Passwords: Best Practices #pass @class, July 31, 2017

Are your passwords secure? How often do you change them often? Do you use the same password on different websites? What is the best way to manage dozens of passwords? In this 90 minute session we'll discuss what constitutes a good password, tools for managing them, and other considerations for keeping username and passwords safe when used on the Internet.

Shared link: https://workflowy.com/s/90tlhGAlMj

- What are the problems with passwords?
  - "It's hard to imagine an idea more inane than passwords. That we protect many of the most important aspects of our lives with little more than a short string of text is an extreme absurdity." Rich Mogull
    http://www.macworld.com/article/2027760/the-everyday-agony-of-the-password.html
  - Passwords are broken
    - Nearly four in ten Americans (39%) would sacrifice sex for one year if it meant they never had to worry about being hacked, having their identity stolen, or their accounts breached.
      https://blog.dashlane.com/study-reveals-extremes-people-go-online-protection/
    - Any decent password is either nearly impossible to remember or too long to deal with.
    - The Worst Passwords of 2016
      https://www.teamsid.com/worst-passwords-2016/
    - "Passwords are not broken, but how we choose them sure is" -- Bruce Schneier
      https://www.schneier.com/essays/archives/2008/11/passwords_are_not_br.html
  - Usernames and passwords: an outdated model
    - an outdated solution to an increasing complex and high-stakes problem.
    - made sense a decade ago when people had few accounts and threats were few and far between.
    - OAuth
      An open standard for authorization, commonly used as a way for Internet users to log into third party websites using their Microsoft, Google, Facebook or Twitter accounts without exposing their password.
      https://en.wikipedia.org/wiki/OAuth
    - No universal standard for password security

        - Passwords don't identify a person uniquely
        - Given the number of people on the Internet, economies of scale make password cracking highly profitable.
    - How to come up with a good password?
    - How to remember it?
      "The only secure password is the one you can't remember"
- How people get our passwords?
    - Guessing
    - Brute force
      Sophisticated cracking (that is, guessing) algorithms can uncover most passwords with shocking speed. And hackers are constantly improving their tools and techniques.
        - Online vs Offline
          https://nakedsecurity.sophos.com/2014/10/24/do-we-really-need-strong-passwords/
    - Theft/hacking/sniffing
        - physical theft
        - hacking (malware)
        - keystroke logging
        - sniffing wireless
        - looking over your shoulder
    - Social Engineering
        - phishing emails
        - phone-calls
    - Post-it notes
      http://lifehacker.com/5852667/the-most-common-hiding-places-for-workplace-passwords
    - "Remember me"
      http://www.hongkiat.com/blog/reveal-hidden-passwords-in-browsers/
    - https://haveibeenpwned.com/
- What doesn't make a good password?
    - the obvious password (one of the passwords on the list of worst passwords)
      https://www.teamsid.com/worst-passwords-2016/
    - the default password

- dictionary word
- anything that is easily guessable about you: name of pet or relative, birthday, anniversary, etc.
- simple transformations and substitutions
- keyboard patterns
- starting with an upper case letter followed by lower case letters
- when a password isn't long enough, adding a letter or two to the base word
- putting digits, especially two or four of them, before or after the letters
- when a special character is required, using "!" and putting it at the end
- not using two special characters in the same password
- any password that you read in an article - hackers read it too.

- What makes a good password?
  - One that you won't forget but that no one else (human or computer) can guess
  - Size of character set used
    - choose from all 95 characters on U.S. keyboard: 26 upper case, 26 lower case, 10 digits, 33 special characters
    - https://www.grc.com/haystack.htm
  - Length (but length alone doesn't guarantee a good password)
    - Once an exhaustive password search begins, the most important factor is password length!
    - Once passwords get above 15 characters, they're very hard to crack even with brute force methods.
    - http://www.orange-business.com/en/blogs/connecting-technology/security/passwords-the-key-to-keeping-your-secrets-locked-up-tight
  - Randomness (very hard to do in general)
  - More suggestions:
    - Resist your natural tendency to mimic familiar words and phrases
    - Avoid beginning the password with an upper case letter—or maybe even any letter
    - Use multiple special characters in the same password
    - Don't always place digits adjacent to each other
  - Three random words or #thinkrandom
    https://www.ncsc.gov.uk/blog-post/three-random-words-or-thinkrandom-0

