TOP 5 THREATS TO K-12 ONLINE STUDENT SAFETY, DATA, AND CIPA COMPLIANCE

The Children's Internet Protection Act (CIPA)[1] requires schools to monitor minors' online content and behavior, safeguard their data, and protect them from online dangers as well as inappropriate or illegal content. The act requires schools to use web filtering technology to block categories of images, but does not specify other technologies. Unfortunately, web filtering is not enough. Without additional cybersecurity technology to detect and stop threats, it's impossible for schools to maintain compliance or, more importantly, keep students and their data safe.

Consider these top threats to K-12 student safety, student data, and compliance as you update internet safety policies and the technologies that enforce them.

1. Phishing Tops the List of K-12 Threat Concerns

From the headlines:

- *Phishing leads to unauthorized access of database containing 500,000 student records; breach goes undiscovered for nine months*
- *Student spear phishes teachers for passwords; elevates his grades and reduces others*

More than half of K-12 ed-tech leaders say phishing is a significant or very significant threat[2]—rightly so, since the education sector clicks on more phishing links than any other industry.[3] Adversaries continually generate realistic, fake websites or email addresses that mimic legitimate businesses and applications. Once they have your username and password, they go after your data or money. Students and educators do not have the time or expertise to discern between these near-perfect imitations. With scores of new websites created every minute, there is no way your web filtering product can block them all.

2. Internal Misuse Initiates Many Data Breaches

From the headlines:

- *School district sued after student Social Security numbers accidentally posted to district website*
- *Student erroneously given administrative privileges gains access to PII of 15,000 students*

"Miscellaneous errors" by educators accounted for 35% of education data breaches last year.[4] Internal misuse also includes bored students or those with malicious intent. Web filtering will not detect or stop internal misuse. Internal misuse can also result in other CIPA violations, such as students viewing inappropriate content through proxy avoidance tools.

3. More Computers Make Monitoring More Difficult

From the headlines:

- *Second-graders searching for "kissing" videos inadvertently access porn from classroom tablets*
- *Sixth-grade teacher reportedly watched porn in class; student viewed and filmed it*

In 2011, "monitoring the online activity of minors" was simple enough: teachers looked over students' shoulders in the computer lab. With the popularity of classroom tablets and 1:1 computing, that is no longer possible. Students and teachers can access internet resources anytime and anywhere. Again, with thousands of new websites created every day, it's unlikely your web filtering software can block them all. Any security policies and technologies should be flexible enough to encompass 1:1 devices, lab computers, and teaching and administrative computers.

4. Cyberbullying at School Compromises Student Safety

From the headlines:

- *Family sues school district after daughter's suicide; says school failed to protect her from cyberbullying by her classmates*

CIPA says schools must adopt a policy that addresses "the safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications." Most schools have bullying policies in place, subject to their state requirements and laws, but policies alone won't prevent cyberbullying. As curricula incorporate more technologies, the pathways for cyberbullying increase. Your cybersecurity technologies should help communicate bullying policies to students and staff as well as detect, investigate, and respond to bullying incidents.

5. Encrypted Traffic Hides Threats, Inappropriate Content

From the headlines:

- *Malware attacks are down, but encrypted attacks are up*[5]

Between 70% and 95% of web traffic is now encrypted. Encrypted traffic can hide threats, inappropriate content, or the stealthy actions of minors looking to circumvent content browsing restrictions. Deciding which traffic to decrypt can be tricky, with new sites and avoidance tools cropping up daily. Some web filtering products decrypt only the top 1,000 websites, leaving shady or new websites unencrypted and uninspected.

Web Filtering: Only a First Step

While CIPA is a good starting point for developing K-12 internet safety policies, the FCC last updated the rules in 2011. Since that time, internet technology has transformed K-12 learning environments and administration, leading to measurable benefits but also new risks. Whether a direct result of this gap or not, the volume of K-12 security incidents and data breaches has snowballed. School districts have been in the headlines for student hacks, unauthorized disclosures, data breaches, and more—all CIPA compliance violations.

