Lander UNIVERSITY

Information Technology Services
http://www.lander.edu/its
help@lander.edu
864.388.8234

Password Management Options

A password manager is an application that stores multiple passwords in a single secure repository. Protected by one master password (and often a second form of authentication), a password manager can help to alleviate much of the hassle associated with creating and remembering a strong, unique password for each of your online accounts.

The additional security and convenience provided by a password manager may be worth considering if you find yourself practicing bad habits, such as:

- Using the same password for more than one account
- Creating passwords that are short or lack complexity
- Using passwords that consist of common words, phrases, or patterns
- Saving passwords in a web browser
- Writing down passwords in a notebook or storing them in a text file.

Lander University does not yet provide an official password management solution for faculty and staff, so this document serves as a resource for employees interested in pursuing a password manager for business or personal use.

None of the products included are endorsed or supported by Lander University or ITS. The following password managers are provided as popular examples of solutions available to consumers. All information is subject to change but is accurate, to the best of our knowledge, as of December 2016.

The information for each product assumes the use of a desktop or laptop as the main password management device, so all features listed may not be available on mobile app versions. Since most password managers offer free and paid versions, this document primarily addresses features included in the free editions.

Comparison of Free Versions

Password Manager	Dashlane	LastPass	LogMeOnce
Device Use	Only one device	Multiple devices (computer, mobile)	Multiple devices (computer, mobile)
Installation	Desktop application; web browser extension	Web browser extension; mobile app	Web browser extension; mobile app
Import Options	Web browsers; other password managers	Web browsers; other password managers	Web browsers
Password Generator	Yes	Yes	Yes
Password Changer	Yes, over 300 supported websites	Yes, 80 supported websites	Available as separately installed tool
Multi-factor Authentication	Touch ID (iOS); Google Authenticator app	LastPass Authenticator; Google Authenticator	Email code; Google Authenticator app
Account Beneficiary	Yes	Yes	Yes
Account Recovery	None	Text message reset	Email reset link

Dashlane

https://www.dashlane.com/

Device Use: With the free version, Dashlane can only be used on a single device; syncing of passwords to mobile devices or other computers is not available in this version. If you find yourself regularly signing in to accounts on multiple devices, particularly across platforms (desktop to mobile, etc.), the single-device restriction of Dashlane's free version will severely limit the usefulness of this password manager.

Installation: From Dashlane's website, download and install the desktop application. This application will walk you through the process of account creation / setup and also install the Dashlane extension for your preferred web browser (works with all major browsers except Microsoft Edge). The desktop application will be used to manage your account, access your password vault, and launch saved sites, while the browser extension allows you to capture passwords when logging in to new sites and automatically sign in to any saved accounts. Free mobile apps are available for both Android and iOS if you choose to use a phone or tablet for your single device.

Import and Add: Dashlane allows users to import passwords saved in most web browsers (Chrome, Firefox, Safari, Internet Explorer) and a few competing password managers, such as LastPass. Passwords for new sites can be manually added in the desktop application or captured via the browser extension. Unlike some other managers (LastPass), Dashlane's browser extension does not provide a manual capture feature to save all data fields in the event that a site has a non-standard login screen.

Passwords: Dashlane allows an unlimited number of passwords to be stored in the vault and also allows multiple credentials to be saved for the same website. Dashlane includes a built-in password generator that offers to upgrade current passwords or create secure passwords for new accounts. Additional features include a password changer to automatically update passwords for over 300 websites and the ability to autofill personal data, including payment information, into web forms.

Multi-factor Authentication (MFA): Dashlane supports additional authentication options beyond the master password, including Touch ID on iOS devices and mobile authentication apps like Google Authenticator.

Emergency Access: Dashlane allows users to designate a password beneficiary to receive access to all or some login credentials in the event of an emergency. This process includes a waiting period after a beneficiary requests access and the ability for the Dashlane user to revoke a beneficiary's access.

Account Recovery: Dashlane does not offer a way to resend or reset a master password. If you forget your master password, the only option will be to delete the Dashlane account and start over.

Premium Edition ($39/year): If you access your accounts across multiple devices, Dashlane Premium is necessary to get the most out of this password manager. In addition to allowing you to sync your password vault across all devices, Dashlane Premium offers an option to store an encrypted backup of your account in the cloud. Although the sharing of passwords is never advised, some users find this necessary for certain accounts, and Dashlane Premium includes unlimited password sharing (free version only allows five shares).

