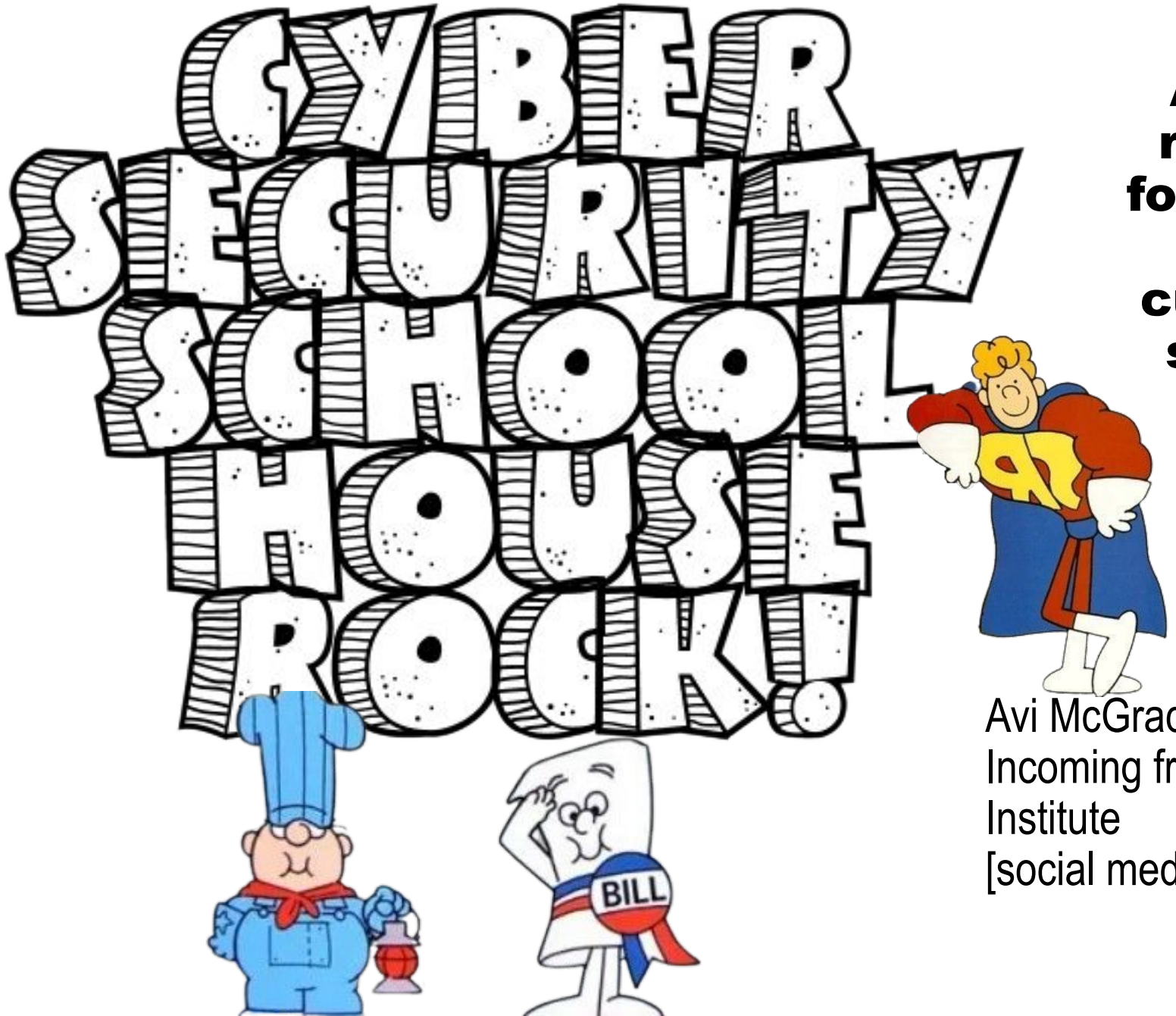

A framework and recommendations for a comprehensive cybersecurity curriculum for K-12 schools in the US

Avi McGrady
Incoming freshman, Rensselaer Polytechnic Institute
[social media handle(s) here]

Who, what, why?

