Keeping Schools Safe

K-12 Network Security Checklist

Top Cyber Threats to Schools

What are the top cyber threats to schools and universities? Below are the most common threats schools need to monitor for and protect against.

1. Phishing and social engineering

Criminals use tactics such as phishing and social engineering to entice people to download malicious software and give them a path to enter the network.

2. Third-party vendor issues

To breach a school district or university, malicious actors may hack a smaller vendor to infiltrate the school's network.

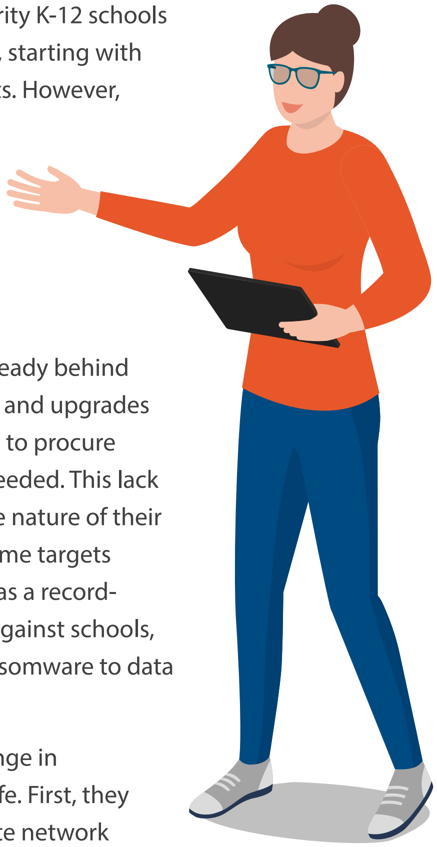
3. Unpatched and outdated software

Updating and installing all software patches and updates expediently is paramount to avoid a breach.

4. Internet of things

The internet of things (IoT) is a network of intertwined devices, software, and other 'things'. With different departments and audiences using a variety of tools in education, it can be hard to tell how many IoT devices are connected to the network at once.

When it comes to network security K-12 schools already have unique challenges, starting with small IT teams and strict budgets. However, unforeseen challenges and a record breaking rise in cyberattacks have further complicated cybersecurity for education.



Due to these budget and staff shortages, many districts are already behind in general technology adoption and upgrades and find themselves scrambling to procure and implement the resources needed. This lack of resources, plus the high-value nature of their data available, make schools prime targets for cyberattacks. In fact, 2020 was a record-breaking year for cyberattacks against schools, with incidents ranging from ransomware to data breaches increasing 18%.

IT teams certainly have a challenge in keeping schools and districts safe. First, they must ensure there is an adequate network setup that includes proper infrastructure and solutions to proactively block and prevent hackers and threats from infiltrating the network. Second, due to today's digital nature of education, they must ensure students and teachers have adequate bandwidth to optimize online learning tools and solutions. Thirdly, they must accommodate all the bring-your-own devices (BYOD) brought onto the campus by students and guests, while still maintaining control over what those devices can access when they connect to the school's network. And finally, schools need to maintain CIPA compliance by blocking students from accessing inappropriate content on websites and applications.

To stay ahead of evolving threats and hackers, while also maintaining CIPA compliance and ensuring the network always stays up and running for critical online learning tools, here are some simple steps schools can take to protect their students, staff and networks:

□ **Update Software**

Installing software patches and maintaining software updates and for all devices is crucial to ensure any vulnerabilities found are swiftly mitigated.

□ **Lock Down Administrative Control**

By preventing students and teachers from downloading applications that could house malware, you can minimize the exposure and protect the network.

□ **Separate Backups**

Keep backups of critical data in a separate, secured location. In the event of a malware or ransomware attack, schools can quickly get their data and configurations restored without paying the ransom.

□ **Separate Network for Guest/student Devices**

Separate the main school network from all the guest and student devices that you don't control. This will enable you to quickly mitigate any issues that may happen on the guest network without impacting the school network's performance and critical information.

□ **Use Captive Portal to Gain Visibility to Guest/ Student Devices**

Use a Captive Portal page that requires users to log in before gaining access to the network. You can then create rules and policies for what those devices can access while connected.

