Finding Your Path in Information Security in the AI Era

Anant Shrivastava

What we want?

- Money (lots of $$$$)
- Fame (followers / likes / comments)
- Stability (9-5 job; 5-9 family and friends)
- Curiosity (interesting but why and how)

Infosec != Hacking

- Infosec = not just hacking, but many domains
- AI makes the path both easier and harder

Refer: https://blog.anantshri.info/cybersecurity-passion-or-profession

Title : Hacker's Manifesto

Author : The Mentor

```
                                ==Phrack Inc.==

                        Volume One, Issue 7, Phile 3 of 10

=-=-=-
```

What is Infosec

Information Security is a field where we focus on securing the information. The protection could be from malicious attackers or simply unintended tampering/access of data.

In short

- keep the bad out
- let the trusted in
- give trusted access to
  - what they are authorized to access
  - when they need the access



Hackers vs Adversaries

- Hacker = curiosity + mindset
- Adversary = resources + mission
- InfoSec sits between them

Reference : https://blog.anantshri.info/hacker-vs-adversary

Enter AI: Rapid Growth

LLM, RAG, vibe coding, agents

AI hype vs. real disruption

Everyone experimenting

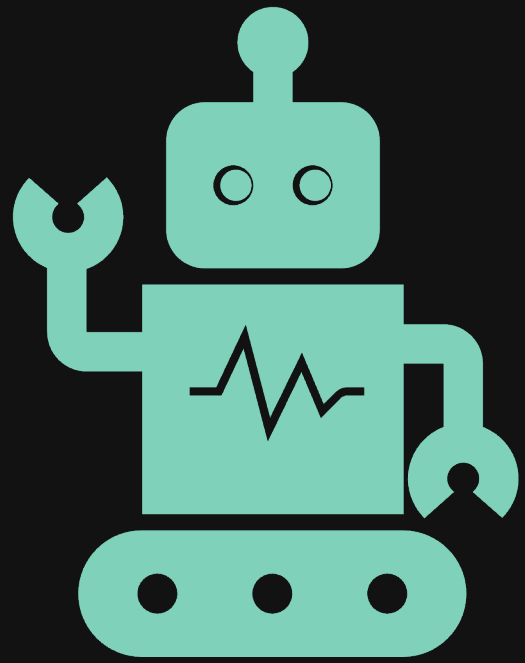
Infosec in the AI Era

- What hasn't changed:
  - Protect data
  - Manage risk
  - Verify access
- What has changed:
  - speed negates the need for efficiency
  - AI-powered attacks (phishing, malware, deepfakes)
  - Security of AI systems themselves
  - Attack surface is exploding



Common Student Questions

- How do I survive in this new era?
- How do I adopt AI safely?
- What cautions should I keep in mind?
- Do I still need to learn coding?



Core Skills for the Digital Age

- Variable speed reading
- Typing speed
- Sustained focus
- Critical thinking & problem solving (trouble shooting)

Refer: https://blog.anantshri.info/mastering-the-essential-skills-for-the-digital-age

