Password Management Systems

Document Outline

1. Important terms
2. Password Security
3. Introduction to Password Management Systems
4. Benefits and drawbacks of password management
5. Security checkup

Important terms

The scope of this program limited to password management, but these terms might help to give context to some of the drawbacks and benefits of password management systems.

Privacy & Security

One definition of privacy I really like is the *authorized* processing of personally identifiable information.[1] Security refers to how that data is protected.[2] This program will focus mostly on security.

Encryption

While technologically advanced, the concept of encryption is relatively easy to understand. Encryption creates keys so only the sender and the intended receiver can decipher the message.[3]

Extension

Software that extends functionality to your web-browser. They are singular in focus and can be used for many different purposes such as translation, ad-blocking, or password management. An example of a very popular extension is the Pinterest 'Save' button. Password managers use browser extensions.

---

[1] BALibrary database subscription. LinkedIn Learning. *Understanding and Prioritizing Data Privacy* (Course): Privacy vs. secrecy (Video)

[2] Web. Norton USA. *Privacy vs. Security: What's the Difference?* https://us.norton.com/internetsecurity-privacy-privacy-vs-security-whats-the-difference.html

[3] Web. New York Times. *What is End-to-End Encryption: Another Bulls-Eye on Big Tech* https://www.nytimes.com/2019/11/19/technology/end-to-end-encryption.html

Passwordless Passkeys

Passkeys don't need to be remembered or typed because they are based on specific data that only you can provide. They use your fingerprint, face scan, or a screen lock.

Google[4] – Passkeys are saved on your local device. You'll need one passkey per device, unless the device has some mechanism to "synchronize" passkeys to other devices already, like with Apple iCloud. You can still continue to log in to your accounts with a password if you prefer.

More information on Passkeys through Google can be found here: https://safety.google/authentication/passkey/

Apple[5] – Passkeys and passwords are stored in your iCloud Keychain. According to Apple's website:

> "In iCloud Keychain, passkeys are end-to-end encrypted, so even Apple can't read them. A passkey ensures a strong, private relationship between a person and your app or website."

They can be shared with trusted contacts. Passkeys with Apple look like a fingerprint touch to unlock a phone or to sign in, as well as looking at your device to use a scan of your face to unlock or access. Because they are stored with iCloud, they can be used across Apple devices, and even be used with non-Apple apps and websites through your iPhone.

More information on Passkeys through Apple can be found here: https://developer.apple.com/news/?id=21mnmxow

Password Security

Regardless of which password management system you use, you can practice good online behavior by following a few important steps:[6]

- Create strong passwords
  - Use 12 characters
  - Combine letters, numbers and symbols
  - Using four random words
  - Ideas for strong passwords are longer lyrics from songs, use abbreviations as stand-ins for letters or words.

[4] Information based on review of Google's Safety Center on Passkeys: https://safety.google/authentication/passkey/.
[5] Information based on a review of Apple's Passkey website: https://developer.apple.com/passkeys/
[6] Web. Google Account Help. *Create a Strong Password and More Secure Account.* https://support.google.com/accounts/answer/32040?hl=en

    - Don’t use weak, easily compromised passwords such as ‘password,’ ‘p@ssw0rd!’, of that contain easily crack-able strings like ‘abcd,’ ‘qwerty’, ‘1234’ etc.
    - Don’t use personal information
- Use unique passwords for sites. It is easy to expose other accounts with the same name and password.
- Use two-factor authentication where available

Introduction to Password Management Systems

Password management systems are specifically designed to enable you to record and correctly enter your passwords. There are a number of different ways you can record and enter your passwords both offline and online. None of these methods can guarantee that your passwords will remain safe and not become exposed, but they can help to make you information more secure and help you keep track of the ever-expanding list of passwords in your life.

Offline examples

Even if you store your passwords offline, you can still add a layer of encryption to them. 1) Instead of writing the actual password out, you would write out obvious clue to a password you know by heart or 2) you can password protect your excel documents.

- Notebook
- Excel document

Online examples[7]

Dedicated software

- 1password
- Bitwarden
- Dashlane
- LastPass
- Keychain

DIY and Built-in Options

- Google documents

[7] List was compiled in part by reviewing information from:
WIRED Magazine: *The Best Password Managers to Secure Your Digital Life*
https://www.wired.com/story/best-password-managers/

- Browser password management[8]

Passwordless Passkeys

- Touch ID/Fingerprint
- Face ID
- Screen lock

Benefits & drawbacks

Offline

- Benefits
    - Passwords will not all be exposed via online breach
    - Others can access if needed
    - Free
- Drawbacks
    - Difficult to update
    - Only useful if you have your notebook/document with you at all times

Online

- Benefits
    - Others can access, if needed (family sharing)
    - Can automatically generate passwords for you
    - Available across devices
    - Dedicated platforms have a high level of data security
    - Have a built-in security checkup to show you how your information is being used

- Drawbacks
    - Entering passwords on new devices or a computer that is not your own
    - Fees (where applicable)

Security Checkup

As we've discussed, many of the online companies have ways for you to checkup on your data and how it being used online. Other ways you might track this:

- Google Account > Security > Password Manager

[8] Web. WIRED Magazine: *Sorry, But Your Browser Password Manager Probably Isn't Enough.* *https://www.wired.com/2016/08/browser-password-manager-probably-isnt-enough/*

- Browsers such as chrome might also alert you when you are signing in that your password should be changed due to a breach