Avi McGrady
Rensselaer Polytechnic

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



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



bitly

3:25:00 for my segment

Why cybersecurity in schools?

- Lack of training creates vulnerable individuals
- Increasing adoption of educational technology ("EdTech") adds attack surface
- 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 to teach these important life skills, we actively sabotage future generations







Widespread problems

- Scams and phishing targeting very young kids
- Cyberbullying, harassment, and online taunting
  - Extortion, stalking, 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



A more thorough cybersecurity education, not just surface level “Don’t click on things.”

Some curriculum should be initiated earlier in the education chain.

Training in stages, revisiting topics when kids get older.

Highlight from Josh Corman interview

There should be a lot more support for cybersecurity education for people who aren't necessarily interested in pursuing information security

There is a massive disparity of talent, in general.

Security touches every part of an organization, so everyone in an organization should be involved in securing that organization, not exclusively the security or IT team.



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 to the victim**: 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**: "When it seems too good to be true, it probably is"	**5-8**: what does online bullying look like and how to respond	**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



K-5: Private information and intro to online safety

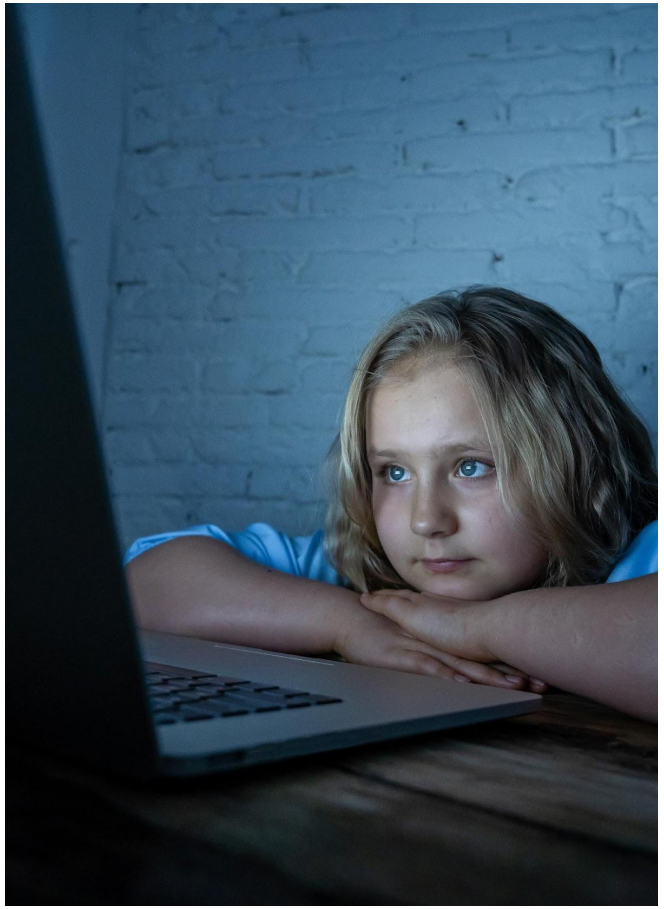
- Private information is a great introduction to cybersecurity for younger kids
- Lessons are taught about how some info should be kept to yourself, like your address, name, family PII, name of school etc..
- It's important to include why this topic is instructed: there are some people who want to trick you, and you can't give them ammo to do that.

K – 8: If it's too good to be true, it probably is



- At a slightly higher age, learning on social engineering can be continued.
- At this level, kids should be educated on piracy and how there are risks associated with torrenting software.
- As an addition, video game cheats and potentially malicious files can also be covered.
- This age commonly begins interacting in online spaces, so it's another add-on to the dangers of social engineering involved with malware.

5-8: Online bullying and harassment, and how to respond



- This subject is covered in most school districts around the US already, but the dynamic has changed with the world's increasing reliance with online communication
- Some things to go over in this range could be how to deal with online harassment or stalking, when to get an adult involved, and how to handle blackmail.
- It's worth it to look at how AI has affected extortion and coercion (image generation and impersonation.)

6 – 12: Socializing safely in online communities

- There is almost a completely absent form of curriculum in this topic in most school districts.
- Due to how common meeting people online has become, this section is crucial to teach kids how to safely communicate and interact with others on the internet.
- An important feature of safe communication is digital footprint, and how the effects reach much further than anticipated.
- "Never post something online you wouldn't want projected in the school auditorium during an assembly."