LastPass

https://www.lastpass.com/

Device Use: LastPass can be used on multiple devices and can sync stored passwords across different types of devices, allowing you to access your password vault on any number of computers and mobile devices. LastPass also offers a mobile app for use on phones or tablets.

Installation: After creating an account with a master password, LastPass is installed as a web browser extension. On a mobile device, you can download the app and sign in with your master password. The mobile app allows users to launch sites from the password vault or add the mobile browser extension.

Import and Add: LastPass allows users to import any passwords saved in web browsers or other password managers. After importing from a browser, LastPass deletes the browser's saved credentials and turns off this automated feature within the browser. New passwords can be saved to the vault by signing in to secure sites and allowing the LastPass extension to capture the credentials.

Passwords: LastPass allows an unlimited number of passwords to be stored in the vault and also allows multiple credentials to be saved for the same website. LastPass includes a built-in password generator which helps to audit your vault for weak or duplicate passwords. Additional features include the ability to autofill credentials into saved websites and to automatically change passwords for approximately 80 websites.

Multi-factor Authentication (MFA): LastPass offers additional authentication options beyond the master password, but these options require a separate mobile app, such as LastPass Authenticator or Google Authenticator.

Emergency Access: LastPass allows you to designate one password heir to receive access to all login credentials in your vault in the event of an emergency. This process includes a waiting period after an heir requests access and the ability for the LastPass user to refuse this request or revoke an heir's access.

Account Recovery: If a phone number has been added to your account, LastPass allows you to request a text-based reset if you forget your master password. If you are still unable to recover or reset your master password, the only option will be to delete the LastPass account and start over.

Premium Edition ($12/year): In addition to all of the features available in the free version, LastPass Premium removes advertisements displayed in the password vault, provides password management for applications, and includes enhanced MFA options, such as fingerprint authentication.

Note: LastPass experienced a data breach in June 2015. Due to the security measures in place at the time, no actual passwords were compromised, but the company did implement additional security features to address the cause of the breach.

LogMeOnce

https://www.logmeonce.com/top-features/

Device Use: LogMeOnce can be used on multiple devices and can sync stored passwords across different types of devices, allowing you to access your password vault on any number of computers and mobile devices. LogMeOnce is available on Windows and Mac OS as a browser extension and on Android and iOS as an app.

Installation: From LogMeOnce's website, sign up for an account. During the account creation process, you can choose a master password for your vault or choose a "passwordless" option that requires a mobile device for authentication. After creating an account, LogMeOnce will prompt you to download and install their web browser extension. Note that this extension will need to be installed on any computer from which you intend to access your LogMeOnce vault.

Import and Add: LogMeOnce allows users to import passwords saved in web browsers, but it does not automatically remove these saved credentials from the browser or turn off the browser's auto-save feature. New passwords can be saved to the vault by allowing the extension to capture credentials when you log in to a secure site or by adding your username and password for any accounts listed in LogMeOnce's selection of supported websites.

Passwords: LogMeOnce allows an unlimited number of passwords to be stored in the vault and also allows multiple credentials to be saved for the same website. LogMeOnce includes a built-in password generator that can create passwords and evaluate their strength, which is measured by how many years it would theoretically take to "crack" the password. Additional features include the ability to autofill credentials into saved websites and to automatically change passwords for a selection of stable websites. The automatic password change feature is available as a separately installed tool and is not recommended unless you use the LogMeOnce service for all of your devices.

Multi-factor Authentication (MFA): In addition to the master password or "passwordless" login, LogMeOnce offers additional free authentication options via email code or the Google Authenticator app. Note that there is a charge for the option to authenticate via a code texted to your mobile phone.

Emergency Access: LogMeOnce allows users to designate one account beneficiary to receive access to all login credentials and up to five app beneficiaries to receive access to one specific website. You can specify start/end dates for when each account or app beneficiary should have access to your credentials. This feature also allows the LogMeOnce user to revoke a beneficiary's access at any time.

Account Recovery: In the event that you forget your master password, LogMeOnce includes a self-service "forgot password" feature that sends a reset link to your associated email address and requires you to correctly answer the security question chosen during account creation.

Ultimate Edition ($39/year): In addition to all of the features available in the free version, LogMeOnce Ultimate removes advertisements displayed in the password vault, offers additional multi-factor authentication (Photo 2FA), and allows an unlimited number of beneficiaries and shared passwords (free version only allows five shares).

Note: On the LogMeOnce dashboard, many features included only in the Ultimate (paid) edition are not hidden from the Premium (free) user. These Ultimate-required additions will prompt you to upgrade your membership, even though they appear available to use.