

Week 05

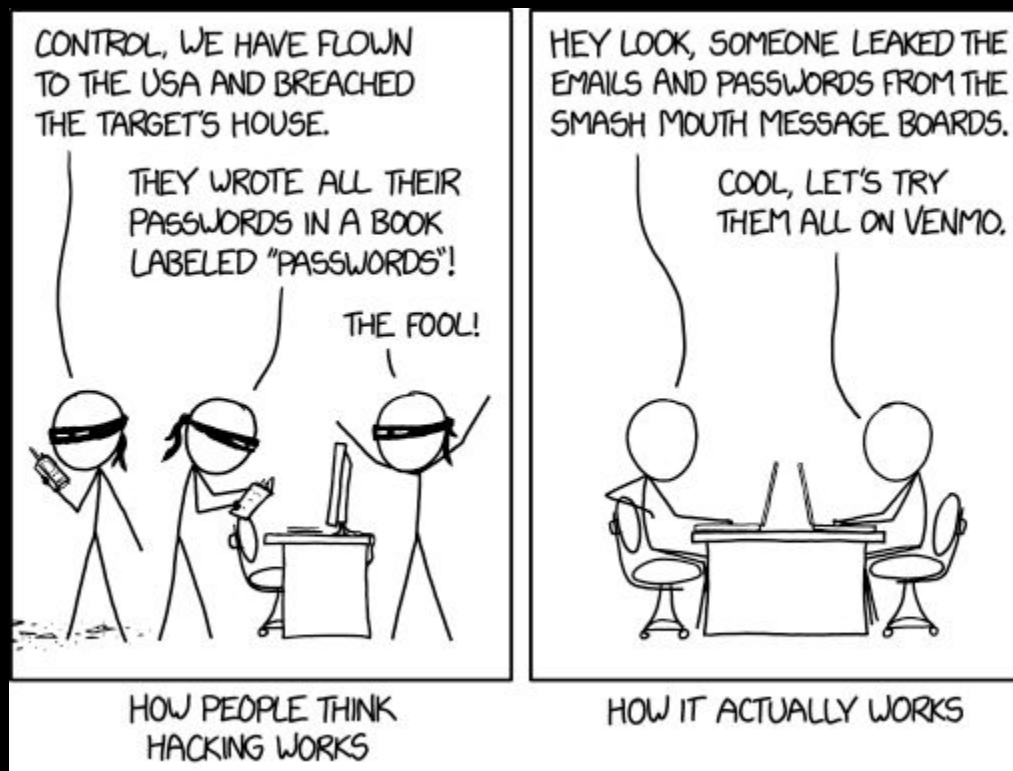
Opsec

(Operational Security)

Slides By: Thomas Quig



sigpwny{dont_do_dumb_stuff}



Announcements

Pwny Server is under my (Thomas) bed right now

Minecraft Server @ mc.sigpwny.club (verify on Discord)

