

Education Sector Bulletin

EXECUTIVE SUMMARY



Since September 2026, the Cal-CSIC has experienced an increase in requests for services following cyber incidents within the Public Education sector. This increase is consistent with broader trends observed by the federal government and private sector reporting and is almost certainly correlated to students and faculty returning to school. The best measures cybersecurity teams within the education sector can take involve fundamental security hygiene.

Background and Technical Trends

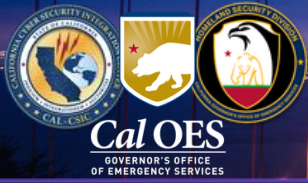


The Cal-CSIC receives information on state entity networks from the California Department of Technology (CDT) Security Operation Center (SOC). The CDT SOC Feed's true-positive malicious incidents show that the most important compromise pattern for schools is the repeated abuse of trusted identities, trusted mail, browser sessions, and remote administration pathways.

Across the reviewed education incidents, the clearest attack chains were:

- **Compromised education accounts** used to access cloud mail, Learning Management Systems (LMS), or other Software-as-a-Service (SaaS).
- **Session or token theft** followed by mailbox access, reconnaissance, and internal trust abuse.
- **Business email compromise (BEC)** that used inbox rules to hide activity and send phishing from trusted school accounts.
- **User-driven execution** through malicious links or ClickFix-style lures, followed by PowerShell and payload download.
- **Remote access software** used as an execution path for follow-on tooling.

These patterns become more dangerous during semester starts, exams, commencement, breaks, and summer or winter job cycles because schools are processing more account changes, more urgent communications, more payroll and HR activity, and more remote or after-hours work. The strategic implication is that seasonal defense should be organized around identity resilience, mail and SaaS monitoring, and rapid containment of trusted-account abuse.



Education Sector Bulletin

Mitigation Overview

CISA has compiled a detailed guide for implementing mitigations and recommendations for organizations within K-12 however the security guidance is applicable to all organizations within the education sector. The main points have been summarized below but please refer to the guide here for more details:

[K-12 Cybersecurity Foundations - Getting Started Guide](#)

- Authentication / Credentials (pg. 15-16)
- Reduce Attack Surface (pg.17-18)
- Implement and / or verify backups (pg. 19)
- Have an Incident Response Plan (pg. 20)

SHARING, REPORTING, AND SUPPORT

Sharing information and intelligence to state, local, federal, and private partners will ensure organizations across California can be better informed and defended.

For questions, concerns, or support or are interested in sharing information or intelligence in any cyber related matter, contact the Cal-CSIC via:

 916.636.2997

 calcsic@caloes.ca.gov

Report suspicious or suspected foreign activity and incidents to:

 Federal Officials at [CISA](#) and/or the [FBI](#) as applicable

 Coordinate with your regional Fusion Center

 Information, intelligence, and IOCs with ISACs