Public K-12s Can Defend Against Today's Cyber Threats with MDBR

Many public K-12s struggle to defend themselves against the barrage of cybersecurity threats they face on a daily basis. Not only are these challenges constantly evolving, but most educational institutions are not equipped with the resources, staff, and expertise they need to manage cybersecurity risk.

1,062

Publicly-disclosed cybersecurity-related incidents involving U.S. public schools since 2016.

114

U.S. public school districts that have experienced more than one cybersecurity incident since 2016.

With the onset of COVID-19 and the shift to virtual learning, public K-12s have exponentially more devices connecting to their networks that are not controlled by the district. This presents new ways for cyber-attacks, like ransomware, to impact their operations, students, and staff.

Luckily, there are resources available to public K-12s to help defend against such threats. All public K-12s can become members of the Multi-State Information Sharing and Analysis Center® (MS-ISAC®).

The MS-ISAC is the focal point for cyber threat prevention, protection, response, and recovery for the nation's state, local, territorial, and tribal governments.

Common Cyber Threat Actors

CYBERCRIMINALS target education entities to make money 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. A typical hacktivist attack on an educational institution is defacing vulnerable websites with messages related to the hacktivist's cause.

INSIDERS are current or former employees, contractors, or other partners who have access to an organization's networks, systems, or data. **MALICIOUS INSIDERS** intentionally misuse their network access to negatively affect the organization, while **UNWITTING INSIDERS** unintentionally cause harm through their actions, such as clicking on a phishing email link.

Common Network/Data Targets

Student/Faculty Personally Identifiable Information (PII)

Student/Faculty Protected Health Information (PHI)

Email and other accounts

Servers/hosts for processing power (e.g. cryptomining) or command and control (C2) infrastructure

Financial documents and information

Any critical data that can be encrypted or wiped to adversely affect operations

Common K-12 Cyber-Attacks in 2020

Both large and small school districts reported ransomware attacks.

Ransomware

K-12 public school districts have paid up to $200K to attackers.

28%

From January through July, 28% of the ransomware incidents reported involved K-12 school districts.

57%

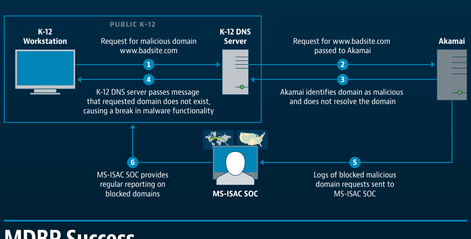
In August and September, 57% of the ransomware incidents reported involved K-12 school districts.

The No-cost Cybersecurity Solution for Public K-12s

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.

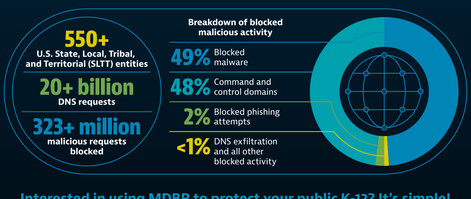
Membership also gives public K-12s access to Malicious Domain Blocking and Reporting (MDBR) at no-cost. MDBR technology promises to solve most of the above cybersecurity threats facing educational institutions today. MDBR technology prevents IT systems from connecting to harmful web domains, helping limit infections related to known malware, ransomware, phishing, and other cyber threats.

How MDBR Works



MDBR Success

Within the first 12 weeks, the MDBR service blocked over 323 million malicious requests from more than 550 state, local, tribal, and territorial government entities, including public K-12 schools.



Interested in using MDBR to protect your public K-12? It's simple!

Become a member of the MS-ISAC and sign up for the MDBR service to get started today.

Visit https://mdbr.cisecurity.org/

References

https://www.wsj.com/articles/hackers-smell-blood-as-schools-grapple-with-virtual-instruction-11603099802

https://k12cybersecure.com/