Fall Recruitment Date Locked! Looking For Sponsors



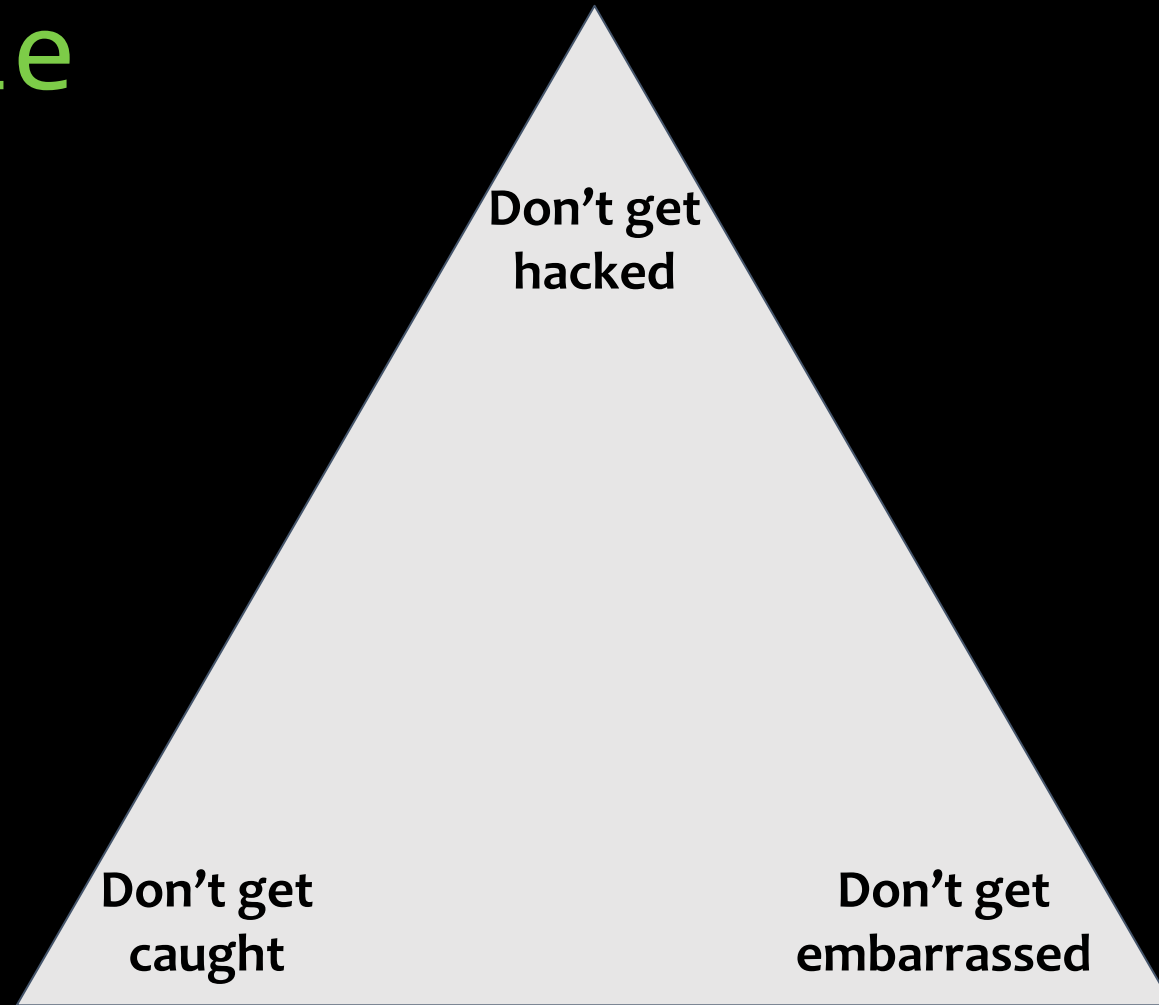
Operational Security

“A process that identifies critical information to determine if friendly actions can be determined by enemy intelligence”

Managing your own personal security and privacy.



The OPSEC Triangle



Don't Get Hacked

This one is definitely important



Not getting hacked 101 - People

- Passwords
 - Random generator or really strong pattern
 - Never Reuse!!!
- Password Manager
 - Allows for random password generation
 - Chrome Default uses Reversible Encryption!
- MFA
 - 2FA is Good, SMS is better than just password but still weak
 - Yubikey >= App-Based > SMS > Just Password
- Awareness
 - “Don’t click on links” is a dated term

Challenges: Password Manager, Enable MFA, Upgrade MFA



Not getting hacked 101 - People

- Passwords
 - Random generator or really strong pattern
 - Never Reuse!!!
- Password Manager
 - Allows for random password generation
 - Chrome Default uses Reversible Encryption!
- MFA
 - 2FA is Good, SMS is better than just password but still weak
 - Yubikey >= App-Based > SMS > Just Password
- Awareness
 - “Don’t click on links” is a dated term

