I H8 Pa55w0rds

A brief history of passwords

1. Your first password? Probably an ATM PIN
2. Passwords become more prevalent
3. Something easy to remember, but hard to guess
4. And we used that password everywhere
5. Computer programs can quickly crack passwords…and they never get tired of trying
    5.1. The shorter the password, the faster the program can crack it through a brute force attack or dictionary attack
6. 8 characters, mix of upper and lower case letters, numbers, maybe a symbol
7. No dictionary words, no common sequences (e.g., 1234), requirements to change the password every few months
8. Strong passwords: 16 characters, unique for every account

Why we hate passwords

9. They slow me down
10. Can’t remember them
11. I just don’t get it
12. I have to know my passwords, I *have* to
13. I don’t have anything of importance

Common solutions

14. Picking a lousy password…and using it everywhere
15. The list in the upper desk drawer
16. The post-it note stuck to the computer screen
17. The book I carry around with me with handwriting I can't make out and multiple entries every time I change my password so I never know which password is correct and maybe even what it applies to
18. The slip of paper in my wallet
19. Other solutions

Layers of passwords

20. Device—Mac, iPhone, iPad, Apple Watch
    - 20.1. Face ID and Touch ID can substitute for having to type in your password or passcode
    - 20.2. Apple Watch can unlock your Mac and your iPhone (if you're wearing a face covering
    - 20.3. iPhone can unlock your Apple Watch
21. Apple ID
    - 21.1. Your account for everything you do with Apple
    - 21.2. User name: An email address you already have
    - 21.3. Password: Unique
22. Everyone else
    - 22.1. User name: Usually an email address, but not always
    - 22.2. Password: Unique

A better solution

23. Password manager
    - 23.1. Creates strong passwords
    - 23.2. Unique for every account
    - 23.3. Securely stores and syncs them
    - 23.4. Plugs them in when needed
    - 23.5. Points out weak or duplicative passwords
    - 23.6. Notes when account info may have been breached
24. Many third-party products
    - 24.1. 1Password, Last Pass, etc.

Keychain

25. Built-in to Apple's devices
    - 25.1. If you use Safari and all Apple devices, it may be all you need
26. Passwords stored and accessed on the device
    - 26.1. Mac: Safari > Preferences > Passwords
    - 26.2. iPhone/iPad: Settings > Passwords
27. Synced through iCloud Keychain
    - 27.1. Website login information
    - 27.2. Credit card information
    - 27.3. Wi-Fi network information
    - 27.4. Login information for the accounts you use in Mail, Contacts, Calendar, and Messages so it's available on all your devices

28. End-to-end encryption
    28.1. In transit between your devices
    28.2. At rest on your devices (protected by the device password passcode) and in iCloud (by tor Apple ID password)
        28.2.1. Apple does not know your Apple ID password and cannot access the contents of your keychain
    28.3. Remember these: Device password/passcode and Apple ID password
    28.4. Let the keychain do the rest

Set up the iCloud Keychain

29. On iPhone and iPad
    29.1. Tap Settings
    29.2. Tap *your name*
    29.3. Tap iCloud
    29.4. Tap Keychain
    29.5. Turn on iCloud Keychain
        29.5.1. You might be asked for your Apple ID password or device passcode
        29.5.2. You might be prompted to turn on Two-Factor Authentication first
30. On Mac
    30.1. From the Apple menu, pick System Preferences
    30.2. Click iCloud or Apple ID

30.3. Enable iCloud Keychain

Enable Password AutoFill

31. On iPhone and iPad
    31.1. Tap Settings
    31.2. Tap Face ID/Touch ID & Passcode
    31.3. Turn on Password AutoFill
    31.4. Tap Other Apps and turn on the switches for other apps
32. On Mac
    32.1. Launch Safari
    32.2. From the Safari menu, pick Preferences…
    32.3. Click AutoFill
    32.4. Enable User Names and Passwords
    32.5. Optionally enable credit cards

Creating strong passwords

33. Visit a website
34. Create an account
    34.1. Provide a user name
    34.2. Let the device suggest a unique strong password
35. When prompted, allow the device to store the log in credentials on its keychain

35.1. Safari options on the Mac: Yes, Not Now, Never

36. New login credentials will sync through iCloud to your other devices' keychain

---

Using the keychain

37. Visit a website

38. Tap/click the user name field to log in

38.1. Device will offer to plug in the user name and password stored on the keychain

38.2. You may need to authenticate on iPhone/iPad with Touch ID, Face ID, or the device passcode to unlock the keychain

39. Tap/click login

40. Works with iPhone/iPad apps, too

40.1. Many apps on iPhone/iPad can use Touch ID and Face ID to allow you to sign in

40.2. Settings > Face ID/Touch ID and Passcode > Other Apps

Viewing and editing passwords

41. Mac: Safari > Preferences > Passwords

42. iPhone/iPad: Settings > Passwords

43. Ask Siri: "Hey Siri, show me my passwords."

44. On iPhone/iPad, tap Edit to make changes

45. On Mac, select an entry and click Details… to make changes

46. Tap/click Share button to share login credentials via AirDrop
    46.1. To receive a password, you must be in the sender's Contacts app
47. Login credentials can be added manually; might be easier to login to a website, and when prompted allow the Keychain to store the credentials
48. Deleting a password from the Keychain does not delete your account with the website; that step needs to be done separately

Security recommendations

49. Allow the device to detect passwords compromised by known data leaks
50. Device will point out problems, actions you should take, and why you should take them

Changing passwords

51. Log in with your current password to the website where you want to change the password
52. Change the password on the website
53. If prompted to update the password on the keychain, do so
    53.1. You may need to log out of the website in order to be prompted to update the password
54. Devices offer a Change Password on Website button or link

Help is on the way

55. A new technology has emerged: Passkeys
56. The Promise of Passkeys: No more passwords
57. Apple, Google, Microsoft are all behind it
58. You create a public key which any website or vendor can have
59. Your device contains a private key
60. Authentication occurs on your device
61. So there are no passwords to create, retain, remember, or store on other websites
62. If a data breach occurs on a third-party website, there is no password to steal
63. Set it up like a password, but choose passkey instead
64. Sign in with a passkey rather than a password using the same process
65. Websites and app developers need to update to add passkeys
66. A few are underway: Kayak (app, but not website), Best Buy (website, but not app), eBay, PayPal (website, but not app)
67. There's a demo here: https://www.passkeys.io/

Just Plain Help

68. Me: Mike Matthews, mamatthews@icloud.com, 925-876-4098
69. Apple Support: support.apple.com

mm—3/16/2023