- Password strength checkers
  - Many of them out there:
    - https://www.microsoft.com/en-us/security/pc-security/password-checker.aspx
    - http://www.passwordmeter.com/
    - https://www-ssl.intel.com/content/www/us/en/forms/passwordwin.html
    - https://www.my1login.com/resources/password-strength-test/
    - https://password.kaspersky.com/
    - https://howsecureismypassword.net/
  - Those password-strength meters are often misleading
    http://readwrite.com/2015/03/27/password-strength-weaker-than-you-think
    https://nakedsecurity.sophos.com/2015/03/02/why-you-cant-trust-password-strength-meters/
  - Passwords that Kill
    https://www.insedia.com/articles/passwords-that-kill-683384ca-928b-425f-be61-2db2c08a79f4
  - Why you STILL can't trust password strength meters
    https://nakedsecurity.sophos.com/2016/08/17/why-you-still-cant-trust-password-strength-meters/
    - “(A hacker’s) first line of attack is likely to be based on dictionary words and rules that mimic the common tricks we use to di5gu!se th3m,” he wrote. “The trouble is that most password strength meters don’t actually measure password strength at all…The only good way to measure the strength of a password is to try and crack it – a serious and seriously time consuming business that requires specialist software and expensive hardware.”
  - One of the best
    http://www.takecontrolbooks.com/resources/0148/zxcvbn/
- Simple Strategy for managing passwords
  - Figure out which passwords you must memorize
  - Create strong but memorable passwords for the few
    - The challenge that we face is to have master passwords that [are] not going to be guessed by password cracking programs, yet we mere mortals are capable of remembering and typing without it being a burden. What makes this a particular challenge is the fact that the bad guys know at least as much about how people pick passwords as we do. They are not only reading the same password picking advice that gets posted in places like this, but they have studied millions of stolen passwords.
    - How to pick a proper password
      https://youtu.be/pMPhBEoVulQ

    - xkcd cartoon: Password Strength
      https://xkcd.com/936/
    - The Diceware Passphrase Home Page
      http://world.std.com/~reinhold/diceware.html
    - Choosing Secure Passwords
      https://www.schneier.com/blog/archives/2014/03/choosing_secure_1.html
    - Fix your terrible, insecure passwords in one minute
      http://www.slate.com/articles/technology/technology/2009/07/fix_your_terrible_insecure_passwords_in_five_minutes.html
    - Toward better master passwords
      https://blog.agilebits.com/2011/06/21/toward-better-master-passwords/?r44b=no
    - Do you find passwords too darn hard? Then poetry's your hidden card!
      https://nakedsecurity.sophos.com/2015/10/24/do-you-find-passwords-too-darn-hard-then-poetrys-your-hidden-card/
- Use a password manager for everything else
    - "Password managers change the whole calculus because they make it possible to have both strong and unique passwords."
    - Why you should use a password manager and how to get started
      http://www.howtogeek.com/141500/why-you-should-use-a-password-manager-and-how-to-get-started/
    - The 6 best password managers, May 25, 2017
      http://www.csoonline.com/article/3198507/security/the-6-best-password-managers.html
    - The Best Password Managers (last updated July 21, 2017)
      http://thewirecutter.com/reviews/best-password-managers/
    - Password managers don't have to be perfect, they just have to be better than not having one
      https://www.troyhunt.com/password-managers-dont-have-to-be-perfect-they-just-have-to-be-better-than-not-having-one/
    - Password Managers:
        - Lastpass
        - 1Password
        - Dashlane
        - Roboform
        - Open source
            - Keypass

        - Password Safe
    - Others
        - https://lesspass.com/#/
        - http://masterpasswordapp.com/

- Best practices
    - One account, one password
    - Use passphrases: a simple password is as almost as good as no password
    - Use a password manager (disable browser password managers)
    - Consider two-factor (multi-factor) authentication: what you know; what you have
    - If possible add a recovery email account
    - Use multiple email accounts (personal, everyday, "throwaway," etc.)
    - Use a dedicated password-reset email account, with two-factor authentication
    - Use different username, if possible
    - Get a CLU: Complex. Long. Unique.
    - It's OK to write down your password
      https://www.schneier.com/blog/archives/2005/06/write_down_your.html
    - Want Safer Passwords? Don't Change Them So Often
      http://www.wired.com/2016/03/want-safer-passwords-dont-change-often/?utm_source=nextdraft&utm_medium=email
    - Don't store your passwords on your inbox or on your desktop, etc.
    - Change passwords frequently? Maybe Not.
        - "Treat your password like your toothbrush. Don't let anybody else use it, and get a new one every six months." Clifford Stoll
        - "Don't bother updating your password regularly. Sites that require 90-day -- or whatever -- password upgrades do more harm than good. Unless you think your password might be compromised, don't change it." Bruce Schneier
    - Security questions
        - Just another, easily guessed password
        - Enter a password hint that has nothing to do with the question itself (but keep track of it)
        - When password security questions aren't secure
          http://www.macworld.com/article/2016925/when-password-security-questions-arent-secure.html

- Traveling? (in password manager create one-time-passwords (OTP))

- Securing yourself online (if there is time)
  - User is the weakest link. Be judicious; use common sense
  - Create and use a standard / non-admin account
  - Use firewall on both router and computer
  - Kreb's 3 basic rules for online safety
  - Regular security updates, both OS and applications
  - Use different browsers for different activities
  - Use different computers for different activities
  - Use virtual computers for different activities
  - Use alternative DNS
    - OpenDNS https://www.opendns.com/
    - Google DNS https://developers.google.com/speed/public-dns/
  - Use HTTPS when connecting to websites: https://www.eff.org/Https-Everywhere
  - Use a VPN if mobile