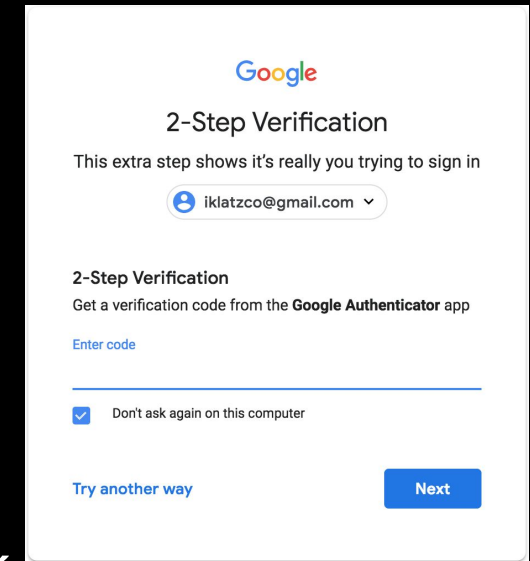
Challenges: Password Manager, Enable MFA, Upgrade MFA



Not getting hacked 101 - People

- Passwords
 - Random generator or really strong pattern
 - Never Reuse!!!
- Password Manager
 - Allows for random password generation
 - Chrome Default uses Reversible Encryption!
- MFA
 - 2FA is Good, SMS is better than just password but still weak
 - Yubikey >= App-Based > SMS > Just Password
- Awareness
 - “Don’t click on links” is a dated term

Challenges: Password Manager, Enable MFA, Upgrade MFA



The screenshot shows the Google 2-Step Verification interface. At the top is the Google logo. Below it, the text reads "2-Step Verification" and "This extra step shows it's really you trying to sign in". A dropdown menu shows the email address "iklatzco@gmail.com". Below that, it says "2-Step Verification" and "Get a verification code from the Google Authenticator app". There is an "Enter code" label and a text input field. A checkbox is checked with the text "Don't ask again on this computer". At the bottom left is a link "Try another way" and at the bottom right is a blue "Next" button.

You can still be phished!



Not getting hacked 101 - People

- Passwords
 - Random generator or really strong pattern
 - Never Reuse!!!
- Password Manager
 - Allows for random password generation
 - Chrome Default uses Reversible Encryption!
- MFA
 - 2FA is Good, SMS is better than just password but still weak
 - Yubikey >= App-Based > SMS > Just Password
- Awareness
 - “Don’t click on links” is a dated term

Challenges: Password Manager, Enable MFA, Upgrade MFA



Not getting hacked 101 - People

- Passwords
 - Random generator or really strong pattern
 - Never Reuse!!!
- Password Manager
 - Allows for random password generation
 - Chrome Default uses Reversible Encryption!
- MFA
 - 2FA is Good, SMS is better than just password but still weak
 - Yubikey >= App-Based > SMS > Just Password
- Awareness
 - “Don’t click on links” is a dated term

Challenges: Password Manager, Enable MFA, Upgrade MFA



Not getting hacked 101 - Orgs

- Segmentation
- Awareness training
- Make sure all org members themselves have good OpSec
- Technical Solutions



Safe Browsing

- AdBlock
 - ublock origin
 - no downside
- Script Block
 - noscript
 - makes internet less pretty



Not getting hacked 101 - Orgs

- Segmentation
- Awareness training
- Make sure all org members themselves have good OpSec
- Technical Solutions



Don't Get Embarrassed

Important for some people



The Three “Online Identity Models”

- You don't exist
 - Randomized accounts for every platform
 - No indication of who you are, watch your content
- You don't care
- You are a celebrity



The Three “Online Identity Models”

- You don't exist
- You don't care
 - Most people do this one
 - Society is becoming more accepting of this one
- You are a celebrity



The Three “Online Identity Models”

- You don't exist
- You don't care
- You are a celebrity
 - Good for recruiters, protects against impersonation
 - Watch what you say, really strong “Don't Get Hacked” measures



Don't Get Caught

If you are worried about this, you may already be too far gone



Personal Data = Radioactive Waste

- 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?