- I recently graduated from New Vista High School in Boulder, CO
- Longstanding interest in cybersecurity and everything hacking
- There were no opportunities offered within reach, so I began mentoring from a longtime connection
- Recognize this is a problem nationwide in the K-12 school system
- Created a culminating project (grad requirement) to put a spotlight on the problem locally.
- Pushed our school district to adopt curriculum and incorporate cybersecurity at all grade levels

Why cybersecurity in schools?

- catastrophic ransomware attacks waiting to happen
- Increasing adoption of educational technology (“EdTech”)
- Students spend more time on screens than any other activity
  - Most kids have multiple devices
- Students, teachers, staff, parents are all potential targets
- The problem of cybercrime grows every year with no end in sight
- By neglecting this we are actively sabotaging the future generation of professionals.

Widespread problems

- Scams and phishing targeting very young kids
- Cyberbullying, harassment, and online taunting
  - Extortion and nonconsensual image sharing
  - Generative AI images making the problem exponentially worse
- Malware embedded in pirated software or spread through chats or social media
- Credit card or payment fraud
- Deep misunderstanding about fundamental principles of internet privacy and security

Highlights from Beau Woods interview

- Beau Woods is the CEO and founder of Strategos security, a cybersecurity firm that covers a variety of different services.
- Beau advocates for a more thorough cybersecurity education instead of the surface level “Don’t click on things.” He thinks that some degree of curriculum should be initiated earlier in the education chain.





Highlight from Josh Corman interview

- Joshua Corman is the founder of I Am The Cavalry, a grassroots organization focused on where bits and bytes overlap flesh and blood. He previously held the position of chief strategist in CISA's COVID Task Force, offering guidance on the pandemic response, contributing cybersecurity knowledge to healthcare infrastructure, and assisting with control systems and life safety projects.
- During our interview, he gave his perspective about some of the topics in my project. He thinks there should be a lot more support for cybersecurity education for people who aren’t necessarily interested in pursuing information security, and that there is a massive disparity of talent in general.
- Another point he touched on was that security hits on every part of an organization, so everyone should be involved instead of exclusively the security department.





What's missing in school curriculum?

- Basic online privacy/safety and what not to disclose online
- Password fundamentals, password managers, MFA
- Instruction in cyber ethics and being a good cyber citizen
- Not just warnings, but explanation why pirated software is risky
- Online risk analysis and harm reduction
- How various forms of cybercrime appear: phishing, malware, fraud, disinformation, bullying, harassment, ransomware
- Understanding consequences, social media history, and how your online presence (good or bad) will follow you through life

A blueprint for US school districts

- Curriculum must happen in all grade levels, every year
- Training in age- and developmentally-appropriate subject matter
  - K-5: what is private information and why you shouldn’t share it
  - K-8: what does online bullying look like and how to respond
  - 3-8: “When it seems too good to be true, it probably is”
  - 6-12: Socializing safely in online communities
  - 6-12: What is executable code and how can it harm you?
  - 9-12: Phishing and fraud online, password management

What programs work well for kids

- Capture the flag events, cybersecurity clubs
- Local conferences (BSides)
- Online programs like HackTheBox, TryHackMe, SANS
- Internships, mentoring, community outreach and volunteer work

What works well for schools and districts

- CISA cybersecurity guidelines for schools
- Department of Education Government Coordinating Council for the Education Facilities Subsector (blech name, important group)
- Participating in US Cyber Games / Cyberpatriot competitions
- NIST Cybersecurity education and games for K12
- Career counselors and ambassadors
- Apprenticeships and internships

We also need cyber-smart legislators

- State boards of education set statewide curriculum requirements
- School district boards fund local initiatives and can reallocate resources to make opportunities available
- State representatives and senators can push for laws and funding to encourage and support these efforts
- Congress, and agencies like CISA and Dept. of Ed, support high-level training and resources
- …which is one reason we need to elect more hackers at all levels of government, because we understand what we need.

Summary

- K12 cybersecurity training builds resilience against cybercrime in the wider population
- There is a deep need for workforce development in cybersecurity, and a population of kids hungry to get into this industry
- Public school systems are the perfect venue to teach these skills
- Schools themselves are targets for cybercrime, and often are poorly resourced to protect their sensitive data and systems
- Developmentally-appropriate cybersecurity instruction is vital to taking a dent out of our society-wide cybercrime problem

Questions?

- How to contact me
  - https://mastodon.social/@hyenaa
- xmechanica@protonmail.com