THIS IS WHERE WE WRITE THE MEETING FLAG ON THE BOARD

this slide is here so we don’t forget

Intro Opsec

Slides by Josh Park & Ian Klatzco, Presented by Thomas Quig FA20

What is “operational security”?

- **the art of not screwing up**
- **or, how to do an illegal and get away with it**

- Threat Modeling
- Compartmentalization
- Rotation (credentials)
- Security Fatigue

- You’re the CIA
- You’re the CISO of an org
- You are a drug dealer
- You’re a student at UIUC

Threat Modeling

- ranking your threats and allocating resources accordingly

- in other words, don't waste time on the small stuff

Compartmentalization

- Don’t link your accounts. Don’t stay logged into everything.
- Keep high-value targets separate from low-value targets
- If one account gets compromised, it’s less likely that more accounts will go down with it

Rotation

- Updating your passwords with some frequency
- Creating new identities / swapping out old ones
- University-enforced password changes

You're the CIA

- You are an agent in $INSERT_UNFRIENDLY_COUNTRY
- You are collecting intel
- Being caught means prison, potentially execution
- Solutions:
  - Don't do anything that draws attention to you.
  - Read 73 Rules of Spycraft.
  - Other required reading. grugq

You're the CISO of an organization

- Is every one of your employees using a Chromebook, iPhone to access all of their accounts?
- And they NEVER use their work devices for personal stuff?
- Can you really trust Doris from accounting to not open an email from FREE ROYAL CRUISE TICKETS at 6pm on a Sunday on her work email?
- Make sure your team has proper Opsec

You’re a drug dealer

- Drug dealing is very illegal
- Buying drugs is also very illegal
- Several local, national, and international agencies out to get you
- Don’t do any transactions publicly.
  - Venmo chal
- Anything on your phone will be used in a court case against you.

You're a student at UIUC

- Use end-to-end encrypted messaging apps for the important stuff
  - (Signal) (WhatsApp, Telegram are **iffy**)
  - See **sms** challenge
- Use a reputable VPN that you pay for, for illegal stuff
  - Don't do illegal stuff
  - Use the school VPN or Algo
- Schedule deletion — delete your old stuff — **Find something embarrassing** chal

So what can you do? (without getting fatigued)

- Use a password manager (LastPass, KeyPass) - Password Manager chal
- Use randomly-generated passwords
- Use a good ad blocker, script blocker - Safe Browsing chal
    - (uBlock Origin, HTTPS everywhere, Privacy Badger)
- Separate email accounts or computers for important and non-important (compartmentalize)

Security Fatigue

- Problem: platitudes and being overwhelmed
- Diminishing returns (see: Threat Modeling)
- eg: randomly generated passwords: pain on mobile

Problems with Tor: “use signal/use tor”

- Tor traffic is really really visibly Tor traffic.
- It requires using a fork of Firefox which doesn’t have Firefox’s engineering effort, so browser is not secure (we’re talking arbitrary JS, HTML RCEs that result in malware on your machine).
- Signal only encrypts messages to other Signal users. It can replace your default SMS/MMS app, but will still send unencrypted messages to non-Signal users