□ **Deploy Threat Intelligence**

Use solutions that have built-in threat intelligence engines that proactively protect against unknown and emerging threats is critical for schools to stay protected against hackers and malware.

□ **Deploy a Next-generation Firewall**

Provide protection at the gateway with a Next-gen firewall solution. Choose an all-in-one solution that encompasses web content and application filtering, bandwidth shaping, advanced threat protection, and VPN connectivity options.

□ **Review Reporting Tools**

Showcase your CIPA compliance with data-driven reporting. Ensure reporting includes detailed audit logs of every traffic event occurring on the network.

□ **Provide Training**

Conduct regular security awareness training for students, teachers and staff. Include instructions on passwords, phishing emails & links, and how to report suspicious activity.

□ **Check Vendors Thoroughly**

Vet all third-party platform providers. Now is the time to assess technology providers, added in the rush for online learning, to ensure they are secure and not exposing students to more risks.

□ **Develop a Cybersecurity Policy**

Develop a cybersecurity policy that includes security measures, regular auditing of cybersecurity preparedness and an updated disaster recovery plan.

□ **Invest in the Future**

Treat network security as more that a subset of IT. Create budget and staffing plans to ensure investments in up-to-date equipment, platforms and training, as well as develop contingency plans, to keep your school and students online and safe.

How Arista Can Help

Arista's Cognitive Unified Edge (CUE) solutions help enable school IT administrators to monitor, protect and control their networks while also providing protection from evolving threats. CUE products provide enhanced security and connectivity, flexible PoE switching, and Wi-Fi 6/6E offerings that work together seamlessly to ensure connectivity, protection, monitoring, and control across the entire network.

Centralized Cloud Based Management

- Visibility across globally dispersed networks & endpoints
- Zero touch deployment for hardware appliances
- Advanced alerting & reporting for CIPA compliance

Next Generation Firewall

- Next-gen firewall, with IPS, VPN & more
- Protection, encryption, control & visibility anywhere
- Block students from accessing inappropriate content
- Onboard security for small network appliances & IoT devices
- Full security processing on-premises or in the cloud

WAN Optimization

- Secure, WAN-optimized connectivity for learning
- Seamless scalability with centralized policy management
- Optimal predictive routing technology for first packet, dynamic path selection

Wired Connectivity

- Scalable PoE compact switches with 12 to 48 ports
- Based on Arista's Extensible Operating System (EOS)
- Wire rate encryption/tunneling
- Multi-gigabit uplink speeds from 1 to 100 Gbps

Wi-Fi 6 Access Points

- Enterprise class Wi-Fi 6 and Wi-Fi 6E technologies
- Optimized performance to scale from 1 to hundreds of users per AP
- Multi-gigabit uplink choices based upon bandwidth needs
- Open, published APIs for integration with ITSM and monitoring tools

Special Pricing on Arista Software

Public Sector pricing is available to qualifying state and local government institutions, public schools and libraries. This package contains the same software as NG Firewall Complete and Micro Edge, but at a greatly reduced rate.

Nonprofit pricing is available to qualifying not-for-profit institutions, NGOs, private schools and religious organizations. This package contains the same software as NG Firewall Complete and Micro Edge, but at a greatly reduced rate.

Santa Clara—Corporate Headquarters
5453 Great America Parkway,
Santa Clara, CA 95054

Phone: +1-408-547-5500
Fax: +1-408-538-8920
Email: info@arista.com

Ireland—International Headquarters
3130 Atlantic Avenue
Westpark Business Campus
Shannon, Co. Clare
Ireland

Vancouver—R&D Office
9200 Glenlyon Pkwy, Unit 300
Burnaby, British Columbia
Canada V5J 5J8

India—R&D Office
Global Tech Park, Tower A, 11th Floor
Marathahalli Outer Ring Road
Devarabeesanahalli Village, Varthur Hobli
Bangalore, India 560103

Singapore—APAC Administrative Office
9 Temasek Boulevard
#29-01, Suntec Tower Two
Singapore 038989