

High Security Accounts

To be stored in secure Hardware on OnlyKey.

Examples:

- Email accounts that are used to reset passwords.
- Accounts that if compromised would be devastating.

Enable two-factor authentication for each account on your OnlyKey.

Medium Security Accounts

To be stored in software password manager like Lastpass or use a shared password. Note: [review the tradeoffs](#).

Examples:

- Social media accounts
- Accounts that if compromised would be inconvenient.

Use two-factor authentication or SMS 2nd factor wherever possible.

Low Security Accounts

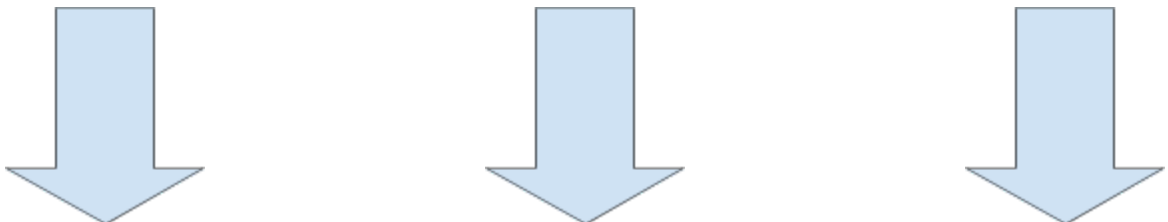
To be stored in software password manager like Lastpass or use a shared password. Note: [review the tradeoffs](#).

Examples:

- Random Forum Sign Up
- Accounts that if compromised you really could care less it would be a minor inconvenience.

Two-factor and SMS 2nd factor optional

* As mentioned in [article here](#) one of the slots of your OnlyKey can be used for a shared password or a password manager account.



What this looks like on your OnlyKey

Configure OnlyKey Slots



[cancel \[x\]](#)

OnlyKey Slot 6a Configuration

Label: Lastpass

UserName: Bob2345

Tab Return

Delay (0-9 seconds):

Password (up to 32 chars):

Re-enter Password:

Delay (0-9 seconds): 3

Options below are for two-factor authentication:

Tab Return

Google Auth OTP:

Options below only work with U.S. version of OnlyKey:

Yubikey OTP

U2F (Experimental)

[cancel \[x\]](#)

OnlyKey Slot 6b Configuration

Label: Shared

UserName: Bob2345

Tab Return

Delay (0-9 seconds):

Password (up to 32 chars):

Re-enter Password:

Delay (0-9 seconds): 3

Options below are for two-factor authentication:

Tab Return

Google Auth OTP:

Options below only work with U.S. version of OnlyKey:

Yubikey OTP

U2F (Experimental)