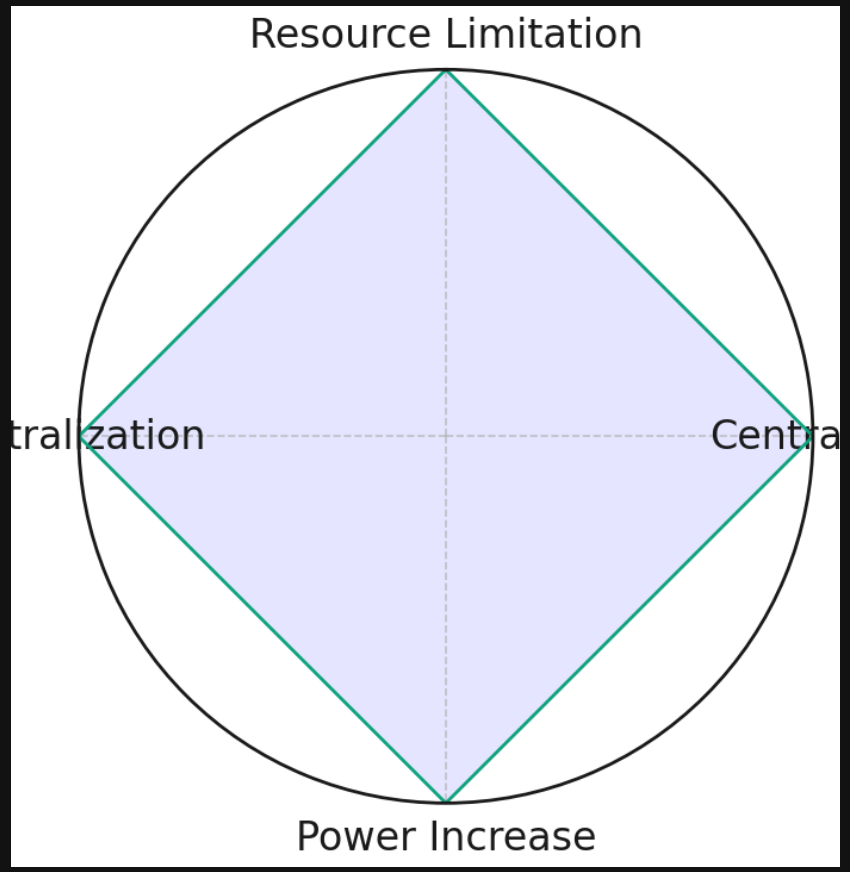
Why Troubleshooting Matters

- Survival skill, not bonus
- Rebuilding ≠ understanding
- Calm + systematic = resilience
- Automate after solving

Refer: https://blog.anantshri.info/troubleshooting-the-survival-skill-we-forgot-we-needed

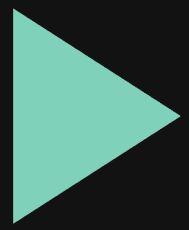
Cycles of Computing

- Centralize → decentralize → repeat
- From mainframes → PCs → cloud → edge → AI
- Adaptability is the constant