CIPA Requirements

In summary, CIPA requires:

1. **Web filtering:** Block or filter pictures that: (a) are obscene, (b) contain child pornography, or (c) are harmful to minors (for computers used by minors).
2. **Monitoring online activity of minors:** Adopt a policy to monitor online activities of minors.
3. **Policy implementation:** Schools and libraries must adopt policies that address minors':
   a. Access to inappropriate matter on the internet
   b. Safety and security when using electronic mail, chat rooms, and other forms of direct electronic communication
   c. Unauthorized access, including so-called "hacking," and other unlawful activities
   d. Personal information and its unauthorized disclosure, use, and dissemination
   e. Access to materials harmful to them

Policy and Technology Considerations for Safety and Compliance

Web filtering is only one aspect of keeping students and data safe. As you work with school stakeholders and the broader community to develop, implement, and enforce internet safety policies, consider these practices to help combat top threats (see Figure 1).

Top Threat	Policy Considerations	Technology Considerations
Phishing	• Incorporate phishing training in staff technology training • Set up process for reporting suspicious emails • Plan a "phish test" for staff and send phony emails	• Implement multi-factor authentication • Block usernames and passwords from being transmitted to illegitimate websites

Internal misuse	• Train students and staff on:
	  ◦ Safe, ethical, and appropriate digital behavior
	  ◦ How to recognize and report threats such as cyberbullying or online predators
		• Enforce Zero Trust: "Never trust, always verify"
		• Scan for sensitive data leaving the network boundary, such as Social Security or credit card numbers
		• Block certain categories of URLs (e.g., hacking, proxy avoidance, anonymizers)
		• Block certain actions (e.g., uploads to file sharing sites)

Monitoring computers and other devices	• Ensure Acceptable Use Policies (AUPs) address:
	  ◦ Different users (e.g., staff, students of different ages)
	  ◦ Different devices (e.g., school-owned vs. BYOD)
	  ◦ Locations of devices (e.g., school vs. home)
	  ◦ Monitoring policies
	  ◦ Expectation of privacy
		• Enforce AUPs with granular security policies that take into account:
		  ◦ User or group and the apps they can access
		  ◦ Allowed devices
		  ◦ Other parameters (location, time of day, etc.)

Cyberbullying	• Develop a cyberbullying awareness program that promotes appropriate digital usage • Include cyberbullying in student AUPs	• Require students to use an always-on VPN • Monitor and possibly block high-risk functions (such as chat and video) in sensitive applications
Decrypting web traffic	• Develop a decryption policy that provides visibility into high-risk applications • Develop a policy for traffic that you choose not to decrypt for legal, regulatory, personal, or other reasons	• Decrypt and inspect content in questionable categories • Ensure privacy and do not decrypt traffic for certain verified sites, such as banking, healthcare, and shopping

Figure 1: Top threats and considerations

For More Information

To learn more about how Palo Alto Networks helps K-12 schools thwart these top five threats, visit our K-12 industry page.

For information on meeting and exceeding CIPA compliance with Palo Alto Networks, read Simplify CIPA Compliance with Palo Alto Networks.

1. Federal Communications Commission Children's Internet Protection Act, https://www.fcc.gov/consumers/guides/childrens-internet-protection-act.
2. "K-12 Cybersecurity: Big Threats and Best Practices," Education Week and the Consortium for School Networking, accessed September 26, 2019, https://www.edweek.org/ew/articles/technology/2019/03/20/k-12-cybersecurity-lessons-learned-from-constant-barrage.html.
3. "2019 Verizon Data Breach Investigations Report," Verizon, accessed September 26, 2019, https://enterprise.verizon.com/resources/reports/dbir/2019/data-breaches-by-industry.
4. Ibid.
5. "Malware-based Attacks Dropped 20% Worldwide," Dark Reading, July 24, 2019, https://www.darkreading.com/threat-intelligence/malware-based-attacks-dropped-20--worldwide/d/d-id/1335328.

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com

top-5-threats-to-k12-online-student-safety-data-and-cipa-compliance-brief-100319