# Superintendent’s Memo #271-20


**COMMONWEALTH of VIRGINIA
Department of Education**

DATE: October 9, 2020

TO: Division Superintendents

FROM: James F. Lane, Ed.D., Superintendent of Public Instruction

## SUBJECT: Ransomware Information and Awareness

The VDOE is hosting a webinar on October 22 at 2:00 p.m. to spread awareness and provide technical assistance concerning ransomware attacks in our schools. It is encouraged that technology and instructional technology personnel responsible for cyber security in your division attend this webinar.

October is National Cybersecurity Awareness Month (NCSAM), a joint effort of the National Cybersecurity & Infrastructure Agency (CISA) and the Department of Homeland Security. The effort continues in its 17th year to raise awareness about the importance of cybersecurity across the Nation. The VDOE joins with CISA to spread cybersecurity awareness in our school divisions.

Ransomware is a form of malicious software that can encrypt files on an infected computer and extort payment for the files to be decrypted. Ransomware can easily spread on a network from computer to computer once a single device has been infected. A recent variant also threatens to breach encrypted data as a method of ensuring the ransom payment is made.

In 2020, the volume of known ransomware attacks has increased dramatically across all industries. Ransomware can be delivered to a computer via infected websites or files. Users are often directed to infected websites through the use of suspicious emails containing links or infected files. This method is called phishing.

Concerning Cybersecurity in our schools, ransomware and phishing attacks continue to be the most prevalent form of attack across the Nation aimed at schools and colleges. In Virginia, multiple school divisions have suffered from ransomware attacks over the past 18 months. These attacks have caused mass disruption to instruction and administrative functions and countless hours of lost productivity.

School divisions are encouraged to follow these basic and minimal best practices for protection against ransomware and phishing attacks.

* Review, configure, and utilize built-in tools for spam identification and blocking within the division’s email environment.
* Ensure the backup of critical systems and data stores is routine, often, and accurate. Extend backup strategies beyond servers to critical workstations or devices.
* Institute end-user training or awareness programs that encourage the recognition of suspicious email, websites, and web links.
* Regularly patch and update all available servers, workstations, and infrastructure devices.

The VDOE’s Chief Information Security Officer, Tim Tillman, and the Office of Information Security will host a webinar on **October 22, 2020 at 2PM** concerning ransomware in our schools. Representatives from FBI Richmond and the Virginia Fusion Center will present ransomware information, strategies, and incident response techniques. Technology and instructional leaders are invited to attend the webinar. Registration is required and is available at <https://cutt.ly/VAransomware>.

Please direct any questions to the Chief Information Security Officer, Tim Tillman, via email at tim.tillman@doe.virginia.gov.