K-12 Ransomware Protection

Leverage ContentKeeper's School Web Filter to Shield Your Network and Data

Key Features:

- **Multi-Layered Malware Protection**
- **Malicious IP/URL Protection**
- **Defense Against Suspicious Apps**
- **Intelligent SSL Inspection**
- **Detailed Reporting on Suspicious App Use and Malware Activity**
- **Live Web Traffic Visibility**

Key Benefits:

- **Multi-Platform Support**
- **Safe Digital Learning**
- **Protect Your School's Investments**
- **Secure Remote Learners**

Ransomware Is on the Rise. Are Your Schools Safe?

K-12 school systems have become prime targets for ransomware attacks, especially with the rapid rise of mobile devices and remote learning. It's critical that a school Web filter be able to scan and identify malicious files and websites, as well as decrypt SSL traffic to expose threats that might otherwise be hidden within encrypted tunnels. School Web filters also must provide a live view of web traffic across all devices and platforms, with in-depth analytics to quickly identify potential attacks.

The Need for Ransomware Security in Web Filtering Tools

A key aspect of keeping students safe is protecting their data from ransomware and other attacks, so they can continue to learn and stay productive. A simple mistake, such as clicking on the wrong link, can result in serious security risks. It's essential for school districts to have strong safeguards in place to protect students, staff, and networks.

The cost of recovering from a ransomware attack is huge. Even when a ransom is paid, school systems report that they don't always get all their data back—and their IT systems nowhere near restored. Many more hours of work are required to get back to square one; a ransom payment is just the start of the expense, as some networks must be completely rebuilt to eliminate the infection.

How Does ContentKeeper Protect K-12 Networks?

School systems need robust defenses against ransomware attacks. Phishing is one of the most common vectors for these types of attacks. ContentKeeper protects against malicious links that are found in phishing emails; URL protection is a powerful tool included with ContentKeeper's Cloud Filtering and Security Platform.

In addition, ContentKeeper's App Defender can prevent students from accessing the Dark Web or using programs to download potentially infected BitTorrent files, two common sources for all kinds of virus-infected content—including ransomware. App Defender also prevents students from using VPNs to get around a school's filter and security policy, even when the VPN application is run from a live-boot flash drive or on a BYOD device.

These are just some of the tools available from ContentKeeper. What's more, the solution's comprehensive reporting features include a live view of web traffic and in-depth analytics, so districts can quickly analyze network and user activity for potential threats.

ContentKeeper.com
k12@ContentKeeper.com
US: +1 888.808.6848
Intl: +61 2 6261 4950