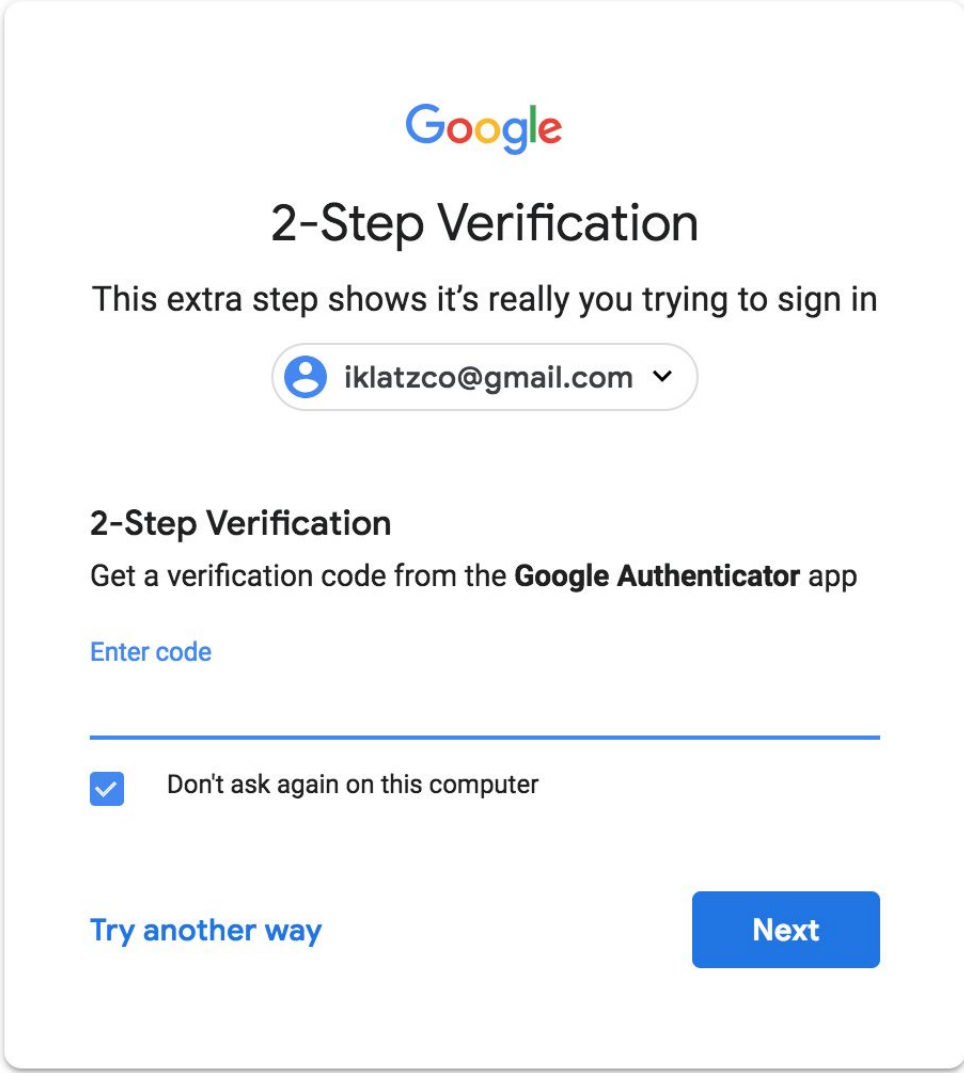
Personal Data = Radioactive Waste (Maciej Ceglowski)

- Easy to generate and store in the short term
- Almost impossible to dispose of
- Requires very long term planning to manage
  - What will happen to data from Twitter/Facebook in 5+ years?
- See challenge: **Find something embarrassing**

2FA

See challenge **Enable 2FA.**

What happens if you lose your phone? You send them your ID.



Types and pitfalls of 2FA

- SMS
  - Way better than nothing, still susceptible to “SIM Swapping Attack”
- App Based
  - Could still phish your 2FA code
- Yubikey
  - Strongest form of 2FA, but be careful you could still be phished (believe it or not).

Edit, then delete

See challenge **Delete your account.**

- Many websites will continue to store all your data after you delete your account.
- Sometimes you can defeat them by editing first, then deleting your account.
- There are entire toolsets to do this (eg reddit)

Compartmentalize

What matters, what doesn’t

- Password complexity
- Virtual Machines

Password Priority

What matters, what doesnt.

Banking, vs Burner

Identity and Access Management

I have a personal discord server.

Don’t give up.

It’s easy to get depressed when you learn about or work in security.

Watch out for the slippery slope fallacy — just because one thing is bad doesn’t mean we should stop trying to make things better (voting records & birthdates).

other fun resources

- CIA guide to pokemon go
- how to master secret work
- moscow rules
- more grugq more grugq