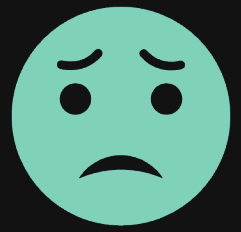


Refer: https://blog.anantshri.info/flip-cycles-of-computing

From SPOF to Linchpin



Start: become indispensable

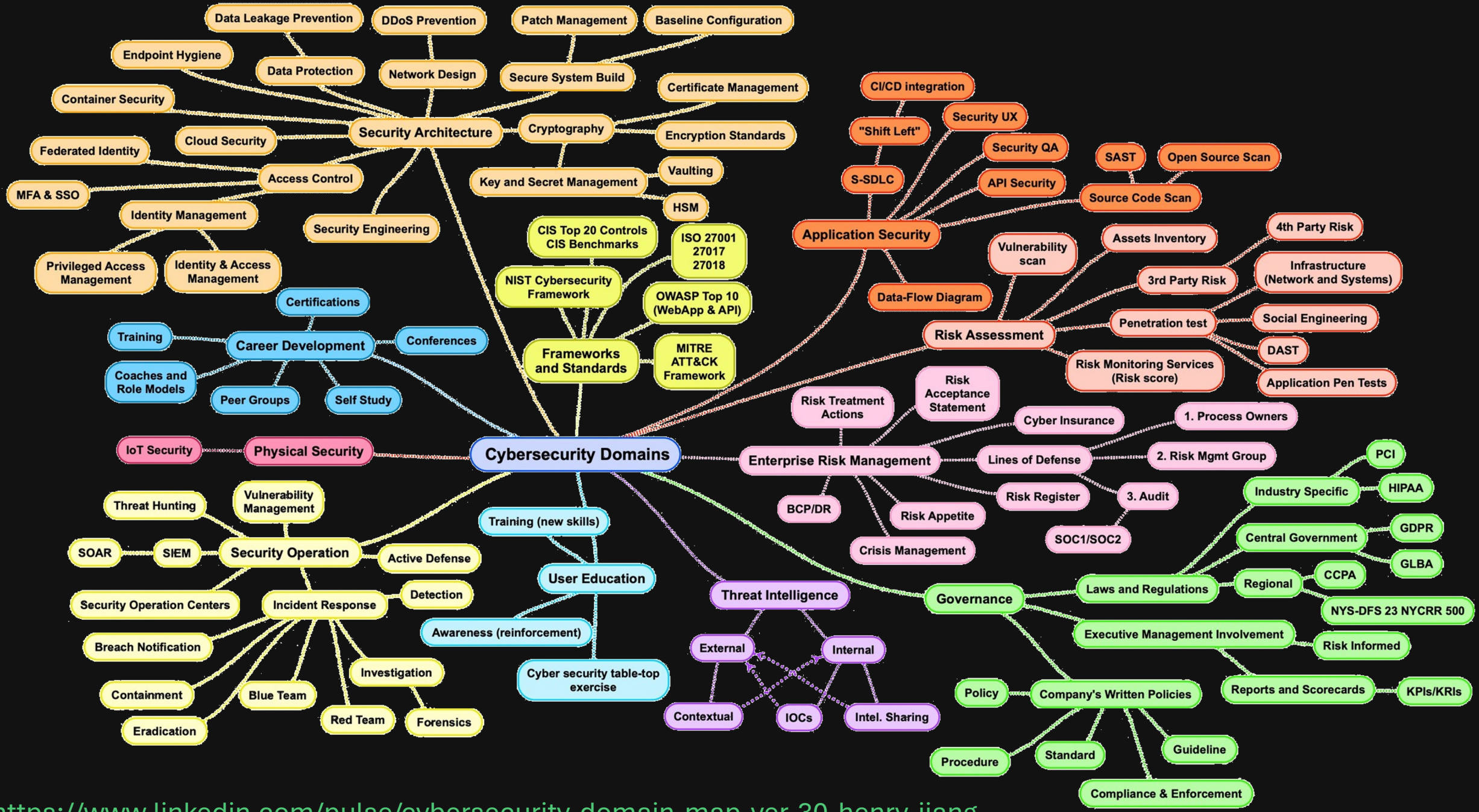


Danger: stuck as Single Point of Failure (SPOF)



Growth: document, automate, and move on

Refer: https://blog.anantshri.info/from-spof-to-linchpin-how-to-grow-without-getting-stuck



https://www.linkedin.com/pulse/cybersecurity-domain-map-ver-30-henry-jiang

Career Maze Choices

Startup = rollercoaster

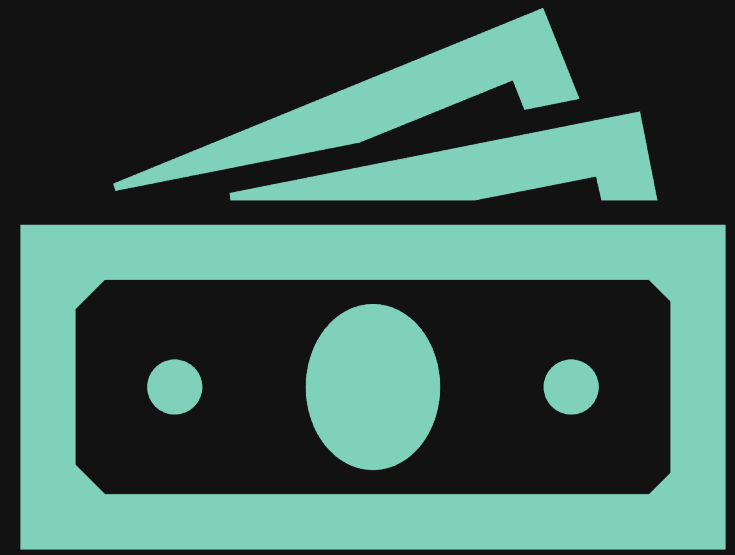
Corporate = carousel

Entrepreneur = carve your own lane

Refer: https://blog.anantshri.info/startups-vs-corporates-unblurring-the-lines-for-job-seekers