6 – 12: executable code, and how it can hurt you

- As kids grow older, they will understand more about computers and how to use them.
- Teaching kids about executable code at this age will be effective to fully communicate the risks that are ever present on devices.
- Talk about windows file extensions, and make sure to include the double-extension trick.
- Do not forget about keeping track of the warnings and alerts on the computer. Misunderstanding often leads people to click through important alerts.
- Make sure to stress that it is OKAY to talk to a trusted adult about virus or malware concerns.



9 – 12: Social engineering, phishing, and passwords



- At this point, students are in high school and are ready to understand areas like social engineering.
- Explain why having a secure password is important.
- Go into phishing, how it works, and talk about common forms of phishing.
- What to do when you are being scammed.

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

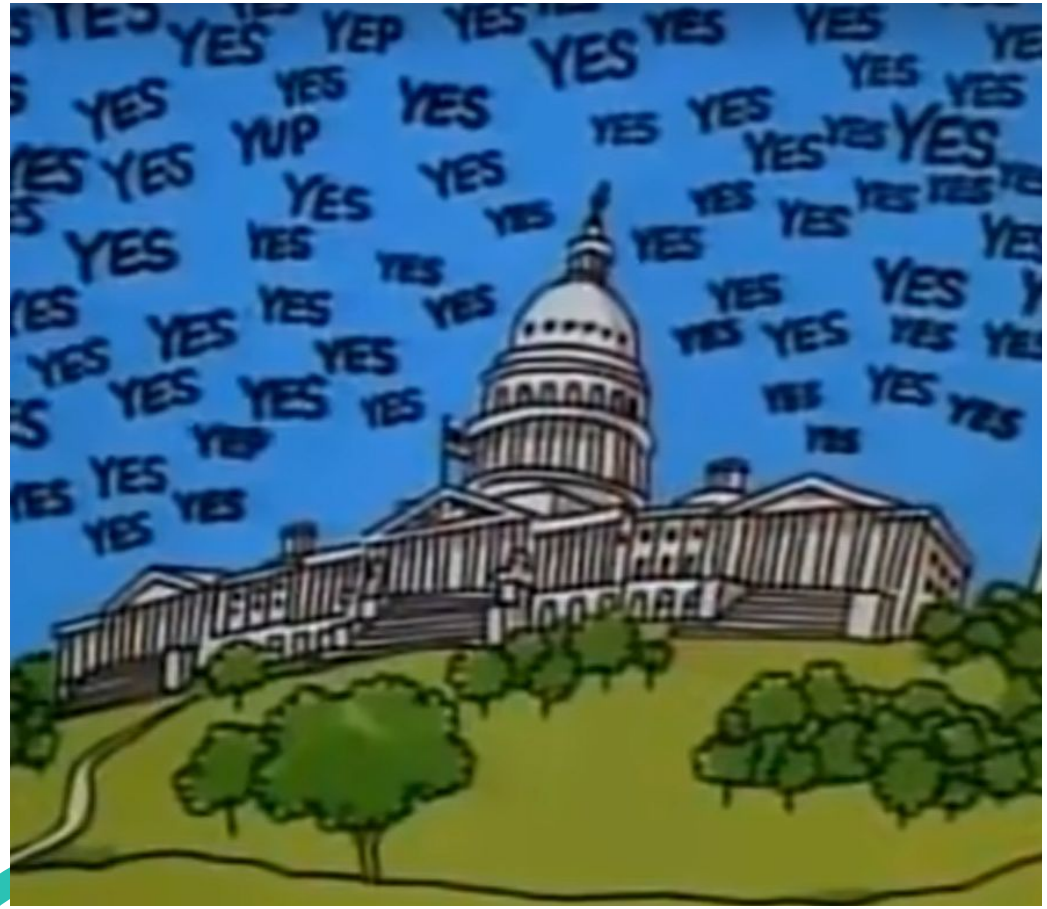


Career counselors and ambassadors



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.

My Call to Action and Your Involvement

- As hackers, many of us understand how dire of a problem this is for our country, and largely, the world.
- This presentation serves as a call to action regarding cybersecurity education and legislation.
- As much as I would like it, I cannot fight this battle alone, and I need your help.
- Get involved by sending letters to your legislators and state board of education.
- If you're a legislator or educator yourself, then make noise about this.



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?

Cisa security guidelines

DOE resources

US Cyber Games



https://mastodon.social/@hyenaa

XMechanica@protonmail.com

avi.mcgrady@gmail.com