Two-Factor Authentication (2FA)

Do it Now

- Set Up 2FA for your most critical accounts:
  - Primary work email address (e.g. with employer)
  - Contact your IT department if you cannot configure
  - Primary professional email address (e.g. work-related gmail)
  - Primary personal email address
  - Google login(s)

Tip: Start with accounts you use most frequently

Consider setting up 2FA for other accounts

- Cloud storage accounts (e.g. iCloud, Dropbox, Box)
- Social accounts (Twitter, Facebook, Instagram, LinkedIn, Reddit, Snapchat)
- Financial accounts (Venmo, Paypal, Square, Mint.com, and other bank and credit card companies' sites)
- Communication applications (e.g. WhatsApp, Signal)
- Work-related or collaborative tools (e.g. Slack)
- Publishing accounts (e.g. Tumblr, Medium, Squarespace, Wordpress)
- Shopping accounts such as Amazon
- Older accounts, such as emails addresses you no longer use

Consider

- List out your accounts before you begin the 2FA process
- If you are most concerned about securing your financial accounts, call your bank and 2FA your financial accounts first
- If you are unsure which accounts allow 2FA, check this list
- If you store confidential information on certain devices, consider login / accounts associated with those devices
- If you are unsure of risks, consider engaging in threat modeling