Financial Awareness

- AI + Security roles = pay high + volatility
- Startups = high pay, high risk (“golden cuffs”)
- Corporates = stable pay, benefits, slower growth
- Startups may pay less, offset with ESOPs
- Rule of thumb: save first, spend later
- ESOPs ≠ guaranteed cash
- Build financial resilience → career flexibility



Lets Talk Money : Monika Halan : https://amzn.to/3VhY2NE

Approach



Resume: highlight AI + security projects



Online presence: blogs, GitHub, talks



Certifications: useful, but not everything



Build on Fundamentals

Leverage AI, Don’t Be Leveraged

AI = tool, not master

Amplifies strengths AND weaknesses

Keep human steering

AI as a Helping Hand



Great for:

Drafts

Brainstorming

Exploration



Weak at:

Truth

Compliance

Edge cases

Core Skills for the AI Age

Variable speed reading : AI is able to generate data at rapid pace. you should be able to consume it.

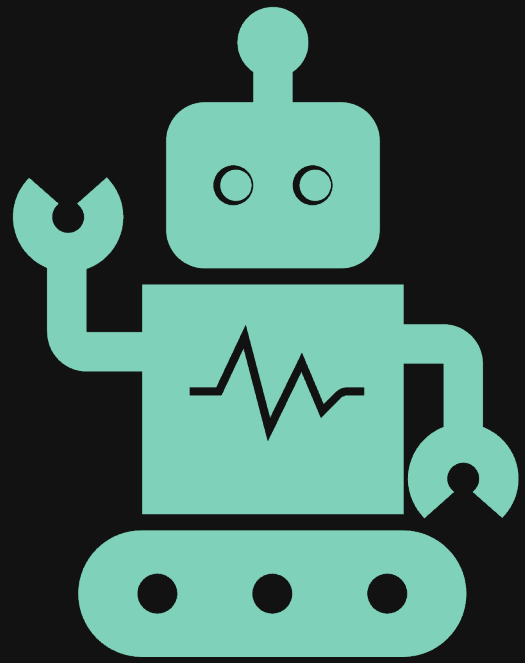
Typing speed : Converting your thoughts to input for AI

Sustained focus : Being able to sit through sessions with AI

Critical thinking & problem solving (trouble shooting) : When the non deterministic system does non deterministic things

Common Student Questions

- How do I survive in this new era?
- How do I adopt AI safely?
- What cautions should I keep in mind?
- Do I still need to learn coding?



How do I survive in this new era?



BUILD ON **CORE SKILLS** (READING, TYPING, FOCUS, TROUBLESHOOTING)

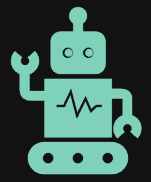


STAY ADAPTABLE: TECH CYCLES ALWAYS FLIP



BUILD FINANCIAL RESILIENCE → FREEDOM TO PIVOT

How do I adopt AI safely?



AI as a **tool, not a master**



Cross-check outputs - don’t trust blindly



Use AI for productivity, not for shortcuts in judgment



Learn how to communicate: Prompt Engineering

What cautions should I keep in mind?

AI will hallucinate → verify everything

Over-reliance creates dependency debt

Don’t ignore fundamentals (security basics, logic, systems)

Do I still need to learn coding?



Yes — not to out-code AI, but to *guide* it



Coding = understanding logic, debugging, and catching AI's mistakes



Helps bridge gaps between business, tech, and AI tools



become an engineer not a code typing assistant (use ai for that)

