CIS Center for Internet Security®

MS-ISAC® Multi-State Information Sharing & Analysis Center®

Strengthen K-12 Cybersecurity at No Cost with an MS-ISAC Membership

Why Should a K-12 Join the MS-ISAC?

When one school faces an attack, it is likely that others will face the same type of attack. By joining the MS-ISAC, public K-12s become part of a community of more than 2,000 schools and districts who share cybersecurity information to improve their readiness against common threats.

With the onset of the COVID-19 pandemic and the shift to virtual learning, the risk to schools has only increased. School districts now rely more heavily on remote access technology and cloud services, which open up new avenues of cyber-attack. Additionally, there are now many more external devices accessing school and district resources, which further increases the risk to education institutions and everyone associated with them.

Members of the MS-ISAC have access to a 24/7 Security Operations Center, expert security resources, and sophisticated services that can both reduce their risk profile and help them defend themselves, at no cost.

The Multi-State Information Sharing and Analysis Center® (MS-ISAC®) is the focal point for cyber threat prevention, protection, response, and recovery for the nation's state, local, territorial, and tribal governments.

A division of the Center for Internet Security® (CIS®), the MS-ISAC collaborates and shares cybersecurity information among its 10,000 members, the U.S. Department of Homeland Security (DHS), and private sector partners.

Threats to K-12 Schools and Districts

CYBERCRIMINALS will target educational institutions for the same reason they target any entity—to make money. This can be done either by stealing and selling sensitive data, installing cryptocurrency miners, encrypting data and holding the key for ransom (ransomware), amongst other nefarious activities.

HACKTIVISTS are politically, socially, or ideologically motivated and target victims for publicity or to effect change, which can result in high profile operations. A typical hacktivist attack on an educational institution is defacing vulnerable websites with messages related to the hacktivist's cause.

INSIDERS include both student and faculty. Their unique and sometimes privileged access to accounts, devices, and networks could be abused for self-serving or destructive purposes.

Common K-12 network/data targets can include:

- **Student/Faculty Personally Identifiable Information (PII)**
- **Student/Faculty Protected Health Information (PHI)**
- **Email and other accounts**
- **Servers/hosts for CPU power, botnets, and command and control (C2) infrastructure**
- **Financial documents and information**
- **Any critical data that can be encrypted or wiped to adversely affect operations**

CIS Center for Internet Security®

MS-ISAC® Multi-State Information Sharing & Analysis Center®

Malicious Domain Blocking and Response (MDBR)

This new service from the MS-ISAC can help stop malicious threats in their tracks. This program leverages a cybersecurity-focused DNS service to block malicious domain requests before a connection is ever established. This helps limit infections related to known malware, ransomware, and phishing.

Ransomware can devastate an organization by shutting off access to critical computer systems until a ransom is paid. K-12 school districts have reportedly paid as much as $200,000 to attackers. MDBR can block the majority of ransomware infections simply by preventing the initial outreach to a ransomware delivery domain. Since its launch in July 2020, the MS-ISAC has welcomed more 550 member organizations to the service.

K-12 schools and districts are strongly encouraged to implement MDBR as soon as possible. It is an easy service that can be set up right away upon joining the MS-ISAC.

Top 4 Benefits of Joining the MS-ISAC for K-12s

1 Access to the 24x7x365 Security Operations Center (SOC)

Provides schools with round-the-clock support for any questions or incidents, including incident response.

2 Malicious Domain Blocking and Reporting (MDBR)

An easy way to reduce vulnerability and strengthen defenses. Schools/districts receive a detailed report every week from the SOC that includes all blocks logged at their location.

3 Participation in the annual National Cybersecurity Awareness Poster Contest

The contest encourages students to use the internet safely. Winning entries are included in the MS-ISAC Calendar. Entries may also be used in other national, regional and state cyber and computer security awareness campaigns.

4 CIS SecureSuite® Membership

No-cost access to resources for implementing and assessing CIS Benchmarks™ and CIS Controls® cybersecurity best practices.

Join Today at No Cost!

When a cyber incident occurs, K-12 school districts are required to devote precious resources to incident response services and other costly remediation efforts, including network upgrades. However, K-12 schools and districts can greatly reduce their risk simply by joining the MS-ISAC at no cost.

Join today at
https://www.cisecurity.org/ms-isac/k-12

Questions?
Contact MS-ISAC Member Services at info@msisac.org.

The MS-ISAC works closely with other organizations, such as the National Council of ISACs, the National Governors' Association, the National Association of State Chief Information Officers, and fusion centers, as well as other public and private sector entities to build trusted relationships to further enhance our collective cyber security posture.

Learn more at https://www.cisecurity.org/ms-isac/.