# AcademicAware

## Awareness Through Information Sharing

The Cybersecurity and Infrastructure Security Agency (CISA) has just launched it's Back to School Campaign. Please see the below message from CISA with important resources pertaining to this next school year.

---

Malicious cyber activity is on the rise across the United States and it is impacting organization of all sizes and in all sectors. Educational institutions are no exception when it comes to being the target of cyber criminals. That's why our team at the Cybersecurity and Infrastructure Security Agency (CISA) launched the 2021 Back to School campaign to bring awareness of the dangers of phishing and ransomware in K-12 and academia settings, and to share cybersecurity best practices.

Numerous reports of cyberattacks against K-12 educational institutions continue to be reported to CISA, FBI and the Multi-State Information Sharing and Analysis Center (MS-ISAC). According to MS-ISAC data, the percentage of reported ransomware incidents against K-12 schools increased at the beginning of the 2020 school year. In August and September, 57% of ransomware incidents reported to the MS-ISAC involved K-12 schools, compared to 28% of all reported ransomware incidents from January through July.

That's why it is important for educational institutions, parents and students to take cybersecurity seriously and learn how to protect themselves against a cyberattack. Malicious cyber actors are targeting school computer systems, slowing access, and rendering the systems inaccessible to basic functions, including remote learning. In some instances, ransomware actors stole and threatened to leak confidential student data unless institutions paid a ransom.

The federal government cannot confront the ever-growing threat of cyberattacks alone. That is why we encourage everyone - students, parents, teachers, and administrators– to explore these actionable cybersecurity resources and implement best practices.

During our Back to School campaign we will provide a range of information and actionable resources to help the educational community understand and mitigate cybersecurity risks. These resources for schools are all centrally located on the K-12 Resources section of StopRansomware.gov. Materials range from best practices for non-technical staff, as well as reference material for system administrators and other technical staff, to enhance their cybersecurity posture.

We encourage everyone - students, parents, teachers, and administrators – to explore these cybersecurity resources and implement best practices. In addition, we encourage chief information security officers of school districts to review StopRansomware.gov – a new website designed to help individuals and organizations prevent attacks that can severely impact business processes and leave organizations without the data they need to operate and deliver mission-critical services.

**This is an open-source product. Redistribution is encouraged.**

**View Virginia Fusion Center Homepage**

Click Here

**Observe Suspicious Activity?**

Report Online


**Virginia Shield Coalition**

***"Awareness Through Information Sharing"***

---

| | | |
|---|---|---|
| | **Need Help with this Email?** | **Useful Links** |
| | View in a browser | VFC Fusion Site |
| VFC Shield | | Shield Homepage |
| *"Awareness Through Information Sharing"* | Download as a PDF | All Products |
| | | Report SAR |
| | | Email Coordinator |