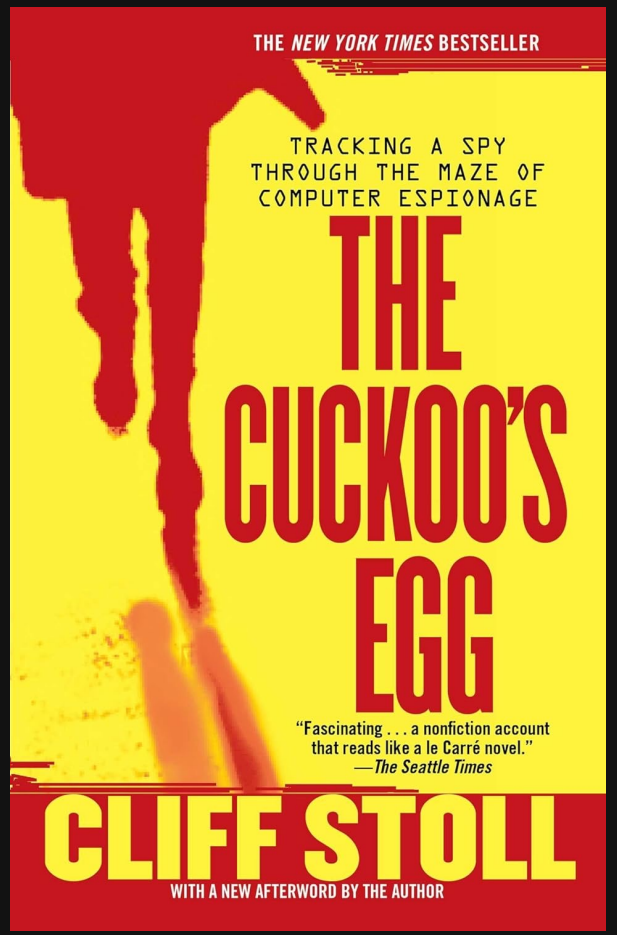
Resources

- https://freestuff.dev
- https://free-for.dev/
- https://www.vulnhub.com/
- https://pwnedlabs.io/
- https://www.hackthebox.com/
- https://tryhackme.com/
- http://www.hacker.org/
- https://sadservers.com/ (defensive)

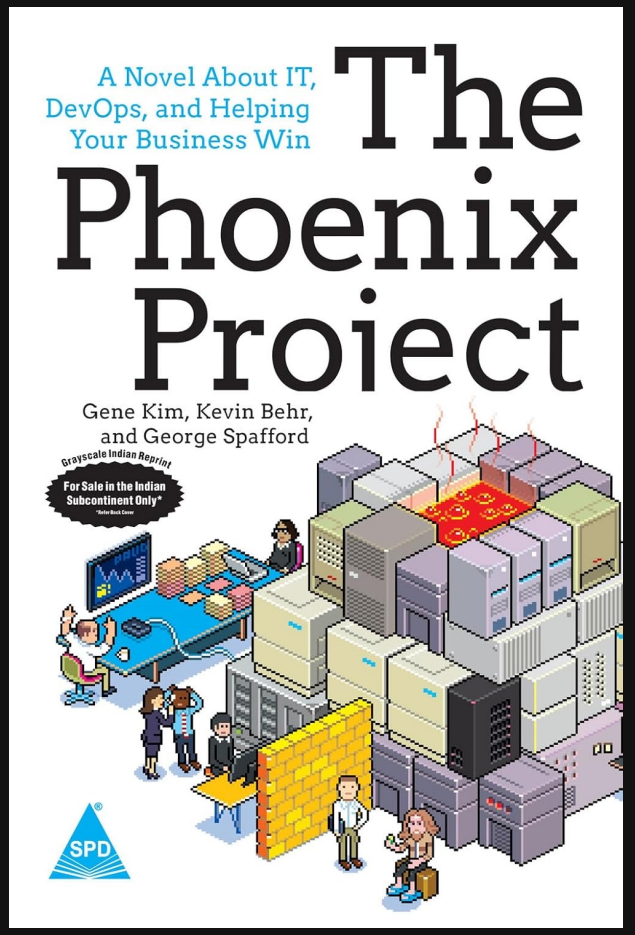
Resources

- Github Student Pack
https://education.github.com/pack
- 1 Free ebook everyday
https://www.packtpub.com/free-learning
- Resources Free for Developers
https://free-for.dev/
- Winter of Code
https://winterofcode.com
- Summer of Code
https://summerofcode.withgoogle.com