Challenges: Find something embarrassing, Delete Your Account



Secure Communication

- Use end-to-end encrypted messaging apps for the important stuff
 - (Signal) (WhatsApp, Telegram are iffy)
- Use a reputable VPN that you pay for, for illegal stuff
- Don't do illegal stuff

Use the school VPN or Algo

Challenges: Signal



If you get caught

Know your rights

Know the law

GET A LAWYER
SHUT THE HELL UP



Privacy

- Lock down your accounts
- Minimum access
 - Does everyone need to see your LinkedIn
- Create an “Asset / Identity Map”

Challenges: Private Payments



Edit Before Deleting

- 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)

Challenges: Delete Your Account



General Tips

Am going to speed through these so we can do challenges.



Overlap

A Lot of these things apply to all sections of opsec

- Three Identity Models, Personal Data = Radioactive Waste, Awareness etc...

Think about how advice from one thing can be applied elsewhere



Risk / Threat Modeling

- Who are you?
 - International Espionage Agent
 - Drug Dealer
 - Student, Security Researcher
 - DevOps at _____ Big Tech
- What are actual threats to you? Don't waste time on small stuff
- Make a model!
 - Spreadsheet
 - Graph, drawing, etc...



Risk / Threat Modeling

- Who are you?
 - International Espionage Agent
 - Drug Dealer
 - Student, Security Researcher
 - DevOps at _____ Big Tech
- What are actual threats to you? Don't waste time on small stuff
- Make a model!
 - Spreadsheet
 - Graph, drawing, etc...



Risk / Threat Modeling

- Who are you?
 - International Espionage Agent
 - Drug Dealer
 - Student, Security Researcher
 - DevOps at _____ Big Tech
- What are actual threats to you? Don't waste time on small stuff
- Make a model!
 - Spreadsheet
 - Graph, drawing, etc...



Risk / Threat Modeling

- Who are you?
 - International Espionage Agent
 - Drug Dealer
 - Student, Security Researcher
 - DevOps at _____ Big Tech
- What are actual threats to you? Don't waste time on small stuff
- Make a model!
 - Spreadsheet
 - Graph, drawing, etc...



EOTW / SHTF Plans

What happens when the world ends / Sh*t hits the fan

Your world ending != the world ending

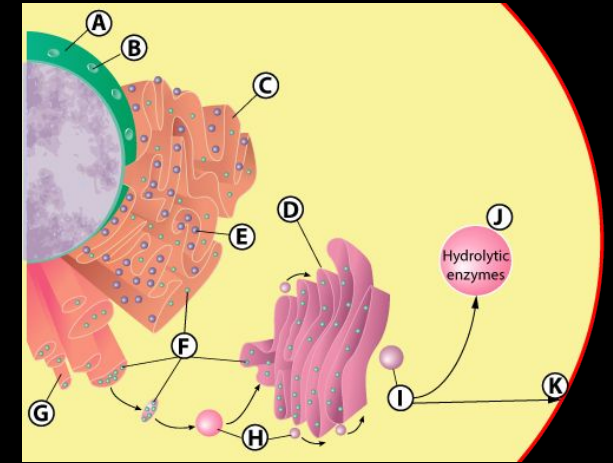
- Go Bag
- Cash
- Backups



Compartmentalization

Have different emails with **different purposes**

- Informal Emails
- Professional Email
- Security Email
- That one old yahoo email you still haven't deleted.



Have multiple roots of trust (run an SMTP on your own domain)

- 100% all about your threat model



Rotation

Rotate passwords occasionally

Rotate identities



Security Fatigue

This is tiring

Diminishing returns

Security vs Convenience (i.e. Random Passwords & Mobile)



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).



Next Meetings

Sunday Seminar: Crash Course on Law and Ethics

- Standard ethical models for security
- How to ethically report a vulnerability
- How NOT to get arrested

Next Thursday: Intro to Reverse Engineering

- Learning tools for how to reverse engineer code
- Binary Reversing
- Ghidra, Ida, r2, disassemblers, etc

