2FA or not 2FA?

That is the question

Summary

Enable two factor authentication (2FA) on your primary email accounts

Set up a second 2FA

Test it!

Multifactor authentication

- Factor = something you ***know***, ***have*** or ***are***
  - passwords, hardware tokens, fingerprints, iris scan, …
- Improves security for your digital identity: one factor is not enough to log in
- 2FA (two factor) is becoming the norm

  Also called 2-step verification

"To improve security I used a two-factor authentication on my account: my social security number and my credit card number."

Why you should have 2 factor authentication?

- If you don’t use 2FA, anybody in the whole world who knows or guesses your password can take over your account.
- Compare: most banking uses it (card and pin)
- Even reduces your phishing risks (Google experience)

What identities should you protect?

Primary email accounts; used for password recovery

Most important external services: backups, Dropbox, customer database

(talk about the rest later)

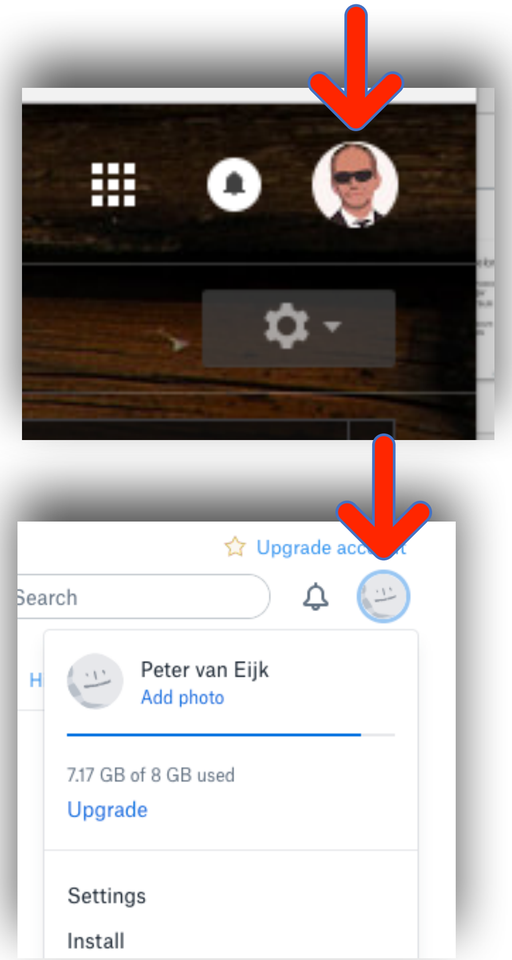
Factors to consider

- App on your phone (i.e. Google Authenticator, Authentiq ID)
- Hardware token (i.e. Yubikey)
- One time passwords
- Fingerprints, face recognition and eye scans (i.e. by your phone)
- Your computer/browser
- Another (email) account
- Security questions
- SMS/text. Not so secure against high profile targeted attack
  - … they all have their own risks

Where to find 2FA in popular services?

The convention these days is that your account is accessed through a profile picture on the top right of your screen

- Gmail: Google Account -> Sign-in and security -> 2-Step Verification
- Hotmail/Outlook/Live/Office 365: View Account -> Security and privacy -> More security settings
- Dropbox: Account settings -> Security



Risks for second factors

Consider these risks, to make sure that you can recover when any of these happen:

- Lose primary computer
- Lose phone
- Lose hardware key
- Forgot password
- Forgot recovery question
- Your online password manager stops working

Rank these in decreasing probability

If you are really paranoid, consider how to recover from two simultaneous losses

Too many passwords?

Use this process for your most important accounts, less than a handful

For other accounts, use a password manager, such as LastPass, Keeper, 1password, Dashlane, or any other, in combination with random, unique passwords per service

Every service will have a password like `7BedN6Rvrh9dt5x`

Worksheet

	What is it?	Your example
User ID	Your digital identity	phaedrus@gmail.com
First factor	Primary means of logging in	Password memorised
Second factor	Second factor, regularly used	Yubikey
Additional second factor	Second factor in case you lose your primary second factor	Soft token (i.e. Google Authenticator on phone)
Recovery process	How you would recover from forgetting your password	Security question

Your assignment

Set it up for you main email

Document it in the worksheet

Try logging in on a different computer

If you are scared, try it on a fresh account first