- Select Bibliography

  - The Everyday Agony of the Password
    http://www.macworld.com/article/2027760/the-everyday-agony-of-the-password.html
  - Passwords are not broken, but how we choose them sure is
    https://www.schneier.com/essays/archives/2008/11/passwords_are_not_br.html
  - Choosing secure passwords
    https://www.schneier.com/blog/archives/2014/03/choosing_secure_1.html
  - Fix your terrible, insecure passwords in five minutes
    http://www.slate.com/articles/technology/technology/2009/07/fix_your_terrible_insecure_passwords_in_five_minutes.html
  - Kill the password: A string of characters won't protect you
    http://www.wired.com/2012/11/ff-mat-honan-password-hacker/all/
  - How Password Managers Keep Your Passwords Safe
    http://www.makeuseof.com/tag/password-managers-keep-passwords-safe/
  - Write down your password
    https://www.schneier.com/blog/archives/2005/06/write_down_your.html
  - Unmasked: An Analysis of 10 Million Passwords

http://wpengine.com/unmasked/

- The worst passwords of 2015
  https://www.teamsid.com/worst-passwords-2015/
- Want Safer Passwords? Don't Change Them So Often
  http://www.wired.com/2016/03/want-safer-passwords-dont-change-often/
- How not to become Mat Honan: A short primer on online security
  http://www.wired.com/2012/08/how-not-to-become-mat-honan/
- The four things you need to do right now to avoid the fate of tech writer Mat Honan
  http://www.slate.com/articles/technology/technology/2012/08/mat_honan_the_four_things_you_need_to_do_right_now_to_avoid_getting_hacked_.html
- New research: Comparing how security experts and non-experts stay safe online
  https://googleonlinesecurity.blogspot.com/2015/07/new-research-comparing-how-security.html
- Perfect Passwords: Selection, Protection, Authentication
  http://www.amazon.com/Perfect-Passwords-Selection-Protection-Authentication/dp/1597490415
- Take Control of Your Passwords, Joe Kissell (available via Safari books)
  https://www.takecontrolbooks.com/passwords
- Get Organized: How I Cleaned Up My Passwords in 5 Weeks
  http://www.pcmag.com/article2/0,2817,2425224,00.asp
- FYI: How I became a password cracker
  http://arstechnica.com/security/2013/03/how-i-became-a-password-cracker/
- FYI: Anatomy of a hack: How crackers ransack passwords
  http://arstechnica.com/security/2013/05/how-crackers-make-minced-meat-out-of-your-passwords/
- FYI: Salted Password Hashing - Doing it Right
  https://crackstation.net/hashing-security.htm

- NEW_MATERIAL
  - Passwords Evolved: Authentication Guidance for the Modern Era
    https://www.troyhunt.com/passwords-evolved-authentication-guidance-for-the-modern-era/
    - In the beginning, things were simple: you had two strings (a username and a password) and if someone knew both of them, they could log in. Easy.
    - Longer is (usually) Stronger
    - Embrace Password Managers
      - The only secure password is the one you can't remember
        https://www.troyhunt.com/only-secure-password-is-one-you-cant/

        - We know that passwords must be "strong", that is that they shouldn't be

predictable or readily brute forced so in other words, the longer and more random, the better.

- We know that passwords shouldn't be reused because disclosure by one service puts the user's other services at risk. This is the whole credential stuffing problem I referred to earlier.
- People cannot create strong, unique passwords across all their services using only their brain to remember which one they used where.

- You're Going To Die Someday. Who Do You Trust With All Your Passwords?
  https://www.buzzfeed.com/nicolenguyen/digital-death-plan-passwords?utm_term=.rixPwA4Vy#.koB8ZnDMp
- Password Storage On a Keychain: Hideez Digital Key Review
  http://www.makeuseof.com/tag/hideez-digital-key-review/
- Could a doodle replace your password?
  https://theconversation.com/could-a-doodle-replace-your-password-56792
- Microsoft Password Guidance
  https://www.microsoft.com/en-us/research/wp-content/uploads/2016/06/Microsoft_Password_Guidance-1.pdf
- Why emojis might be your next password
  https://theconversation.com/why-emojis-might-be-your-next-password-76973
- The long history, and short future, of the password
  https://theconversation.com/the-long-history-and-short-future-of-the-password-76690
- Why we choose terrible passwords, and how to fix them
  https://theconversation.com/why-we-choose-terrible-passwords-and-how-to-fix-them-76619
- The math behind passwords
  http://securitymusings.com/article/3732/the-math-behind-passwords
- How to Remember All the Passwords You Need in Your Life
  http://blog.credit.com/2017/04/how-to-remember-all-the-passwords-in-your-life-171957/