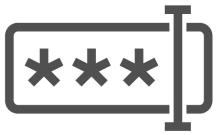
PASSWORD MANAGERS & TWO FACTOR AUTHENTICATION



Password Managers

Password managers generate and store strong, unique passwords for you. The most important thing to is to pick a well known password manager, and to use it! Begin with updating your old passwords and then consistently using the manager when creating new accounts.

Some common ones:

- 1 Password
  - https://support.1password.com/
- Last Pass
  - https://www.lastpass.com/
- Kee Pass
  - http://keepass.info/
  - https://play.google.com/store/apps/details?id=com.android.keepass
  - https://itunes.apple.com/us/app/minikeepass-secure-password/id451661808?mt=8
  - https://www.keepassx.org/downloads
- SpiderOak Encryptr
  - https://spideroak.com/solutions/encryptr

Two Factor Authentication

Using two factor authentication means that you will provide a service with your password and some kind of one-time code. That code can come from a SMS message that the service sends you, a special authentication app that you install on your phone, or a hardware token like a YubiKey.

- Facebook: https://www.facebook.com/about/basics/how-to-keep-your-account-secure
- Twitter: https://support.twitter.com/articles/20170388
- Google: https://support.google.com/accounts/answer/185839?hl=en
- Yahoo: https://help.yahoo.com/kb/SLN5013.html
- Outlook.com: https://support.microsoft.com/en-us/help/12408/microsoft-account-about-two-step-verification

- Yubikey: hardware tokens that you can buy online (for example from Yubico or Amazon) and can be used on many services above: https://www.yubico.com/start/

Find more services to enable two-factor authentication on: https://twofactorauth.org/