

# OPERATIONAL SECURITY



PROTECTING MY PC

---


DIMITRIS LAMPRINOS



WHY SHOULD I HEAR YOU?  
(AGAIN)

1

## CRITICAL DATA

- X {Web banking, Facebook} credentials?
- X High sensitivity mails?
- X Private files that we don't want to share?
- X Our browsing history?
- X Closed source projects?
- X Our digital signature (GPG)?
- X Cryptocurrency private keys?
- X Inappropriate Photos 



WHAT IS OPERATIONAL SECURITY?



## OPERATIONAL SECURITY

- X OPSEC originated as a military term
- X Prevent potential adversaries from discovering critical operations-related data.
- X Five step process:
  1. Identify critical information
  2. Determine threats
  3. Analyze vulnerabilities
  4. Assess risks
  5. Apply appropriate countermeasures



2.

## THREAT MODEL

PROCESS BY WHICH POTENTIAL THREATS CAN BE  
IDENTIFIED, ANALYZED AND PRIORITIZED



What are we getting protected from?

Can be



Friends and Family, Ex Girlfriend

Non targeted attacks

Targeted attack for industrial  
espionage

Government



## GAINING ACCESS

- X Full online identity theft
- X Persistent Threat:
  - Full logging
  - Access even to end-to-end encrypted data
  - Modify everything is being sent to you
  - Modify everything is being sent from you
  - (Incrimination?)
- Botnet





## SOME OF MY PRACTICES (PARANOID LEVEL: 1)

- X Passwords
  - Different passwords
  - At least 10 digits
  - Non vulnerable to dictionary attacks
- X Locking my laptop
- X Updates
- X Antivirus
- X Cover my camera



## SOME OF MY PRACTICES (PARANOID LEVEL: 2)

- X 2 Factor authentication
- X Change passwords frequently
- X Email on every login from another device
- X Run suspicious code or executables as another user
  - Github repositories that are not well established
  - Packages (pip, npm) can be uploaded from everyone
- X Avoid plugging untrusted USB devices
- X Login pages only via HTTPS



## SOME OF MY PRACTICES (PARANOID LEVEL: 3)

- X Avoid closed-source projects in my PC
- X Leaning the lid every time I enter my password
- X Run suspicious code or executables on Virtual Machine
- X Never download files via HTTP (prefer self-building code)
- X Linux
- X Use Full Disk Encryption
- X Consider my phone compromised



## SOME OF MY PRACTICES (PARANOID LEVEL: 4)

- X Consider my computer being a microphone
- X Shred when deleting important files (man shred)  
So they cannot be recovered
- X Make sure my PC is unique, so I cannot get tricked by a cloned PC (e.x. unique stickers)
- X Bounty games



WHAT IS MY PARANOID LEVEL?







# THANK YOU!

You can find me at  
@pkakelas

<https://pkakelas.com>

GPG: 5456 5COE 57FA 7A55 AB49 COD1 65E3 D29D 92B4 1043