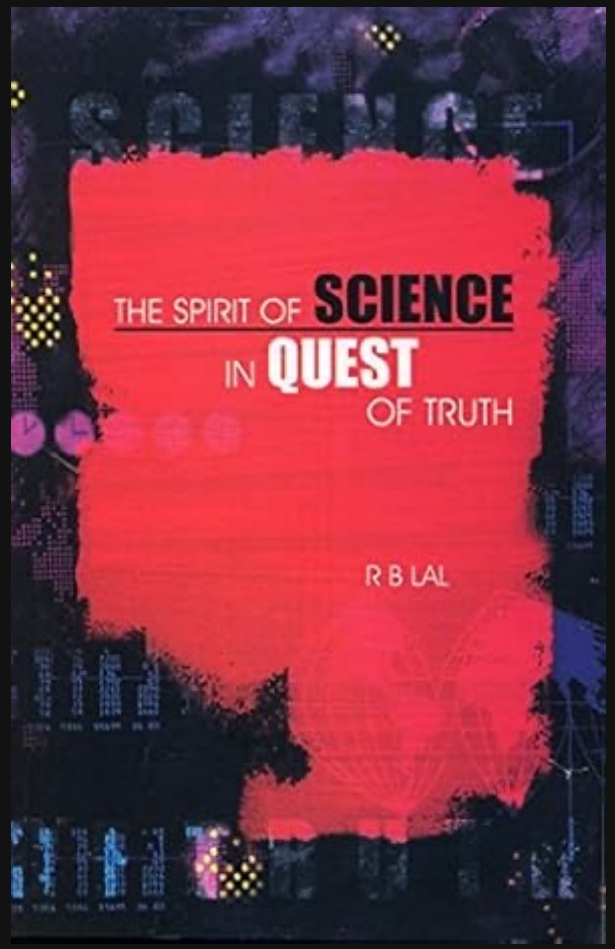
Book Reading Resources



https://amzn.to/4pnSHlP



https://amzn.to/4n711Vd



https://amzn.to/4n5ATdk

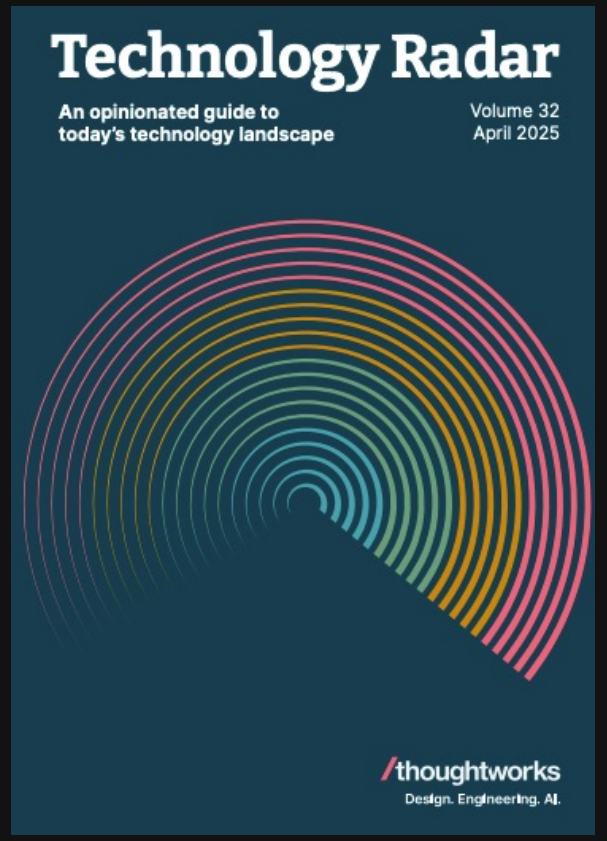
Online Magazines



https://phrack.org/



https://pagedout.institute/



https://www.thoughtworks.com/radar

Principles to Carry Forward

Learn to question everything	Be expert in one field, but also gain generalist breadth	Remember: security supports business needs	Form groups of like-minded people
Secure your own system and network first	Avoid calling yourself a “Hacker” too early	Self-proclaimers are not respected in security communities	Let your work speak louder than your words

Closing



Hacker = mindset, not job title



AI = your latest playground



Core skills + adaptability + curiosity = growth

Thanks for Listening



https://blog.anantshri.info/career-notes-references