HMC's Guide to Password Managers

You may have read or been told to not use the same password everywhere and to make complex passwords, but these two information security recommendations might seem too challenging because you have accounts and passwords for everything. Below are two simple suggestions for simplifying and managing passwords and protecting your data.

Passphrases

The days of crazy, complex passwords are over. Those passwords are hard to remember, difficult to type, and can sometimes even be easy for a cyber attacker to crack. The key to passwords is to make them long; the more characters you have the better. These are called passphrases: a type of strong password that uses a short sentence or random words. Here are two examples:

Time to go to the dog park!

Sun-moon-rise-and-glow

Both of these are strong, with over twenty characters, easy to remember, and simple to type but difficult to crack. You will run into websites or situations requiring you to add symbols, numbers, or uppercase letters to your password, which is fine. Remember though, it's the length of the passphrase that is most important.

Password Managers

The most common way that online accounts are compromised is through password reuse. If the same password is used for multiple sites, attackers only need to breach one account, then use the

associated email and password to “hack” into all other accounts on different sites. The best way to prevent account theft is to use a strong and unique password on every site. It can get really difficult to remember or keep track of multiple different passwords, so a password manager can help by storing all of your different passwords for you in one secure location behind a strong master password.

Password managers are special computer programs that securely store all your passwords in an encrypted vault. You only need to remember one password: the one for your password manager. The password manager then automatically retrieves your passwords whenever you need them and logs you in to websites for you. They also have other features such as storing your answers to secret questions, warning you when you reuse passwords, a password generator that ensures you use strong passwords, and many other features. Most password managers also securely sync across almost any computer or device, so regardless of what system you are using you have easy, secure access to all your passwords.

The CIS Department uses the LastPass app for password management. Please contact the HelpDesk to learn more helpdesk@hmc.edu. Choosing the right password manager for you depends on your own personal preferences and purpose of use. Here are some other suggestions of popular and reliable password managers:

Browser Password Managers:

- May be securely synced between devices that use the same account and browser
    - Common ones are Google accounts or Apple IDs
    - Most use encrypted cloud storage
- Not as powerful as third-party password managers:
    - Limited to specific browser and/or device, i.e. you cannot share passwords between Google Chrome and Safari
    - Browsers do not have password-sharing functionality
    - Most will not check your password for strength, and will not suggest or generate passwords for you
- Better than nothing!

LastPass (HMC has a campus license for faculty and staff. Students are Free):

- App available for Mac, iOS, Android
- Browser extensions for Chrome, Firefox, Internet Explorer, Edge, Opera

    - Universal installers available for Windows, MacOS, and Linux that can add the extension to all browsers at once.
- All data stored with AES-256 bit encryption with PBKDF2 SHA-256 and salted hashes for security
- Free version:
    - Only allows 1 user on account
    - Synced information access on all associated devices
    - One-to-one data sharing
    - Securely save and fill passwords, credit card information, delivery addresses
    - Encrypted storage of sensitive notes, insurance policy details, etc.
    - Includes unique password generator and security audits on existing passwords to analyze strength
    - Multi-factor authentication
- Premium version ($3/month):
    - All features of free version with advanced multi-factor options
    - One-to-many data sharing
    - Provides app support to log into apps on a mobile device
        - Invaluable feature to protect mobile data such as emails and social media information from phone theft
    - Emergency access feature
    - Priority tech support
    - Includes 1GB encrypted file storage

1Password (30-day free trial, $3/month):

- Supports Mac, iOS, Android, Windows, ChromeOS
- Offers easy access plug-ins for most common web browsers
- Acts as an additional authentication app
- Generate new unique, strong passwords
- Creates a secret key to the encryption key for added security
    - No one, not even 1Password, can decrypt stored passwords without the key -- don't lose it!
- Integrated with many mobile apps, even ones with restricted inter-app communication
- Features Travel Mode which gives users the ability to delete any sensitive data from devices before travel, then restore it on command
    - Prevents any foreign parties from accessing your password cache
    - Safely cross borders without sensitive information
- Unlimited password and item storage, 1GB document storage, and 24/7 email customer support
- Offers 365 day item history to restore deleted passwords

Bitwarden (Free, offers upgrades):

- Popular among open-source software advocates

    - All of Bitwarden code is open source -- allows user contribution to eliminate flaws and bugs
    - All code is audited by a third party to maintain security
- App support for Android, iOS, Windows, MacOS, and Linux
- Offers extensions for all major web browsers (Chrome, Firefox, etc.), as well as less common browsers like Opera, Brave, and Vivaldi
- Provides a semi-automated password fill-in tool on sites with previously saved credentials!
    - Requires selection of saved accounts
    - Allows easy switching between usernames
- Offers paid upgrade accounts
    - Cheapest option is $10/year: unlocks 1GB of encrypted file storage, two-factor authentication, password hygiene and vault health reports, and priority customer support.

<u>Dashlane</u> (Free, offers upgrades):

- App available for Windows, MacOS, Android, iOS, and Linux
- Browser extensions for Firefox, Chrome, and Edge
- Free 30 day trial of Premium or Premium Plus
- Option to not store any data on Dashlane's servers for total password privacy -- user is responsible for managing and syncing password information between devices
- Free version:
    - Stores logins for up to 50 accounts behind two-factor authentication, saves and auto-fills form and payment information, generates personalized security alerts
    - Uses a personal secret key to encrypt password and information cache (like 1Password)
    - Securely share up to 5 Dashlane accounts
    - Stored information only available on one (1) device; no syncing of data across devices
- Premium ($5/month):
    - All features of the free version, but allows unlimited passwords
    - Securely share unlimited Dashlane accounts on each device
    - Synchronize data across unlimited devices
    - Monitors dark web for data breaches and sends personalized alerts if compromised information is detected
    - Offers a personal VPN for WiFi Protection and secure file storage (useful for ID documents, insurance policies, etc.)
- Premium Plus ($10/month):
    - All features of Premium plan
    - Includes credit monitoring, identity recovery support, and Identity Theft Insurance

<u>Keeper</u> (Free, offers upgrades):

- Most robust range of app support: Windows 7+, Linux, MacOS, Android, iOS, Blackberry, Kindle, and Nook, among others

- Browser extensions for all the major browsers (Chrome, Firefox, Safari, Internet Explorer), as well as lesser known ones like Opera
- Some features are only available with specific location download
    - Apple fingerprint authentication only available with downloads from the App Store
    - Integration with Edge browser only available with downloads from the Microsoft Store
- Available in over 13 languages
- Two-factor authentication with security keys