON’T

- Do not use the same password for multiple important accounts.
- Do not use the same security question and answer for multiple important accounts.
- Do not use the names of your families, friends or pets in your passwords.
- Do not use postcodes, house numbers, phone numbers, birthdates, ID card numbers, social security numbers, and so on in your passwords.
- Do not let your Web browsers(Firefox, Chrome, Safari, Opera, IE) store your passwords, since all passwords saved in Web browsers can be revealed easily.
- Do not log in to important accounts on the computers of others, or when connected to a public Wi-Fi hotspot, Tor, free VPN or web proxy.
- Do not store your critical passwords in the cloud.
- Do not tell your passwords to anybody in the email.

How Often Change Your Password?

- Changing password can be a stress task, specially if you have many accounts.
  - Don’t change your passwords, unless you suspect they’ve been compromised.
- If you prefer change your passwords:
  - every 10 weeks
  - 6 months or
  - once a year

Stay connected to Allidm

Find us on Facebook:

https://www.facebook.com/allidm

Follow us on Twitter:

https://twitter.com/aidy_idm

Look for us on LinkedIn:

http://www.linkedin.com/in/identityandaccessmanagement

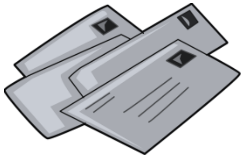
Visit our blog:

http://www.allidm.com/blog

Contact Us

On this presentation we’ll talk about some useful topics that you can use no matter which identity and access management solution or product you are working on.

If you know one that make a big difference please tell us to include it in the future.



aidy.allidm@gmail.com